K_1-congruences Between L-values of Elliptic Curves

Thomas Ward, BA

Thesis submitted to The University of Nottingham
for the degree of Doctor of Philosophy

June 2009

Abstract

We study the L-values of an elliptic curve E twisted by an Artin representation ρ. Specifically, we consider the case when ρ factors through the false Tate curve extension $\mathbb{Q}_{FT}/\mathbb{Q}$, which is defined by

$$\mathbb{Q}_{FT} := \bigcup_{n\geq 1} \mathbb{Q}\left(\mu_{p^n}, \sqrt[p^n]{\Delta}\right),$$

where p is an odd prime and Δ is a p-power free integer.

First, we consider a semistable elliptic curve E; we construct an integral-valued p-adic measure which interpolates the values $L(E, \rho \otimes \psi, 1)$ for a family of characters ψ. To do this, we exploit the fact that the value $L(E, \rho, 1)$ may be written as the Rankin convolution of two Hilbert modular forms, when ρ factors through the false Tate curve extension. Recent developments in non-abelian Iwasawa theory predict certain strong congruences between these p-adic L-functions, and we shall establish weakened versions of these congruences.

Next, we prove analogous results for an elliptic curve E with complex multiplication; we do this using work of Hida and Tilouine on the p-adic interpolation of Hecke L-functions over a CM-field. We go on to investigate the ratio of the automorphic and motivic periods associated to E over the totally real field $\mathbb{Q}(\mu_{p^n})^+$. We describe how the p-valuation of this ratio may be explicitly calculated, and use the computer package MAGMA to produce some numerical examples. We end by proving a formula for the growth of this quantity in terms of the Iwasawa invariants associated to the $\mathbb{Z}_p^2$-extension of the CM-field.

Acknowledgements

I would like to thank my supervisor, Daniel Delbourgo, for his continued guidance, instruction and motivation, which has been invaluable over the course of my PhD. I also thank my secondary supervisor, Nikolaos Diamantis, for his help and encouragement.

I thank Tim Dokchitser, Vladimir Dokchitser, Thanasis Bouganis and Neil Dummigan for their useful advice on my work. I am also grateful to John Cremona, Christian Wuthrich, Fabien Trihan, Konstantin Ardakov, and my fellow PhD students at Nottingham for many helpful conversations.

I thank my parents for their love and support, without which I would never have completed this thesis.

Finally, I wish to thank the EPSRC for funding my PhD studies, and the University of Nottingham for giving me the opportunity to carry out this research.

Contents

Chapter 1

Introduction

Iwasawa theory is a central area of modern number theory, with many deep results and tantalising conjectures. It provides links between the special values of motivic L-functions, and important arithmetic invariants of the motives.

A key concept in Iwasawa theory is that of a p-adic L-function: a p-adic analytic function which interpolates values of a complex Dirichlet series, for a given prime number p. The first example was the p-adic Riemann zeta function, which has its origins in Kummer's famous congruences between the Bernoulli numbers. Kubota and Leopoldt showed that these congruences were equivalent to the existence of a continuous function $\zeta_{p-\mathrm{adic}}(s, \omega^a)$ defined for $s \in \mathbb{Z}_p$, with the interpolation property

$$\zeta_{p-\mathrm{adic}}(1-k, \omega^k) \;=\; (1-p^{k-1})\zeta(1-k)$$

for every integer $k > 1$. Here we must point out that ω denotes the Teichmüller character modulo p, and the twist ω^a represents a choice of one of $p-1$ 'branches' of the p-adic zeta function. Each branch $\zeta_{p-\mathrm{adic}}(s, \omega^a)$ is analytic, except for $a \equiv 0 \mod (p-1)$; in this case there is a simple pole at $s = 1$, with residue $1 - p^{-1}$.

Iwasawa showed that the p-adic zeta function may be naturally interpreted as an

element $\mathcal{Z}$ of the completed group ring $\mathbb{Z}_p[[G]]$, where

$$G \;=\; \mathrm{Gal}\left(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}\right).$$

If we write $\chi : G \xrightarrow{\sim} \mathbb{Z}_p^\times$ for the cyclotomic character, then the interpolation property can be expressed as

$$\chi^k(\mathcal{Z}) \;=\; (1-p^{k-1})\,\zeta(1-k)$$

for all $k > 1$. This analytic p-adic zeta function is related to the algebraic invariants of the cyclotomic fields by the main conjecture of Iwasawa theory. This conjecture (which is now a theorem of Mazur and Wiles) asserts that $\mathcal{Z}$ is the characteristic element of a particular $\mathbb{Z}_p[[G]]$-module, constructed from the ideal class groups of the tower $\left(\mathbb{Q}(\mu_{p^n})\right)_{n\geq 1}$.

Much work has been done to generalise these ideas to the setting of elliptic curves. The analytic side of the the theory is provided by the Hasse-Weil L-series $L(E,s)$ associated to an elliptic curve E. If the curve is defined over the rational numbers, $L(E,s)$ is known to have an analytic continuation to the whole complex plane and satisfy a functional equation, thanks to the work of Wiles et al.

However, the algebraic side of the theory presents more problems: the appropriate p-adic Lie extension in this case is $\mathbb{Q}(E[p^\infty])/\mathbb{Q}$, given by adjoining the co-ordinates of all the p-power torsion points of $E(\overline{\mathbb{Q}})$. If E does not have complex multiplication, Serre has shown that $\mathcal{G} = \mathrm{Gal}\left(\mathbb{Q}(E[p^\infty])/\mathbb{Q}\right)$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$; in particular it is not commutative. In this case it was less clear how to formulate the main conjecture, as the definition of the characteristic ideal no longer works so well for $\mathbb{Z}_p[[\mathcal{G}]]$-modules.

Thankfully, recent progress has been made in the article [CFK$^+$05] of Coates, Fukaya, Kato, Sujatha and Venjakob: they present a new definition of characteristic elements, lying in the group $K_1\big(\mathbb{Z}_p[[\mathcal{G}]]\big)$, and conjecture the existence of a non-abelian p-adic L-function $\mathcal{L}_E$ lying in this K_1-group. The element $\mathcal{L}_E$ may be 'evaluated' at any Artin representation ρ of $\mathrm{Gal}(\mathbb{Q}(E[p^\infty])/\mathbb{Q})$, and should give the

twisted L-value $L(E, \rho, 1)$ multiplied by some explicit simple factors. According to the GL_2 main conjecture of [CFK$^+$05], $\mathcal{L}_E$ should be a characteristic element of the Selmer group of E over $\mathbb{Q}(E[p^\infty])$.

Even though we now know what form the non-abelian p-adic L-function should take, constructing it appears very difficult. Instead, let us consider a less challenging non-commutative p-adic Lie extension: we define

$$\mathbb{Q}_{FT} \;:=\; \mathbb{Q}\Big(\mu_{p^\infty},\, \sqrt[p^\infty]{\Delta}\Big),$$

the so-called 'false Tate curve extension' of $\mathbb{Q}$, whose Galois group is a semi-direct product of $\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$. In this case, the conjectures of [CFK$^+$05] predict an analogous p-adic L-function $\mathcal{L}_{E/\mathbb{Q}_{FT}}$, lying in a K_1-group.

In his recent paper [Kat05], Kato has shown that the existence of $\mathcal{L}_{E/\mathbb{Q}_{FT}}$ is equivalent to a set of explicit congruences between a family of abelian p-adic L-functions $\{\mathcal{L}(E, \rho_n) : n \geq 1\}$. Each ρ_n is a fixed Artin representation of $\mathrm{Gal}(\mathbb{Q}_{FT}/\mathbb{Q})$, and the element $\mathcal{L}(E, \rho_n)$ satisfies an interpolation property

$$\psi\Big(\mathcal{L}(E, \rho_n)\Big) \;=\; \text{simple factors} \;\times\; \frac{L(E, \rho_n \otimes \psi, 1)}{\text{complex period}}$$

at appropriate finite-order characters $\psi : \mathbb{Z}_p^\times \to \mathbb{C}^\times$. In this thesis, we will study the non-abelian twisted L-values $L(E, \rho, 1)$ for representations ρ which factor through $\mathbb{Q}_{FT}/\mathbb{Q}$. Our aim is to establish a version of the 'K_1-congruences' predicted by Kato.

In Chapter 2 we give the notation and background which we will need. We recall the definition of the L-series attached to an elliptic curve, and how it may be twisted by an Artin representation. We go on to give a very brief account of the GL_2 main conjecture, as set out by Coates et al in [CFK$^+$05]. We explicitly describe the Artin representations of $\mathbb{Q}_{FT}/\mathbb{Q}$, and give the congruences which are predicted by Kato in this case.

In Chapter 3 we review the definitions and basic properties of Hilbert modular forms, following Panchishkin [Pan91] and Shimura [Shi78]. In particular, we study

the Rankin convolution $L(\mathbf{f}, \mathbf{g}, s)$ of two Hilbert modular forms $\mathbf{f}$ and $\mathbf{g}$. This is motivated by the following fact: if $E/\mathbb{Q}$ is an elliptic curve and ρ is an irreducible Artin representation which factors through $\mathbb{Q}_{FT}/\mathbb{Q}$, one can write the twisted L-function $L(E, \rho, s)$ as a Rankin convolution $L(\mathbf{f}_E, \mathbf{g}_\rho, s)$.

The material in Chapter 4 is original work, and it appears in the article [DW08]. We construct the abelian p-adic L-functions $\mathcal{L}(E, \rho_n)$ for a semistable elliptic curve E, by studying the special values $L(\mathbf{f}_E, \mathbf{g}_{\rho_n \otimes \psi}, 1)$ for finite-order twists $\psi : \mathbb{Z}_p^\times \to \mathbb{C}^\times$. Using the machinery of Hilbert modular forms, we then prove our first set of K_1-congruences (Theorem 4.6.7).

Next, we turn our attention to elliptic curves with complex multiplication. It is well known that the L-series of a CM elliptic curve may be written as a product of Hecke L-series, so in Chapter 5 we review some results on the p-adic interpolation of Hecke L-functions over a CM-field. In particular, we are interested in the p-adic L-function constructed by Hida in [Hid91], which interpolates another version of the Rankin convolution.

In Chapter 6 we tackle the K_1-congruences for the case of CM elliptic curves. The result (Theorem 6.1.3) follows from making an appropriate specialisation of Hida's p-adic L-function. When comparing the motivic p-adic L-function $\mathcal{L}(E, \rho_n)$ with its Rankin convolution counterpart, we encounter two error terms: one related to a congruence module of $\mathbf{f}_E$, and another to the ratio of the Néron periods with the Petersson inner product $\langle \mathbf{f}_E, \mathbf{f}_E \rangle$. We discuss how the p-part of these terms may be explicitly calculated, and compute some numerical examples to show how fast it grows as we climb the cyclotomic tower. Finally, we obtain a formula for the growth of this error in terms of the Iwasawa invariants of the $\mathbb{Z}_p^2$-extension (Theorem 6.1.6).

Chapter 2

Background

In this chapter we give some background on the material that will be studied in the following chapters.

First, we recall the definition and basic properties of the L-series $L(E, \rho, s)$ associated to an elliptic curve E twisted by an Artin representation ρ. We then briefly discuss the Iwasawa theory of elliptic curves, and in particular the GL_2 main conjecture which was formulated by Coates, Fukaya, Kato, Sujatha and Venjakob in [CFK$^+$05]. The problem of constructing the (conjectural) non-abelian p-adic L-function $\mathcal{L}_E$ predicted in their article is the motivation for this thesis.

Kato proves in [Kat05] that, in certain cases, the existence of $\mathcal{L}_E$ is equivalent to congruences between abelian p-adic L-values associated to twists $E \otimes \rho$. We will describe Kato's results in a simple case: that of the false Tate curve extension of $\mathbb{Q}$.

The material on Iwasawa theory is based on Venjakob's survey [Ven], and the reference for l-adic representations and L-series is Tate's exposition [Tat79].

2.1 Properties of l-adic Representations

Let K be a number field. Throughout we fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ inside which all our number fields lie, so we may define the absolute Galois group $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. For a rational prime l, an *l-adic representation* of G_K will be a continuous homomorphism

$$\rho_l \ : \ G_K \longrightarrow \mathrm{GL}(V_l)$$

where V_l is a finite dimensional vector space over $\mathbb{Q}_l$.

Suppose we have a set $V = \{V_l \mid l \text{ prime}\}$ of l-adic representations of G_K. Given a finite place v of K, if we choose any rational prime l such that $v \nmid l$ we may define a local polynomial

$$P_v(V/K, T) \ = \ \det\left(1 - \Phi_v T \,\middle|\, V_l^{I_v}\right)$$

where I_v is the inertia subgroup and $\Phi_v \in \mathrm{Gal}(\overline{K}_v/K_v)$ is a geometric Frobenius element at v (i.e. Φ_v is chosen so that its image modulo I_v is Frob_v^{-1}). We will say that our set V is *compatible* if the definition of $P_v(V/K, T)$ is independent of the choice of l (provided $v \nmid l$). Assuming V is a compatible set of l-adic representations of G_K, we attach a complex L-series to V as an Euler product:

$$L(V/K, s) \ := \ \prod_v P\left(V/K,\ q_v^{-s}\right)^{-1}.$$

where $q_v = \#k_v$ is the cardinality of the residue field at v. This L-series should converge when $\mathrm{Re}(s)$ is sufficiently large, and for the particular examples of V we will look at, it will have a meromorphic continuation to the whole complex plane.

2.2 Artin Representations

Let K be a number field as above, and let ρ be a finite-dimensional complex representation of $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. If there exists a finite extension M/K such that ρ factors through the quotient map

$$\mathrm{Gal}(\overline{\mathbb{Q}}/K) \twoheadrightarrow \mathrm{Gal}(M/K)$$

then we call ρ an *Artin representation over* K. Such a representation may always be realised over a finite extension of $\mathbb{Q}$, so we may certainly write

$$\rho \ : \ G_K \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}).$$

Given a rational prime l, we fix an embedding

$$\overline{\mathbb{Q}} \ \hookrightarrow \ \overline{\mathbb{Q}}_l$$

and we attach an l-adic representation to ρ by simply extending scalars from $\overline{\mathbb{Q}}$ to $\overline{\mathbb{Q}}_l$:

$$V_l(\rho) \ := \ \rho \otimes \overline{\mathbb{Q}}_l.$$

One can check that $\{V_l(\rho)\}$ is a compatible set of l-adic representations, so we may define the *Artin L-function* $L(\rho, s)$ to be the L-function associated to $\{V_l(\rho)\}$ in the sense of Section 2.1. To be precise,

$$L(\rho, s) \ = \ \prod_v \det\Big(1 - \Phi_v \, q_v^{-s} \,\Big|\, V_l^{I_v}\Big)^{-1}.$$

Artin L-functions display a useful property known as *Artin formalism*: suppose M and K are two number fields such that $M \supset K$, and ρ is an Artin representation over M. Then there is a representation $\mathrm{Ind}_M^K(\rho)$ obtained by inducing ρ from $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$ to $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, and we have the identity

$$L(\rho/M, s) \ = \ L\big(\mathrm{Ind}_M^K(\rho)/K, s\big).$$

The Artin L-function $L(\rho/K, s)$ is known to have a meromorphic continuation to the entire complex plane. Further, there is a certain product of Gamma factors $L_\infty(\rho, s)$ such that the completed L-function

$$\tilde{L}(\rho, s) \ = \ L_\infty(\rho, s) \, L(\rho, s)$$

satisfies the functional equation

$$\tilde{L}(\rho, s) \ = \ \epsilon(\rho, s) \, \tilde{L}(\rho^\vee, 1 - s)$$

where $\rho^\vee$ is the contragredient representation of ρ, and the epsilon factor $\epsilon(\rho, s)$ is given by

$$\epsilon(\rho, s) \;=\; w(\rho)\;\left(|D_K|^{\dim \rho} N_{K/\mathbb{Q}}(\mathfrak{f}_\rho)\right)^{1/2-s}$$

where $w(\rho)$ is a complex number of absolute value 1, and $\mathfrak{f}_\rho$ is the global conductor of ρ over K (as defined in Chapter VI of [CF67]).

2.3 The L-function of an Elliptic Curve

Let E be an elliptic curve over a number field K. Let l be a rational prime, and write $E[l^n]$ for the l^n-torsion points in $E(\overline{\mathbb{Q}})$. This group is abstractly isomorphic to $(\mathbb{Z}/l^n\mathbb{Z}) \times (\mathbb{Z}/l^n\mathbb{Z})$, and has a natural Galois action of $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, so we get a representation

$$\rho_{l^n} \;:\; G_K \longrightarrow \mathrm{Aut}\big(E[l^n]\big) \;\cong\; \mathrm{GL}_2\left(\frac{\mathbb{Z}}{l^n\mathbb{Z}}\right).$$

We can take the projective limit of these finite modules to obtain the *l-adic Tate module*

$$T_l(E) \;:=\; \varprojlim_n E[l^n]$$

and we obtain an action of G_K:

$$\rho_{l^\infty} \;:\; G_K \longrightarrow \mathrm{Aut}\big(T_l(E)\big) \;\cong\; \mathrm{GL}_2\left(\mathbb{Z}_l\right).$$

Then we define an l-adic representation of G_K by extending scalars to $\overline{\mathbb{Q}}_l$:

$$V_l(E) \;:=\; T_l(E) \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}}_l.$$

It can be checked that the set $\{V_l(E)\}$ is a compatible set of l-adic representations, so we may associate an L-series to $\{V_l(E)\}$ in the sense of Section 2.1. This is the *Hasse-Weil L-series of E over K*, and we denote it by $L(E/K, s)$.

One may give a more explicit description of $L(E/K, s)$. Let v be a finite place of K at which E has good reduction, and let $\tilde{E}_v$ be the reduced curve over the residue

field k_v. Define the integer $a_v(E)$ by

$$a_v(E) \;:=\; 1 + q_v - \#\tilde{E}_v(k_v)$$

and then we can write the local polynomial as

$$P_v(E,T) \;=\; 1 - a_v(E)\,T + q_v\,T^2.$$

If instead E has bad reduction at v, we put

$$P_v(E,T) \;:=\; \begin{cases} 1+T & \text{if } E \text{ has split multiplicative reduction at } v \\ 1-T & \text{if } E \text{ has non-split multiplicative reduction at } v \\ 1 & \text{if } E \text{ has additive reduction at } v \end{cases}$$

Then the L-series $L(E,s)$ is given by the following Euler product, which converges for $\mathrm{Re}(s) > 3/2$.

$$L(E,s) \;:=\; \prod_v P_v(E, q_v^{-s})^{-1}$$

where v ranges over all finite places of K.

Further, given an Artin representation ρ over K, we can define the twisted L-function $L(E,\rho,s)$ as the L-function associated to the l-adic representations $V_l(E) \otimes V_l(\rho)$.

Conjecture 2.3.1. *Let E be an elliptic curve over a number field K, and ρ an Artin representation of G_K. Then the twisted L-function $L(E,\rho,s)$ can be continued to an analytic function on the entire complex plane. Further, if we write*

$$\Gamma_{\mathbb{C}}(s) \;=\; \pi^{-s-1/2}\,\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)$$

and define the completed L-function

$$\tilde{L}(E,\rho,s) \;=\; \Gamma_{\mathbb{C}}(s)^{[K:\mathbb{Q}]\dim\rho}\,L(E,\rho,s),$$

we have a functional equation of the form

$$\tilde{L}(E,\rho,s) \;=\; \epsilon_K(E,\rho,s)\;\tilde{L}(E,\rho^\vee,2-s).$$

Here we write $\epsilon_K(E, \rho, s)$ for the global epsilon factor associated to the twist $E \otimes \rho$, which is defined in [Tat79]. When $K = \mathbb{Q}$ it may be written

$$\epsilon_{\mathbb{Q}}(E, \rho, s) \;=\; w(E, \rho)\, N(E, \rho)^{1-s}$$

where $w(E, \rho)$ is a complex number of absolute value 1, and $N(E, \rho)$ is the global conductor of $E \otimes \rho$.

If we set ρ to be the trivial representation of G_K, we have a conjectural functional equation for $L(E/K, s)$ as a special case of Conjecture 2.3.1.

Suppose now that E is defined over $\mathbb{Q}$ by a fixed minimal Weierstrass equation, and let ω_E be the Néron differential on E. Choose generators γ_+ and γ_- of the subspaces of $H_1\big(E(\mathbb{C}), \mathbb{Z}\big)$ on which complex conjugation acts by $+1$ and -1 respectively. We then have the transcendental Néron periods associated to E:

$$\Omega_E^+ \;=\; \int_{\gamma+} \omega_E, \qquad\qquad \Omega_E^- \;=\; \int_{\gamma-} \omega_E.$$

We will follow the usual convention that $\gamma_\pm$ are chosen so that Ω_E^+ and $-i\Omega_E^-$ are positive real numbers.

Conjecture 2.3.2. *Let E be an elliptic curve and ρ an Artin representation, both defined over $\mathbb{Q}$. Write $d^+(\rho)$ and $d^-(\rho)$ for the dimensions of the subspaces of $V(\rho)$ on which complex conjugation acts by $+1$ and -1 respectively. Then*

$$\frac{L(E, \rho, 1)}{{\Omega_E^+}^{d^+(\rho)} {\Omega_E^-}^{d^-(\rho)}} \;\in\; \overline{\mathbb{Q}}.$$

This algebraicity conjecture is a consequence of Deligne's period conjecture.

2.4 Modularity of Elliptic Curves

Let E be an elliptic curve over $\mathbb{Q}$, with conductor N_E and L-series

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

We will say that the curve E is *modular* if there is a modular cusp form f_E of weight 2 and level N_E such that

$$f_E(z) \;=\; \sum_{n=1}^{\infty} a_n(E)\ \exp(2\pi i n z),$$

i.e. the Fourier coefficients of f_E are the same as the Dirichlet coefficients of $L(E,s)$. This assertion is equivalent to the existence of a *modular parametrisation* of E, by which we mean a surjective $\mathbb{Q}$-rational morphism

$$\varphi_E \;:\; X_0(N_E) \;\twoheadrightarrow\; E$$

where $X_0(N)$ is the usual compactified modular curve.

Theorem 2.4.1. *All elliptic curves over $\mathbb{Q}$ are modular.*

This very important result was proved for semistable elliptic curves by Wiles and Taylor, and was extended to all elliptic curves over $\mathbb{Q}$ by Breuil, Conrad, Diamond and Taylor (see [Wil95] and [BCDT01]).

Given any elliptic curve E over $\mathbb{Q}$, it is a consequence of Theorem 2.4.1 that Conjecture 2.3.1 holds for E; that is, the L-function $L(E,s)$ has the claimed analytic continuation and functional equation.

2.5 Selmer Groups

For an elliptic curve E over a number field K, the p-primary Selmer group $\mathrm{Sel}_K(E)_{p^\infty}$ is defined by the short exact sequence

$$0 \;\longrightarrow\; \mathrm{Sel}_K(E)_{p^\infty} \;\longrightarrow\; H^1\left(K, E[p^\infty]\right) \;\longrightarrow\; \prod_v H^1\left(K_v, E(\overline{K}_v)\right)[p^\infty]$$

where the product is taken over all non-archimedean places v of K. Similarly, the Tate-Shafarevich group $Ш_K(E)$ is defined by the exact sequence

$$0 \;\longrightarrow\; Ш_K(E) \;\longrightarrow\; H^1\left(K, E\right) \;\longrightarrow\; \prod_v H^1\left(K_v, E(\overline{K}_v)\right).$$

These groups are connected to the Mordell-Weil group $E(K)$ by the following exact sequence:

$$0 \longrightarrow E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_K(E)_{p^\infty} \longrightarrow Ш_K(E)[p^\infty] \longrightarrow 0.$$

We define the Pontryagin dual of the Selmer group to be

$$X(E/K) = \mathrm{Sel}_K(E)^\vee_{p^\infty} := \mathrm{Hom}\left(\mathrm{Sel}_K(E)_{p^\infty}, \mathbb{Q}_p/\mathbb{Z}_p\right).$$

When K is a p-adic Lie extension of $\mathbb{Q}$, this module plays a key role in the Iwasawa theory of elliptic curves.

2.6 Iwasawa Theory for Elliptic Curves

For the remainder of this chapter, we fix an elliptic curve E over $\mathbb{Q}$ and an odd prime p at which E has good ordinary reduction.

Let $K_n = \mathbb{Q}(E[p^n])$ be the field generated over $\mathbb{Q}$ by the coordinates of the p^n-torsion points of E, and let

$$K_\infty = \bigcup_{n \geq 1} K_n.$$

Then the representation ρ_{p^n} from Section 2.3 factors through $K_n/\mathbb{Q}$, and therefore ρ_{p^∞} factors through $K_\infty/\mathbb{Q}$. The Galois group $G = \mathrm{Gal}(K_\infty/\mathbb{Q})$ is a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$, so G is a p-adic Lie group (i.e. a topological group with local coordinates in a p-adic field, given by analytic charts).

We define the Iwasawa algebra of G:

$$\Lambda(G) := \varprojlim_U \mathbb{Z}_p[G/U],$$

where U runs over all open normal subgroups of G. In contrast to classical cyclotomic Iwasawa theory, $\Lambda(G)$ is not commutative.

The group $X(E/K_n) = \mathrm{Sel}(E/K_n)^\vee$ has a natural Galois action, which makes it into a compact $\mathbb{Z}_p[\mathrm{Gal}(K_n/\mathbb{Q})]$-module. Passing to the projective limit, we can regard

$$X(E/K_\infty) \;=\; \varprojlim_n \mathrm{Sel}(E/K_n)^\vee$$

as a finitely generated $\Lambda(G)$-module. In the Iwasawa theory of elliptic curves, one wants to formulate an appropriate main conjecture which relates this Λ-module to an analytic p-adic L-function.

Suppose that E admits complex multiplication by an order in the ring $\mathcal{O}_K$, for some imaginary quadratic field K. It can be shown that the group $\mathrm{Gal}\big(K(E[p^\infty])/K\big)$ has structure

$$\mathrm{Gal}\big(K(E[p^\infty])/K\big) \;\cong\; \mathbb{Z}_p^2 \;\times\; \text{finite abelian group}\,;$$

in particular it is abelian. In this case the theory is relatively well understood: a version of the main conjecture can be formulated. It is known as the *two variable main conjecture*, and has been proved by Rubin in many cases.

If the curve E does not admit complex multiplication, a theorem of Serre (see [Ser98]) implies that $G = \mathrm{Gal}\big(\mathbb{Q}(E[p^\infty])/\mathbb{Q}\big)$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ (for this reason it is referred to as the 'GL_2 case'). Here G is non-abelian, and the theory becomes much more difficult; in particular the naive definition of characteristic elements for $\Lambda(G)$-modules breaks down, and a new approach is required to formulate the main conjecture.

2.7 The GL_2 Main Conjecture

In the key paper [CFK$^+$05], Coates, Fukaya, Kato, Sujatha and Venjakob establish a new version of characteristic elements in the GL_2 case, by using the K-group $K_1(\Lambda(G))$. This allows them to formulate a GL_2 main conjecture, which we now briefly summarise. We now must assume $p \geq 5$ for technical reasons.

In [CFK$^+$05], Coates et al first define a canonical Ore set $\mathcal{S}^*$ of $\Lambda(G)$ (the term 'Ore set' essentially means that the right localisation $\Lambda(G)_{\mathcal{S}^*}$ may be defined). They consider the category $\mathfrak{M}_H(G)$ of all finitely generated $\Lambda(G)$-modules which are $\mathcal{S}^*$-torsion. The module $X(E/K_\infty)$ is conjectured to lie in $\mathfrak{M}_H(G)$, and this can be checked explicitly in certain cases.

There is a long exact sequence of K-groups containing the connecting map

$$\partial_G \ : \ K_1\left(\Lambda(G)_{\mathcal{S}^*}\right) \longrightarrow K_0\left(\mathfrak{M}_H(G)\right)$$

and it is proved in [CFK$^+$05] that, under our assumptions on E and p, the map ∂_G is surjective. Therefore if $M \in \mathfrak{M}_H(G)$ one may define a characteristic element of M to be any $\xi_M \in K_1(\Lambda(G)_{\mathcal{S}^*})$ such that

$$\partial_G(\xi_M) \ = \ [M] \ \ \in \ K_0\left(\mathfrak{M}_H(G)\right).$$

This definition deals with the algebraic side of the main conjecture; now we discuss the conjectural analytic p-adic L-function. Let $\rho : G \longrightarrow \mathrm{GL}_n(F)$ be an Artin representation, where F is a finite extension of $\mathbb{Q}$, and let ξ be an element of $K_1(\Lambda(G)_{\mathcal{S}^*})$. In [CFK$^+$05], Coates et al outline a recipe which assigns to ξ and ρ an element

$$\xi(\rho) \ \in \ F \cup \{\infty\},$$

so we may 'evaluate' ξ at the Artin representation ρ. The p-adic L-function is conjectured to be an element $\mathcal{L}_E$ of $K_1(\Lambda(G)_{\mathcal{S}^*})$ such that evaluating it at ρ yields essentially the complex L-value $L(E, \rho, 1)$. Let us state the exact interpolation formula: we write

$$R \ = \ \{p\} \ \cup \ \{ \text{ primes } q \ : \ \mathrm{ord}_q(j_E) < 0\}$$

and define

$$L_R(E, \rho, s) \ := \ \prod_{q \notin R} P_q(E, \rho, q^{-s})^{-1}$$

to be the L-function of $E \otimes \rho$ with the Euler factors at the primes in R removed. We let N_ρ be the conductor of ρ, and put

$$f_p(\rho) \ := \ \mathrm{ord}_p(N_\rho).$$

As we assumed that E is ordinary at p, we may factorise the local polynomial $P_p(E,T)$ as

$$1 - a_p(E)\,T + p\,T^2 \;=\; (1-\alpha_p T)\,(1-\alpha'_p T)$$

where $\alpha_p \in \mathbb{Z}_p^\times$ and $\alpha'_p \in p\,\mathbb{Z}_p$.

We write $\rho^\vee$ for the contragredient representation of ρ, and $\epsilon_p(\rho)$ for the local epsilon factor at p attached to ρ. In fact, this local epsilon factor depends on a choice of additive character and Haar measure on $\mathbb{Q}_p$, and we adopt the standard choices which are used in [CFK$^+$05]. As before we write $d^+(\rho)$ and $d^-(\rho)$ for the dimensions of the subspaces of $V(\rho)$ on which complex conjugation acts by $+1$ and -1 respectively. The periods $\Omega_E^\pm$ are the transcendental Néron periods as before.

Now we are able to state the following conjectures of Coates, Fukaya, Kato, Sujatha and Venjakob from [CFK$^+$05].

Conjecture 2.7.1. *Assume that $p \geq 5$ and that E has good ordinary reduction at p. Then there exists $\mathcal{L}_E \in K_1(\Lambda(G)_{\mathcal{S}^*})$ such that, for all Artin representations ρ of G, we have $\mathcal{L}_E(\rho) \neq \infty$ and*

$$\mathcal{L}_E(\rho) \;=\; \epsilon_p(\rho)\;\frac{P_p(\rho^\vee,\alpha_p^{-1})}{P_p(\rho,\alpha_p'^{-1})}\;\;\alpha_p^{-f_p(\rho)}\;\;\frac{L_R(E,\rho,1)}{\Omega_E^{+\,d^+(\rho)}\Omega_E^{-\,d^-(\rho)}}.$$

In fact, Conjecture 2.7.1 also makes sense in the case when E admits complex multiplication. In this case the conjecture follows from the existence of the two-variable p-adic L-function of E, which features in the two-variable main conjecture.

Conjecture 2.7.2. **(GL_2 Main Conjecture)** *Assume that $p \geq 5$, that E has good ordinary reduction at p, and that $X(E/K_\infty) \in \mathfrak{M}_H(G)$. Then the p-adic L-function $\mathcal{L}_E \in K_1(\Lambda(G)_{\mathcal{S}^*})$ is a characteristic element of $X(E/K_\infty)$.*

Recently, Burns has shown that Conjecture 2.7.2 is equivalent to a family of classical abelian versions of the main conjecture, and the assertion that $\mathcal{L}_E$ exists (see [Bur07]). The existence of $\mathcal{L}_E$ has not yet been shown for any elliptic curve without complex multiplication.

2.8 The False Tate Curve Extension

To gain an insight into Conjecture 2.7.1 we could first try to prove a simpler version of it: we could replace the extension $\mathbb{Q}(E[p^\infty])/\mathbb{Q}$ by a more elementary non-abelian p-adic Lie extension.

Let $\Delta > 1$ denote a p-power free integer which is prime to p. The so-called *false Tate curve extension* of $\mathbb{Q}$ is defined as

$$\mathbb{Q}_{FT} := \bigcup_{n\geq 1} \mathbb{Q}\left(\mu_{p^n}, \sqrt[p^n]{\Delta}\right).$$

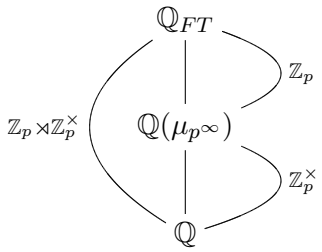
It is easy to see that

$$\mathrm{Gal}\left(\mathbb{Q}\left(\mu_{p^n}, \sqrt[p^n]{\Delta}\right)/\mathbb{Q}\right) \cong \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right) \rtimes \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^\times$$

so, by infinite Galois theory, $\mathrm{Gal}(\mathbb{Q}_{FT}/\mathbb{Q})$ is the projective limit of these groups:

$$\mathrm{Gal}(\mathbb{Q}_{FT}/\mathbb{Q}) \cong \begin{pmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix} \lhd \mathrm{GL}_2(\mathbb{Z}_p).$$

In other words, the Galois group is a semi-direct product of two p-adic Lie groups of dimension one. In terms of a field diagram,



The Artin representations of $G_{FT} := \mathrm{Gal}\left(\mathbb{Q}_{FT}/\mathbb{Q}\right)$ can be made very explicit: it is proved in [Dok05] that G_{FT} has a unique self-dual representation of dimension $\phi(p^n) = p^n - p^{n-1}$, which we denote by ρ_n, for each $n \geq 1$.

Further, it can be shown that each of these representations is induced from a 1-dimensional representation over a cyclotomic field. To be precise: if we write $U^{(n)}$

for the kernel of the quotient map $\mathbb{Z}_p^\times \twoheadrightarrow (\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times$, then we have

$$\mathrm{Gal}\left(\mathbb{Q}_{FT}/\mathbb{Q}(\mu_{p^n})\right) \;\cong\; \begin{pmatrix} U^{(n)} & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix}.$$

For each $n \geq 1$ let $\zeta_{p^n} \in \overline{\mathbb{Q}}$ be a p^n-th root of unity, chosen so that $\zeta_{p^n}^p = \zeta_{p^{n-1}}$ for all n. Then we may define a 1-dimensional representation

$$\chi_n \;:\; \mathrm{Gal}\left(\mathbb{Q}_{FT}/\mathbb{Q}(\mu_{p^n})\right) \longrightarrow \overline{\mathbb{Q}}^\times, \quad \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \longmapsto \zeta_{p^n}^b$$

and one can check that ρ_n is given by

$$\rho_n = \mathrm{Ind}_{\mathbb{Q}(\mu_{p^n})}^{\mathbb{Q}} \chi_n.$$

Writing ρ_0 for the trivial representation, every irreducible representation of G_{FT} has the form $\rho_n \otimes \psi$ for some $n \geq 0$, and some character

$$\psi : \mathrm{Gal}\left(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}\right) \longrightarrow \overline{\mathbb{Q}}^\times.$$

Bouganis and V. Dokchitser [BD07] have established an important algebraicity result for the representations of $\mathrm{Gal}(\mathbb{Q}_{FT}/\mathbb{Q})$. For any Artin representation ρ, we write $\mathbb{Q}(\rho)$ for the minimal field over which ρ can be realised.

Theorem 2.8.1. *(Bouganis, V. Dokchitser) If E is an elliptic curve over $\mathbb{Q}$ and ρ is an Artin representation which factors through $\mathbb{Q}_{FT}/\mathbb{Q}$, then Conjecture 2.3.2 holds for E and ρ. Further, we have*

$$\epsilon(\rho,0)^{-1}\, \frac{L(E,\rho,1)}{\Omega_E^{+\,d^+(\rho)}\, \Omega_E^{-\,d^-(\rho)}} \;\in\; \mathbb{Q}(\rho)$$

where $\epsilon(\rho,s)$ is the epsilon factor appearing in the functional equation of $L(\rho,s)$.

As part of a more general version of Conjecture 2.7.1, Coates et al predict the existence of an element

$$\mathcal{L}_{E/\mathbb{Q}_{\mathrm{FT}}} \in K_1\big(\Lambda(G_{FT})_{\mathcal{S}^*}\big)$$

which satisfies the same interpolation formula as $\mathcal{L}_E$ at all Artin representations of G_{FT} (except that we replace the set of primes R by the set $\{q \text{ prime} : q \text{ divides } p\Delta\}$).

2.9 Kato's Congruences

In his recent paper [Kat05], Kato proved that the existence of the p-adic L-function $\mathcal{L}_{E/\mathbb{Q}_{\mathrm{FT}}} \in K_1\big(\Lambda(G_{FT})_{\mathcal{S}^*}\big)$ is equivalent to a set of explicit congruences. In this section we review some of Kato's results, following the notation from [Kat05] where possible.

Kato's article covers the structure of the K_1-group $K_1(\mathbb{Z}_p[[G]])$ for any open subgroup G of

$$G_{FT} \;=\; \begin{pmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix}$$

but for simplicity we will only discuss his results in the case $G = G_{FT}$.

We recall the representation ρ_n from the previous section. Fixing an embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ we can extend scalars to $\overline{\mathbb{Q}}_p$ to obtain a representation

$$\rho_n \;:\; G \longrightarrow \mathrm{GL}_{\phi(p^n)}(\overline{\mathbb{Q}}_p)$$

which is induced from the character

$$\chi_n \;:\; \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \longmapsto \zeta_{p^n}^b .$$

For $n \geq 0$, we write $U^{(n)}$ for the subgroup of $\mathbb{Z}_p^\times$ given by

$$U^{(n)} \;=\; \ker\left(\mathbb{Z}_p^\times \twoheadrightarrow \left(\frac{\mathbb{Z}_p}{p^n\mathbb{Z}_p}\right)^\times\right).$$

We define another character $\tilde{\chi}_n$, taking values in $\mathbb{Z}_p[\zeta_{p^n}][[U^{(n)}]]$, by

$$\tilde{\chi}_n \;:\; \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \longmapsto \zeta_{p^n}^b \, \langle a \rangle \,,$$

where $a \mapsto \langle a \rangle$ denotes the canonical embedding of $\mathbb{Z}_p^\times$ into its group ring $\mathbb{Z}_p[\zeta_{p^n}][[\mathbb{Z}_p^\times]]$. Inducing $\tilde{\chi}_n$ to G yields a representation

$$\tilde{\rho}_n \;:\; G \longrightarrow \mathrm{GL}_{\phi(p^n)}\left(\mathbb{Z}_p[\zeta_{p^n}][[U^{(n)}]]\right).$$

It can be checked that $\tilde{\rho}_n$ induces a homomorphism

$$\Theta_{G,n} \ : \ K_1(\mathbb{Z}_p[[G]]) \longrightarrow \mathbb{Z}_p[[U^{(n)}]]$$

such that composing the canonical map $\mathbb{Z}_p[[G]]^\times \longrightarrow K_1(\mathbb{Z}_p[[G]])$ with $\Theta_{G,n}$ yields the map $f \mapsto \det\big(\tilde{\rho}_n(f)\big)$. Then we have a canonical map

$$\Theta_G \ := \ \prod_{n\geq 0} \Theta_{G,n} \ \ : \ \ K_1(\mathbb{Z}_p[[G]]) \ \longrightarrow \ \prod_{n\geq 0} \mathbb{Z}_p[[U^{(n)}]]^\times.$$

Kato's main result is a description of the image of Θ_G. Let us write

$$N_{i,j} \ : \ \mathbb{Z}_p[[U^{(i)}]]^\times \longrightarrow \mathbb{Z}_p[[U^{(j)}]]^\times$$

for the natural norm map, and

$$\phi \ : \ \mathbb{Z}_p[[\mathbb{Z}_p^\times]] \longrightarrow \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$$

for the ring homomorphism induced by the p-power map on $\mathbb{Z}_p^\times$. For an element

$$(a_n)_{n\geq 0} \ \in \ \prod_{n\geq 0} \mathbb{Z}_p[[U^{(n)}]]^\times$$

we set

$$b_n = \frac{a_n}{N_{0,n}(a_0)} \qquad \text{and} \qquad c_n = \frac{b_n}{\phi(b_{n-1})}$$

for all $n \geq 0$, and we have the following theorem from [Kat05].

Theorem 2.9.1. *(Kato) The image of the map Θ_G consists precisely of those*

$$(a_n)_{n\geq 0} \ \in \ \prod_{n\geq 0} \mathbb{Z}_p[[U^{(n)}]]^\times$$

which satisfy the congruence

$$\prod_{1\leq i\leq n} N_{i,n}(c_i)^{p^i} \ \equiv \ 1 \mod p^{2n}$$

for all $n \geq 1$.

Because of this connection to $K_1(\mathbb{Z}_p[[G]])$, we will sometimes refer to a congruence of the above form as a 'K_1-congruence'.

Remark 2.9.2. In [Kat05], Kato also proves a localised version of Theorem 2.9.1, which describes the image of an analogous map

$$\Theta_{G,\mathcal{S}^*} \ : \ K_1\big(\mathbb{Z}_p[[G]]_{\mathcal{S}^*}\big) \ \longrightarrow \ \prod_{n\geq 0} \mathrm{Quot}\left(\mathbb{Z}_p[[U^{(n)}]]\right)^{\times}.$$

Now we consider the elliptic curve E again. According to a general conjecture (see Coates and Perrin-Riou [CPR89]), for each $n \geq 1$ there exists a p-adic L-function

$$\mathcal{L}(E, \rho_n) \ \in \ \mathbb{Z}_p[[U^{(n)}]] \otimes \mathbb{Q}$$

with the following interpolation property: if $\psi : \mathbb{Z}_p^{\times} \to \overline{\mathbb{Q}}^{\times}$ is a character of finite order, then the image of $\mathcal{L}(E, \rho_n)$ under the ring homomorphism $\mathbb{Z}_p[[U^{(n)}]] \otimes \mathbb{Q} \to \overline{\mathbb{Q}}$ induced by ψ coincides with the complex L-value $L(E, \rho_n \otimes \psi, 1)$ up to certain simple factors (which are essentially the factors from Conjecture 2.7.1).

The conjectures of the non-abelian theory imply that the abelian p-adic L-functions $\mathcal{L}(E, \rho_n)$ for all $n \geq 0$ should arise from the single non-abelian p-adic L-function $\mathcal{L}_{E/\mathbb{Q}_{\mathrm{FT}}} \in K_1(\mathbb{Z}_p[[G]]_{\mathcal{S}^*})$. For example, let us consider a special case: when the p-primary part of $\mathrm{Sel}_{\mathbb{Q}_{FT}}(E)$ is trivial, conjecturally $\mathcal{L}(E, \rho_n) \in \mathbb{Z}_p[[U^{(n)}]]^{\times}$ and $\mathcal{L}_{E/\mathbb{Q}_{\mathrm{FT}}} \in K_1(\mathbb{Z}_p[[G]])$. Further, we should have

$$\Theta_G\big(\mathcal{L}_{E/\mathbb{Q}_{\mathrm{FT}}}\big) \ = \ \big(\mathcal{L}(E, \rho_n)\big)_{n\geq 0} \, ,$$

so the existence of $\mathcal{L}_{E/\mathbb{Q}_{\mathrm{FT}}} \in K_1(\mathbb{Z}_p[[G]])$ is equivalent to a set of congruences between the p-adic L-functions $\mathcal{L}(E, \rho_n)$.

To verify these congruences, it would suffice to check them for the special values $\psi\big(\mathcal{L}(E, \rho_n)\big)$ for all characters $\psi : \mathbb{Z}_p^{\times} \to \overline{\mathbb{Q}}^{\times}$ of finite order. That is, we must prove congruences between the twisted L-values $L(E, \rho_n \otimes \psi, 1)$ multiplied by the prescribed period and other factors. In the following chapters we will attempt to do this, by studying convolution L-series of Hilbert modular forms.

Chapter 3

Hilbert Modular Forms

In this chapter we review the definitions and basic properties of Hilbert modular forms. These adelic automorphic forms can be seen as a generalisation of classical modular forms; we will discuss Fourier expansions, Hecke operators, and the Petersson inner product in the Hilbert modular setting.

Our motivation for studying Hilbert modular forms is the following: when E is an elliptic curve over $\mathbb{Q}$ and ρ is an Artin representation factoring through the false Tate curve extension $\mathbb{Q}_{FT}/\mathbb{Q}$, the twisted L-function $L(E, \rho, s)$ can be written as the Rankin convolution $L(\mathbf{f}, \mathbf{g}, s)$ of two Hilbert modular forms defined over the totally real subfield of $\mathbb{Q}(\mu_{p^n})$.

Our discussion follows Chapter 4 of Panchishkin's book [Pan91]; a more detailed account is given in Shimura's article [Shi78].

3.1 Definitions of Hilbert modular forms

Let F be a totally real field. Throughout this section we write $d = [F : \mathbb{Q}]$, D_F for the discriminant of F and $\mathfrak{d}$ for the different of F. We consider the group $\mathrm{GL}_2(F)$, which may be regarded as the group $G_{\mathbb{Q}}$ of $\mathbb{Q}$-rational points on an algebraic subgroup G

of GL_{2d}.

We may identify the adelisation $G_{\mathbb{A}} = G(\mathbb{A})$ with the group

$$\mathrm{GL}_2(F_{\mathbb{A}}) \;\cong G_\infty \;\times G_{\widehat{\mathbb{Q}}},$$

where $G_\infty = \mathrm{GL}_2(F_\infty) \cong \mathrm{GL}_2(\mathbb{R})^d$, and $G_{\widehat{\mathbb{Q}}} = \mathrm{GL}_2(\widehat{F})$. Here $\widehat{F} = \mathcal{O}_F \otimes_{\mathbb{Z}} \widehat{\mathbb{Q}}$, and $\widehat{\mathbb{Q}} = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$. We write G_∞^+ for the identity component of G_∞, which is given by

$$G_\infty^+ \;\cong\; \mathrm{GL}_2^+(\mathbb{R})^d \;=\; \Big\{(\alpha_1, ..., \alpha_d) \in \mathrm{GL}_2(\mathbb{R})^d \;:\; \det \alpha_\nu > 0 \;\text{ for all } \nu\Big\}.$$

Let $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ denote the complex upper half-plane. The group G_∞^+ acts on $\mathcal{H}^d$ via

$$(\alpha_1, ..., \alpha_d) \;:\; (z_1, ..., z_d) \longmapsto (\alpha_1(z_1), ..., \alpha_d(z_d))$$

where each copy of $\mathrm{GL}_2(\mathbb{R})$ acts on $\mathcal{H}$ in the usual way:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \;:\; z \longmapsto \frac{az+b}{cz+d}\,.$$

Let f be a function $f : \mathcal{H}^d \longrightarrow \mathbb{C}$, and α an element of $\mathrm{GL}_2(\mathbb{R})$. For $k \in \mathbb{N}$ we define the weight k action of α on f by

$$\left(f\big|_k\alpha\right)(z) \;=\; \mathcal{N}(cz+d)^{-k}\,\mathcal{N}(\det\alpha)^{k/2}\,f(\alpha z)$$

where $\mathcal{N}(z) = z_1 ... z_d$.

Now we define our congruence subgroups in the Hilbert modular setting. Let $\mathfrak{c}$ be an integral ideal of $\mathcal{O}_F$, and $\mathfrak{p}$ a prime ideal. We write $\mathfrak{c}_\mathfrak{p} = \mathfrak{c}\mathcal{O}_\mathfrak{p}$ for the $\mathfrak{p}$-part of $\mathfrak{c}$, and $\mathfrak{d}_\mathfrak{p} = \mathfrak{d}\mathcal{O}_\mathfrak{p}$ for the local different at $\mathfrak{p}$. Then we define $W(\mathfrak{p}) \subset \mathrm{GL}_2(F_\mathfrak{p})$ by

$$W(\mathfrak{p}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F_\mathfrak{p}) : b \in \mathfrak{d}_\mathfrak{p}^{-1};\; c \in \mathfrak{d}_\mathfrak{p}\mathfrak{c}_\mathfrak{p};\; a, d \in \mathcal{O}_\mathfrak{p};\; ad - bc \in \mathcal{O}_\mathfrak{p}^\times \right\}$$

and $W = W_\mathfrak{c} \subset G_{\mathbb{A}}$ by

$$W \;=\; G_\infty^+ \;\times \prod_{\text{all } \mathfrak{p}} W(\mathfrak{p}).$$

If ψ is a Hecke character, we extend ψ to $W_{\mathfrak{c}}$ in the following way: let $\psi_0 : (\mathcal{O}_F/\mathfrak{c})^\times \longrightarrow \mathbb{C}^\times$ be the $\mathfrak{c}$-part of ψ, then set

$$\psi \ : \ W_{\mathfrak{c}} \longrightarrow \mathbb{C}^\times, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \psi_0(a_{\mathfrak{c}} \bmod \mathfrak{c})$$

where $a_{\mathfrak{c}}$ is the $\mathfrak{c}$-part of a.

Let us fix a positive integer k, an integral ideal $\mathfrak{c}$ and a Hecke character of finite order ψ. We now state five conditions on a function $\mathbf{f} : G_{\mathbb{A}} \longrightarrow \mathbb{C}$ that will be used to define a Hilbert modular form of parallel weight k, level $\mathfrak{c}$ and character ψ. We denote by ι the involution of $G_{\mathbb{A}}$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\iota = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Condition (Aut 1): If $\alpha \in G_{\mathbb{Q}}$ and $s \in F_{\mathbb{A}}^\times = \text{centre}(G_{\mathbb{A}})$, we have

$$\mathbf{f}(s\alpha x) \ = \ \psi(s)\, \mathbf{f}(x)$$

for all $x \in G_{\mathbb{A}}$.

Condition (Aut 2): If $w \in W_{\mathfrak{c}}$ with $w_\infty = 1$, we have

$$\mathbf{f}(xw) \ = \ \psi(w^\iota)\, \mathbf{f}(x)$$

for all $x \in G_{\mathbb{A}}$.

Condition (Aut 3): If we write $w(\theta) = (w_1(\theta_1), \ldots, w_d(\theta_d))$ with

$$w_\nu(\theta_\nu) \ = \ \begin{pmatrix} \cos\theta_\nu & -\sin\theta_\nu \\ \sin\theta_\nu & \cos\theta_\nu \end{pmatrix},$$

so that $w(\theta) \in \mathrm{SO}_2(\mathbb{R})^d$, we have

$$\mathbf{f}\big(xw(\theta)\big) \ = \ \mathbf{f}(x)\, \exp(-ik\{\theta\})$$

for all $x \in G_{\mathbb{A}}$, where $\{\theta\} = \theta_1 + \cdots + \theta_d$.

Condition (Hol): For any $x \in G_{\mathbb{A}}$ with $x_\infty = 1$ there exists a holomorphic function $g_x : \mathcal{H}^d \longrightarrow \mathbb{C}$ such that for all $y \in G_\infty^+$ we have

$$\mathbf{f}(xy) \;=\; \left(g_x\big|_k\, y\right)(\mathbf{i})$$

where $\mathbf{i} = (\sqrt{-1}, \ldots, \sqrt{-1}) \in \mathcal{H}^d$. If $F = \mathbb{Q}$ we also require g_x to be holomorphic at the cusps in the usual sense.

Condition (Cusp): For every $g \in G_{\mathbb{A}}$,

$$\int_{F_{\mathbb{A}}/F} \mathbf{f}\left(g \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\right) dt \;=\; 0.$$

Definition 3.1.1. *A Hilbert modular form of parallel weight $k \in \mathbb{N}$, level $\mathfrak{c} \lhd \mathcal{O}_F$ and Hecke character ψ is a function*

$$\mathbf{f} \;:\; G_{\mathbb{A}} \longrightarrow \mathbb{C}$$

satisfying the automorphy conditions **(Aut 1)**, **(Aut 2)** *and* **(Aut 3)** *and the holomorphy condition* **(Hol)**. *The complex vector space of all such forms is denoted by $\mathcal{M}_k(\mathfrak{c}, \psi)$.*

If $\mathbf{f}$ also satisfies the cuspidality condition **(Cusp)**, *we say that $\mathbf{f}$ is a Hilbert cusp form. We write $\mathcal{S}_k(\mathfrak{c}, \psi)$ for the subspace of cusp forms in $\mathcal{M}_k(\mathfrak{c}, \psi)$.*

Remark 3.1.2. In general, the weight k is in fact a vector $(k_1, \ldots, k_d) \in \mathbb{N}^d$, where $d = [F : \mathbb{Q}]$; the term 'parallel weight' refers to the special case in which all the k_j's are equal. In this thesis we will only use Hilbert modular forms of parallel weight, so we restrict our definition to these alone. We refer the reader to Shimura [Shi78] for the details of non-parallel weights.

The holomorphy condition allows us to describe $\mathbf{f} \in \mathcal{M}_k(\mathfrak{c}, \psi)$ more explicitly in terms of modular forms on $\mathcal{H}^d$. Let $h = \#\widetilde{\mathrm{Cl}}(F)$ be the narrow class number of F,

and choose ideles $t_1, ..., t_h \in F_{\mathbb{A}}^{\times}$ such that $\tilde{t}_\lambda \lhd \mathcal{O}_F$ (the ideals generated by the t_λ) are all prime to p, and form a complete set of representatives for $\widetilde{\mathrm{Cl}}(F)$.

Given $\mathbf{f} \in \mathcal{M}_k(\mathfrak{c}, \psi)$ we set $f_\lambda = g_{x_\lambda^{-\iota}}$ for $\lambda = 1, \ldots, h$, where

$$x_\lambda^{-\iota} \;=\; \begin{pmatrix} t_\lambda^{-1} & 0 \\ 0 & 1 \end{pmatrix} \in G_{\mathbb{A}}$$

and g_x is the function defined in the statement of **(Hol)**. One can check that f_λ is a modular form on $\mathcal{H}^d$; to be precise $f_\lambda(z) \in \mathcal{M}_k(\Gamma_\lambda(\mathfrak{c}), \psi_0)$ where the congruence subgroup $\Gamma_\lambda(\mathfrak{c}) \subset G_{\mathbb{Q}}^+$ is given by

$$\begin{aligned} \Gamma_\lambda(\mathfrak{c}) \;&:=\; x_\lambda \, W_{\mathfrak{c}} \, x_\lambda^{-1} \\ &=\; \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,:\, b \in \tilde{t}_\lambda^{-1} \mathfrak{d}_F^{-1};\; c \in \tilde{t}_\lambda \mathfrak{c}\, \mathfrak{d}_F;\; a, d \in \mathcal{O}_F,\; ad - bc \in \mathcal{O}_F^{\times} \right\}. \end{aligned}$$

We mean by this statement that

$$f_\lambda\big|_k \gamma \;=\; \psi(\gamma)\, f_\lambda$$

for all $\gamma \in \Gamma_\lambda(\mathfrak{c})$. It can be checked that the λ-component decomposition provides an isomorphism of vector spaces:

$$\begin{aligned} \mathcal{M}_k(\mathfrak{c}, \psi) \;&\xrightarrow{\sim}\; \bigoplus_{\lambda=1}^{h} \mathcal{M}_k\left(\Gamma_\lambda(\mathfrak{c}), \psi\right), \\ \mathbf{f} \;&\longmapsto\; (f_1, \ldots, f_h). \end{aligned}$$

3.2 Fourier Expansions

Let us write $\tau_1, ..., \tau_d$ for the embeddings $F \hookrightarrow \mathbb{R}$. We define the additive map

$$\mathbf{e}_F(\xi z) \;=\; \exp\left(2\pi i \sum_{a=1}^{d} \xi^{\tau_a} z_a \right)$$

where $z = (z_1, \ldots, z_d) \in \mathcal{H}^d$ and $\xi \in F$. Also, we will refer to an element $\xi \in F$ as *totally positive* if $\tau_a(\xi) > 0$ for $a = 1, \ldots, d$ (and we will sometimes denote this by writing $\xi \gg 0$).

If $\mathbf{f} \in \mathcal{M}_k(\mathfrak{c}, \psi)$, each component f_λ has a Fourier expansion of the form

$$f_\lambda(z) = \sum_\xi a_\lambda(\xi)\, \mathbf{e}_F(\xi z),$$

where the sum ranges over all totally positive $\xi \in \tilde{t}_\lambda$ and $\xi = 0$. If $\mathbf{f}$ is a cusp form, then $a_\lambda(0) = 0$ for $\lambda = 1, \ldots, h$.

Given any integral ideal $\mathfrak{m} \lhd \mathcal{O}_F$, we may write $\mathfrak{m} = \xi \tilde{t}_\lambda^{-1}$ for a unique λ, and some totally positive $\xi \in \tilde{t}_\lambda$. Then we define the coefficients $C(\mathfrak{m}, \mathbf{f})$ by

$$C(\mathfrak{m}, \mathbf{f}) = \begin{cases} a_\lambda(\xi)\, N_{F/\mathbb{Q}}(\tilde{t}_\lambda)^{-k/2} & \text{if the ideal } \mathfrak{m} = \xi \tilde{t}_\lambda^{-1} \text{ is integral;} \\ 0 & \text{if } \mathfrak{m} \text{ is not integral.} \end{cases}$$

We observe that $C(\mathfrak{m}, \mathbf{f})$ is well defined: if ξ and ξ' satisfy $\mathfrak{m} = \xi \tilde{t}_\lambda^{-1} = \xi' \tilde{t}_\lambda^{-1}$, we must have $\xi' = \xi\epsilon$ for a unit $\epsilon \in \mathcal{O}_F^\times$. The automorphy properties of f_λ imply that

$$f_\lambda(z) \;=\; N_{F/\mathbb{Q}}(\epsilon)^{k/2}\, f_\lambda(\epsilon z)$$

but $N_{F/\mathbb{Q}}(\epsilon) = 1$ since ϵ is a unit. Therefore $f_\lambda(z) = f_\lambda(\epsilon z)$ which implies $a_\lambda(\xi) = a_\lambda(\xi')$.

We have the Fourier expansion

$$\mathbf{f}\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}\right) \;=\; \sum_\zeta C(\zeta\tilde{y}, \mathbf{f})\, |y|^{k/2}\, \mathbf{e}_F(\zeta \mathbf{i} y_\infty)\, \mathbf{e}_F(\zeta x)$$

where the sum ranges over all totally positive $\zeta \in F$ and $\zeta = 0$. In this formula $\mathbf{e}_F$ denotes both the additive character

$$\begin{array}{rccl} \mathbf{e}_F \;:\; \mathbb{C}^d & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \exp\left(2\pi i \sum_{a=1}^{d} z_d\right) \end{array}$$

and the additive character of adeles $\mathbf{e}_F : F_{\mathbb{A}}/F \longmapsto \mathbb{C}$ which agrees with the above $\mathbf{e}_F$ on the infinite component.

3.3 Hecke Operators

We consider the semi-group $Y_{\mathfrak{c}} := G_{\mathbb{A}} \cap \Big(G_\infty^+ \times \prod_{\mathfrak{p}} Y_{\mathfrak{c}}(\mathfrak{p}) \Big)$, where for each prime ideal $\mathfrak{p}$ we have

$$Y_{\mathfrak{c}}(\mathfrak{p}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F_{\mathfrak{p}}) : a\mathcal{O}_{\mathfrak{p}} + \mathfrak{c}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}},\ b \in \mathfrak{d}_{\mathfrak{p}}^{-1}, c \in \mathfrak{c}_{\mathfrak{p}}\mathfrak{d}_{\mathfrak{p}},\ d \in \mathcal{O}_{\mathfrak{p}} \right\}.$$

The *Hecke algebra* $\mathbb{H}_{\mathfrak{c}}$ is defined to be the set of formal finite sums $\sum_y c_y W y W$ with $y \in Y_{\mathfrak{c}}$ and $c_y \in \mathbb{C}$, where W is as defined in Section 3.1. It is made into an algebra with the obvious addition, and the standard multiplication given by decomposition of double cosets into a union of left cosets (as in the classical case).

Let us define the action of $\mathbb{H}_{\mathfrak{c}}$ on $\mathcal{M}_k(\mathfrak{c}, \psi)$. For $y \in Y_{\mathfrak{c}}$, we decompose the double coset WyW into a disjoint union of right cosets:

$$WyW \ = \bigcup_j W y_j.$$

Then for $\mathbf{f} \in \mathcal{M}_k(\mathfrak{c}, \psi)$ we define a function $\mathbf{f}|WyW$ on $G_{\mathbb{A}}$ by

$$\big(\mathbf{f}\big|WyW\big)(x) \ = \ \sum_j \psi(y_j)\, \mathbf{f}(x\, y_j^\iota)$$

for all $x \in G_{\mathbb{A}}$, where ψ is extended to Y via setting

$$\psi \ : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ \longmapsto \ \psi_0(a_{\mathfrak{c}} \bmod \mathfrak{c}).$$

It is easy to confirm that $\mathbf{f}|WyW$ is also an element of $\mathcal{M}_k(\mathfrak{c}, \psi)$.

For an integral ideal $\mathfrak{m} \lhd \mathcal{O}_F$ we then define the *Hecke operator* $T_{\mathfrak{c}}(\mathfrak{m})$ to be the sum of all cosets WyW such that $y \in Y_{\mathfrak{c}}$ and $\widetilde{\det y} = \mathfrak{m}$. We then define the *normalised Hecke operator* $T'_{\mathfrak{c}}(\mathfrak{m})$ by

$$T'_{\mathfrak{c}}(\mathfrak{m}) \ := \ N_{F/\mathbb{Q}}(\mathfrak{m})^{(k-2)/2}\, T_{\mathfrak{c}}(\mathfrak{m}).$$

One easily checks the following formula which describes the action of $T'_{\mathfrak{c}}(\mathfrak{m})$ on the Fourier coefficients of $\mathbf{f}$:

$$C\big(\mathfrak{m},\, \mathbf{f}\big|T'_{\mathfrak{c}}(\mathfrak{n})\big) \ = \ \sum_{\mathfrak{a} \supset \mathfrak{m}+\mathfrak{n}} \psi(\mathfrak{a})\, N(\mathfrak{a})^{k-1}\, C(\mathfrak{a}^{-2}\mathfrak{m}\mathfrak{n}, \mathbf{f}).$$

Let be $\mathbf{f}$ a newform of level $\mathfrak{c}$; if $\mathbf{f}$ is a common eigenfunction of all the Hecke operators $T'_{\mathfrak{c}}(\mathfrak{m})$, and normalised by $C(\mathcal{O}_F, \mathbf{f}) = 1$, then we refer to $\mathbf{f}$ as *primitive of level* $\mathfrak{c}$.

3.4 Linear Operators on Hilbert modular forms

We will use certain linear operators on the space of Hilbert modular forms. Let $\mathfrak{q} \lhd \mathcal{O}_F$ be an integral ideal, and $q \in F_{\mathbb{A}}^{\times}$ an idele such that $\tilde{q} = \mathfrak{q}$. We define the operators $\mathfrak{q}$ and $U(\mathfrak{q})$ on $\mathbf{f} \in \mathcal{M}_k(\mathfrak{c}, \psi)$:

$$\begin{aligned} (\mathbf{f}|\mathfrak{q})(x) &= N_{F/\mathbb{Q}}(\mathfrak{q})^{-k/2}\, \mathbf{f}\left(x \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}\right) \\ \big(\mathbf{f}|U(\mathfrak{q})\big)(x) &= N_{F/\mathbb{Q}}(\mathfrak{q})^{k/2-1} \sum_{v \in \mathcal{O}_F/\mathfrak{q}} \mathbf{f}\left(x \begin{pmatrix} 1 & v \\ 0 & q \end{pmatrix}\right). \end{aligned}$$

These operators may also be described by their effect on the Fourier coefficients of $\mathbf{f}$, namely

$$C(\mathfrak{m}, \mathbf{f}\big|\mathfrak{q}) \;=\; C(\mathfrak{m}\mathfrak{q}^{-1}, \mathbf{f}) \qquad \text{and} \qquad C(\mathfrak{m}, \mathbf{f}|U(\mathfrak{q})) = C(\mathfrak{m}\mathfrak{q}, \mathbf{f}).$$

We will also need the involution $J_{\mathfrak{c}}$, which is defined by

$$(\mathbf{f}|J_{\mathfrak{c}})(x) \;=\; \psi(\det(x)^{-1})\, \mathbf{f}\left(x \begin{pmatrix} 0 & 1 \\ c_0 & 0 \end{pmatrix}\right)$$

where c_0 is an idele such that $\tilde{c}_0 = \mathfrak{c}\mathfrak{d}_F^2$. Then, if $\mathbf{f} \in \mathcal{M}_k(\mathfrak{c}, \psi)$, we have $\mathbf{f}|J_{\mathfrak{c}} \in \mathcal{M}_k(\mathfrak{c}, \psi^{-1})$. One also checks from the definition that

$$\mathbf{f}|J_{\mathfrak{m}\mathfrak{c}} \;=\; N_{F/\mathbb{Q}}(\mathfrak{m})^{k/2}\; \big(\mathbf{f}\big|J_{\mathfrak{c}}\big)\; \big|\mathfrak{m}.$$

Further, when $\mathbf{f}$ is a primitive form in $\mathcal{M}_k(\mathfrak{c}, \psi)$, we have

$$\mathbf{f}|J_{\mathfrak{c}} = \Lambda(\mathbf{f})\, \mathbf{f}^{\iota},$$

where the 'pseudo-eigenvalue' $\Lambda(\mathbf{f})$ is a root of unity, and $\mathbf{f}^{\iota} \in \mathcal{M}_k(\mathfrak{c}, \psi^{-1})$ is the Hilbert modular form defined by $C(\mathfrak{m}, \mathbf{f}^{\iota}) = \overline{C(\mathfrak{m}, \mathbf{f})}$.

3.5 The Petersson Inner Product

We use Panchishkin's normalisation of the Petersson inner product on Hilbert modular forms: for

$$\mathbf{f} = (f_1, \ldots, f_h) \in \mathcal{S}_k(\mathfrak{c}, \psi) \quad \text{and} \quad \mathbf{g} = (g_1, \ldots, g_h) \in \mathcal{M}_k(\mathfrak{c}, \psi)$$

this is defined to be

$$\langle \mathbf{f}, \mathbf{g} \rangle_{\mathfrak{c}} := \sum_{\lambda=1}^{h} \int_{\Gamma_\lambda(\mathfrak{c})\backslash \mathcal{H}^d} \overline{f_\lambda(z)} g_\lambda(z) N(y)^k d\mu(z)$$

where the measure μ is given by

$$d\mu(z) = \prod_{j=1}^{d} y_j^{-2} dx_j dy_j.$$

The normalised Hecke operators $T'_{\mathfrak{c}}(\mathfrak{m})$ are ψ-Hermitian with respect to the Petersson inner product: if

$$\mathbf{f} \,\big|\, T'_{\mathfrak{c}}(\mathfrak{m}) = \lambda(\mathfrak{m})\, \mathbf{f}$$

for all $\mathfrak{m}$ with $\mathfrak{m}$ prime to $\mathfrak{c}$, then $\lambda(\mathfrak{m}) = \psi(\mathfrak{m})\overline{\lambda(\mathfrak{m})}$ and

$$\psi(\mathfrak{m}) \left\langle \mathbf{f} \big| T'_{\mathfrak{c}}(\mathfrak{m}),\, \mathbf{g} \right\rangle = \left\langle \mathbf{f},\, \mathbf{g} \big| T'_{\mathfrak{c}}(\mathfrak{m}) \right\rangle.$$

3.6 The Trace Map

Let $\mathfrak{c}$ and $\mathfrak{c}'$ be ideals of $\mathcal{O}_F$ such that $\mathfrak{c}$ divides $\mathfrak{c}'$. Then we have the trace map

$$\mathrm{Tr}_{\mathfrak{c}}^{\mathfrak{c}'} : \mathcal{M}_2(\mathfrak{c}', \psi) \longrightarrow \mathcal{M}_2(\mathfrak{c}, \psi),$$

which is defined by

$$\left(\mathbf{g} \big| \mathrm{Tr}_{\mathfrak{c}}^{\mathfrak{c}'}\right)(x) = \sum_{v \in T} \mathbf{g}\left(x \begin{pmatrix} 1 & 0 \\ c\,v & 1 \end{pmatrix} \right).$$

where c is an idele such that $\tilde{c} = \mathfrak{c}$, and T is a set of coset representatives for $\mathcal{O}_F/\mathfrak{m}$ where $\mathfrak{c}' = \mathfrak{m}\mathfrak{c}$.

This map has the property

$$\langle \mathbf{f}, \mathbf{g} \rangle_{\mathfrak{c}'} \;=\; \left\langle \mathbf{f}, \mathbf{g} \middle| \mathrm{Tr}_{\mathfrak{c}}^{\mathfrak{c}'} \right\rangle_{\mathfrak{c}}$$

for any two Hilbert modular forms $\mathbf{g} \in \mathcal{M}_2(\mathfrak{c}', \psi),\ \mathbf{f} \in \mathcal{S}_2(\mathfrak{c}, \psi)$. Further, from [Pan91] equation (4.11) we have the following useful identity:

$$\mathbf{g} \big| \mathrm{Tr}_{\mathfrak{c}}^{\mathfrak{c}'} \;=\; \mathbf{g} \big| J_{\mathfrak{c}'} \circ U(\mathfrak{c}'\mathfrak{c}^{-1}) \circ J_{\mathfrak{c}}.$$

This arises from the definitions of the operators U and J, and the matrix identity

$$\begin{pmatrix} 1 & 0 \\ c\,v & 1 \end{pmatrix} = (cm)^{-1} \begin{pmatrix} 0 & 1 \\ c\,m & 0 \end{pmatrix} \begin{pmatrix} 1 & v \\ 0 & m \end{pmatrix} \begin{pmatrix} 0 & 1 \\ c & 0 \end{pmatrix}$$

which holds for any c, m and v.

3.7 Eisenstein Series

Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals of $\mathcal{O}_F$, and ω a Hecke character of finite order defined modulo an integral ideal $\mathfrak{c}(\omega)$. In Section 4 of [Pan91], Panchishkin defines a Hilbert Eisenstein series $K_m^q(s; \mathfrak{a}, \mathfrak{b}; \omega)$ of parallel weight m. We will only require the particular case $q = 0,\ m = 1$, and in this case the Eisenstein series has λ-components

$$\begin{aligned} K_1^0(s; \mathfrak{a}, \mathfrak{b}; \omega)_\lambda(z) \quad &= \quad N_{F/\mathbb{Q}}(\tilde{t}_\lambda)^{1/2}\, \mathcal{N}(y) \\ &\times \quad \sum_{c,d} \ \mathrm{sign}(N_{F/\mathbb{Q}}(d))\, \omega(d\mathcal{O}_F)\, \mathcal{N}(cz+d)^{-1} \left|\mathcal{N}(cz+d)\right|^{-2s} \end{aligned}$$

for $s > 1$. Here $N(z) = z_1 \ldots z_{[F:\mathbb{Q}]}$, and the sum is taken over the set of equivalence classes

$$(c, d) \in \frac{\tilde{t}_\lambda \mathfrak{d}\mathfrak{a} \times \mathfrak{b}}{\sim}$$

where the relation $\sim$ is defined by $(c, d) \sim (uc, ud)$ for all $u \in \mathcal{O}_F^\times$.

Remark 3.7.1. In general this Eisenstein series is a C^∞-Hilbert modular form. These are defined by replacing the holomorphy condition (**Hol**) from Section 3.1 by

an analogous condition where we demand that the functions g_x are C^∞ rather than holomorphic. To recover a holomorphic modular form, one can apply a holomorphic projection operator, as Panchishkin does in Section 4.6 of [Pan91]. However for our specific case, the Eisenstein series is already holomorphic and we avoid this step.

In the following chapter we will use the Eisenstein series $K_1^0(s; \mathfrak{c}, \mathcal{O}_F; \omega)$ for a particular integral ideal $\mathfrak{c}$. It is necessary to convert this to another Eisenstein series which has a user-friendly Fourier expansion; we can do this via the involution $J_\mathfrak{c}$. Using [Pan91] (4.6), one can show:

$$K_1^0(0; \mathfrak{c}, \mathcal{O}_F; \omega)\big|J_\mathfrak{c} \;=\; \frac{(4\pi i)^{[F:\mathbb{Q}]}}{D_F^{1/2}\, N_{F/\mathbb{Q}}(\mathfrak{c}\mathfrak{d}_F^2)^{1/2}}\, E_1(0,\, \omega).$$

Here E_1 is the Eisenstein series defined in (4.13) of [Pan91], with λ-components

$$E_1(0,\, \omega)_\lambda(z) = \frac{N_{F/\mathbb{Q}}(\tilde{t}_\lambda)^{-1/2} D_F^{1/2}}{(-4\pi i)^{[F:\mathbb{Q}]}} \sum_{c,d} \operatorname{sign}(N_{F/\mathbb{Q}}(c))\, \omega(c\,\mathcal{O}_F)\, N_{F/\mathbb{Q}}(cz+d)^{-1}$$

such that ω is an ideal character modulo $\mathfrak{c}$, and the sum ranges over

$$(c, d) \;\in\; \frac{\mathcal{O}_F \times \tilde{t}_\lambda^{-1}\mathfrak{d}_F^{-1}}{\sim}\,.$$

The Fourier expansion of each λ-component is computed in [Pan91] Prop 4.2:

$$E_1(0, \omega)_\lambda(z) \;=\; N_{F/\mathbb{Q}}(\tilde{t}_\lambda)^{-1/2} \sum_{0 \ll \xi \in \tilde{t}_\lambda} a_\lambda(\xi)\; \mathbf{e}_F(\xi z)$$

with

$$a_\lambda(\xi) \;=\; \sum_c \omega^{-1}(\tilde{c})\,,$$

where the sum ranges over all $c \in \mathcal{O}_F$ such that there is a decomposition $\tilde{\xi} = \tilde{b}\,\tilde{c}$ for some $b \in \tilde{t}_\lambda$.

3.8 L-series

Given a Hilbert modular form $\mathbf{f} \in \mathcal{M}_k(\mathfrak{c}, \psi)$ we may associate an L-series to $\mathbf{f}$ like so:

$$L(\mathbf{f}, s) \;:=\; \sum_\mathfrak{m} C(\mathfrak{m}, \mathbf{f})\, N_{F/\mathbb{Q}}(\mathfrak{m})^{-s}.$$

The series converges only when $s > (k+1)/2$, but may be continued to a holomorphic function on the entire complex plane.

Further, if $\mathbf{f} \in \mathcal{M}_k(\mathfrak{c}, \psi)$ is a common eigenfunction of all the Hecke operators, we have an Euler product formula for $L(\mathbf{f}, s)$. To be precise, suppose

$$\mathbf{f}\big|T'_{\mathfrak{c}}(\mathfrak{m}) \;=\; \lambda(\mathfrak{m})\,\mathbf{f}$$

for all $\mathfrak{m} \lhd \mathcal{O}_F$, which means $C(\mathfrak{m}, \mathbf{f}) = \lambda(\mathfrak{m})C(\mathcal{O}_F, \mathbf{f})$ for all $\mathfrak{m}$. If we normalise $\mathbf{f}$ by setting $C(\mathcal{O}_F, \mathbf{f}) = 1$, then

$$L(\mathbf{f}, s) \;\;=\;\; \sum_{\mathfrak{m}} \lambda(\mathfrak{m})\, N_{F/\mathbb{Q}}(\mathfrak{m})^{-s},$$

and we have the following Euler product:

$$L(\mathbf{f}, s) \;=\; \prod_{\mathfrak{p}} \Big(1 \;-\; \lambda(\mathfrak{p})\, N_{F/\mathbb{Q}}(\mathfrak{p})^{-s} \;+\; \psi(\mathfrak{p})\, N_{F/\mathbb{Q}}(\mathfrak{p})^{k-1-2s}\Big)^{-1}$$

where $\mathfrak{p}$ ranges over all prime ideals of $\mathcal{O}_F$.

3.9 Rankin Convolutions

Given two Hilbert modular forms $\mathbf{f} \in \mathcal{S}_k(\mathfrak{c}(\mathbf{f}), \psi)$ and $\mathbf{g} \in \mathcal{M}_l(\mathfrak{c}(\mathbf{g}), \omega)$ with $k > l \geq 1$, we can associate the Rankin convolution L-function $L(\mathbf{f}, \mathbf{g}, s)$ to them. The basic convolution L-series is defined as follows:

$$L(\mathbf{f}, \mathbf{g}, s) \;:=\; \sum_{\mathfrak{n}} C(\mathbf{f}, \mathfrak{n})\, C(\mathbf{g}, \mathfrak{n})\, N_{F/\mathbb{Q}}(\mathfrak{n})^{-s}$$

where the sum is taken over all integral ideals of $\mathcal{O}_F$.

Suppose now that $\mathbf{f}$ and $\mathbf{g}$ are Hecke eigenforms, so that their L-series admit Euler products. For each prime $\mathfrak{q}$ of F we may factorise the Hecke polynomials like so:

$$\begin{aligned} 1 - C(\mathfrak{q}, \mathbf{f})\, T + \psi(\mathfrak{q})\, T^2 &= \big(1 - \alpha(\mathfrak{q})\, T\big)\big(1 - \alpha'(\mathfrak{q})\, T\big) \\ 1 - C(\mathfrak{q}, \mathbf{g})\, T + \omega(\mathfrak{q})\, T^2 &= \big(1 - \beta(\mathfrak{q})\, T\big)\big(1 - \beta'(\mathfrak{q})\, T\big). \end{aligned}$$

Then the Rankin convolution has the following Euler product decomposition, given in Panchishkin [Pan91]:

$$\begin{aligned} & L_{\mathfrak{c}}(2s+2-k-l,\psi\omega)\ L(\mathbf{f},\mathbf{g},s) \\ = & \prod_{\mathfrak{q}} \left(1-\alpha(\mathfrak{q})\beta(\mathfrak{q})N_{F/\mathbb{Q}}(\mathfrak{q})^{-s}\right)^{-1}\left(1-\alpha'(\mathfrak{q})\beta(\mathfrak{q})N_{F/\mathbb{Q}}(\mathfrak{q})^{-s}\right)^{-1} \\ \times & \left(1-\alpha(\mathfrak{q})\beta'(\mathfrak{q})N_{F/\mathbb{Q}}(\mathfrak{q})^{-s}\right)^{-1}\left(1-\alpha'(\mathfrak{q})\beta'(\mathfrak{q})N_{F/\mathbb{Q}}(\mathfrak{q})^{-s}\right)^{-1} \end{aligned}$$

where $\mathfrak{c}=\mathfrak{c}(\mathbf{f})\mathfrak{c}(\mathbf{g})$ and

$$L_{\mathfrak{c}}(s,\psi\omega) \ = \sum_{\mathfrak{n}+\mathfrak{c}=\mathcal{O}_F} \psi(\mathfrak{n})\omega(\mathfrak{n})N_{F/\mathbb{Q}}(\mathfrak{n})^{-s}$$

is the standard Hecke L-function of $\psi\omega$ with the Euler factors at the primes dividing $\mathfrak{c}$ removed. Further, if we define a completion factor

$$\gamma_d(s) \ = \ (2\pi)^{-2ds}\,\Gamma(s)^d\,\Gamma(s+1-l)^d$$

then we have the completed Rankin convolution

$$\Psi(\mathbf{f},\mathbf{g},s) \ := \ \gamma_d(s)\,L_{\mathfrak{c}}(2s+2-k-l,\psi\omega)\,L(\mathbf{f},\mathbf{g},s).$$

Then $\Psi(\mathbf{f},\mathbf{g},s)$ admits a holomolphic continuation to the entire complex plane, and satisfies a certain functional equation (see Shimura [Shi78]). Further, it can be shown that the value

$$\frac{\Psi(l+r,\mathbf{f},\mathbf{g})}{(2\pi i)^{d(1-l)}\,\langle\mathbf{f},\mathbf{f}\rangle_{\mathfrak{c}(\mathbf{f})}}$$

is algebraic for all integers r with $0\le r\le k-l-1$ (see [Shi78] again).

3.10 Base Change

The theory of base change involves lifting cuspidal automorphic representations of GL_n from one field to another; but we will not discuss automorphic representations in this thesis at all, so we state only a simple version of base change for Hilbert modular forms.

Let F'/F be an abelian extension of totally real number fields, and $\mathbf{f} \in \mathcal{M}_k(\mathfrak{c}, \psi)$ a Hilbert modular form over F. Then there exists a Hilbert modular form $\mathbf{f}_{/F'} \in \mathcal{M}_k(\mathfrak{c}', \psi')$ over F' whose L-series satisfies

$$L(\mathbf{f}_{/F'}, s) \;=\; \prod_{\eta \in \widehat{G}} L(\mathbf{f}, \eta, s)$$

where $\widehat{G}$ denotes the character group of $G = \mathrm{Gal}(F'/F)$. We refer to $\mathbf{f}_{/F'}$ as the base change of $\mathbf{f}$ to the field F'. Its existence is established in Langlands [Lan80].

In particular, consider an elliptic curve E over $\mathbb{Q}$ and its associated newform $f_E \in S_2^{\mathrm{new}}(\Gamma_0(N_E))$ which has the property

$$L(f_E, s) \;=\; L(E, s).$$

Then if F is an abelian totally real number field, there exists a Hilbert modular form $\mathbf{f}_E \in \mathcal{S}_2(\mathfrak{c}(\mathbf{f}_E), \mathbf{1})$ which is the base change of f_E to F, whose L-series satisfies

$$L(\mathbf{f}_E, s) \;=\; \prod_{\psi \in \widehat{\mathrm{Gal}}(F/\mathbb{Q})} L(E, \psi, s) \;=\; L(E/F, s).$$

3.11 Hilbert Modular Forms from Induced Representations

Let F be a totally real field as before, and K/F a totally imaginary quadratic extension. We introduce the following notation: for a finite-order character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathbb{C}^\times$, we write $\chi^\dagger : \mathcal{I}_F \to \mathbb{C}^\times$ for the character of ideals obtained by composing χ with the reciprocity map of class field theory. Specifically, $\chi^\dagger$ is normalised by

$$\chi^\dagger(\mathfrak{q}) \;=\; \chi(\mathrm{Frob}_{\mathfrak{q}}^{-1})$$

for almost all primes $\mathfrak{q}$ of F, where $\mathrm{Frob}_{\mathfrak{q}}$ denotes an arithmetic Frobenius element at $\mathfrak{q}$.

We have the following theorem due to Serre:

Theorem 3.11.1. *If ρ is an Artin representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ which is induced from a 1-dimensional representation χ_ρ of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, then there exists a Hilbert modular form $\mathbf{g}_\rho$ over F such that $\mathbf{g}_\rho \in \mathcal{S}_1(\mathfrak{c}(\mathbf{g}_\rho), (\det\rho)^\dagger)$ and*

$$L(\mathbf{g}_\rho, s) = L(\rho, s).$$

Further, $\mathbf{g}_\rho$ is primitive if and only if χ_ρ is a primitive character.

Comparing the L-series coefficients of $L(\mathbf{g}_\rho, s)$ and $L(\rho, s)$, the theorem implies that the Fourier coefficients of $\mathbf{g}_\rho$ are given by

$$C(\mathfrak{m}, \mathbf{g}_\rho) \;=\; \sum_{\substack{\mathfrak{a} \lhd \mathcal{O}_K, \\ \mathfrak{a}\bar{\mathfrak{a}} = \mathfrak{m}}} \chi_\rho^\dagger(\mathfrak{a}).$$

The character $(\det\rho)^\dagger$ can be written as

$$(\det\rho)^\dagger(\mathfrak{a}) \;=\; \theta_{K/F}\,(\mathfrak{a})\;\chi_\rho^\dagger(\mathfrak{a}\mathcal{O}_K)$$

where $\theta_{K/F}$ is the quadratic character of K/F, given on primes of $\mathcal{O}_F$ by

$$\theta_{K/F}(\mathfrak{q}) = \begin{cases} 1 & \text{if } \mathfrak{q} \text{ splits in } K/F \\ -1 & \text{if } \mathfrak{q} \text{ is inert in } K/F \\ 0 & \text{if } \mathfrak{q} \text{ ramifies in } K/F. \end{cases}$$

3.12 Hilbert Modular Forms from the False Tate Curve Extension

As in the previous chapter, we consider the false Tate curve extension of $\mathbb{Q}$: we write

$$\mathbb{Q}_{FT} \;=\; \bigcup_{n\geq 0} \mathbb{Q}(\mu_{p^n},\, \sqrt[p^n]{\Delta})$$

and $G_{FT} = \mathrm{Gal}(\mathbb{Q}_{FT}/\mathbb{Q})$. Recall that G_{FT} has a unique self-dual Artin representation of dimension $\phi(p^n)$ for each $n \geq 0$, which is induced from a character χ_n

over the field $K_n = \mathbb{Q}(\mu_{p^n})$. Setting $F_n = K_n^+$, we define a 2-dimensional Artin representation ρ_n over F_n by

$$\rho_n \;:=\; \mathrm{Ind}_{K_n}^{F_n} \chi_n.$$

Then, by Theorem 3.11.1 there exists a Hilbert modular form $\mathbf{g}_{\rho_k}$ lying in $\mathcal{M}_1(\mathfrak{c}(\mathbf{g}_{\rho_k}), (\det \rho_k)^\dagger)$ which satisfies $L(\mathbf{g}_{\rho_k}, s) = L(\rho_k, s)$.

For any $n \geq k$, we have an abelian extension F_n/F_k, so we may consider the base change $\mathbf{g}_{\rho_k/F_n}$ of $\mathbf{g}_{\rho_k}$ to F_n. The following lemma shows that this Hilbert modular form is also associated to an induced representation.

Lemma 3.12.1. *If* $\rho_k = \mathrm{Ind}_{K_k}^{F_k}(\chi_{\rho_k})$, *then*

$$\begin{aligned} L(\mathbf{g}_{\rho_k/F_n}, s) &= L(\mathrm{Res}_{F_n} \rho_k, s) \\ &= L\big(\mathrm{Ind}_{K_n}^{F_n}(\mathrm{Res}_{K_n} \chi_{\rho_k}), s\big), \end{aligned}$$

where $\mathrm{Res}_{K_n} \chi_{\rho_k}$ *denotes the restriction of* χ_{ρ_k} *from* $\mathrm{Gal}(\overline{\mathbb{Q}}/K_k)$ *to* $\mathrm{Gal}(\overline{\mathbb{Q}}/K_n)$.

Proof. Firstly, by our definition of the base change

$$L(\mathbf{g}_{\rho_k/F_n}, s) \;=\; \prod_{\psi \in \hat{G}} L(\rho_k \otimes \psi, s) \;=\; L(\rho_k \otimes \mathrm{Reg}_{F_n/F_k}, s)$$

where $G = \mathrm{Gal}(F_n/F_k)$, and $\mathrm{Reg}_{F_n/F_k} = \mathrm{Ind}_{F_n}^{F_k} \mathbf{1}$ denotes its regular representation. However, the Artin formalism implies

$$L(\rho/M, s) = L(\mathrm{Ind}\, \rho/L, s)$$

whenever ρ is an Artin representation over M, and L is a subfield of M. Therefore

$$L(\rho_k \otimes \mathrm{Reg}_{F_n/F_k}, s) \;=\; L(\rho_k \otimes \mathrm{Ind}_{F_n}^{F_k} \mathbf{1}, s) \;=\; L(\mathrm{Res}_{F_n} \rho_k \otimes \mathbf{1}, s)$$

and the result follows because $\mathrm{Res}_{F_n} \rho_k = \mathrm{Ind}_{K_n}^{F_n}(\mathrm{Res}_{K_n} \chi_{\rho_k})$. □

In a slight abuse of notation, we will write ρ_k/F_n as shorthand for the Artin representation $\mathrm{Res}_{F_n} \rho_k = \mathrm{Ind}_{K_n}^{F_n}(\mathrm{Res}_{K_n} \chi_{\rho_k})$. This emphasises the connection with the base change of $\mathbf{g}_{\rho_k}$.

Now let E be an elliptic curve over $\mathbb{Q}$, and f_E its associated cusp form. We write $\mathbf{f}_E$ for the base change of f_E to F_n, and compare the Rankin convolution

$$L_{\mathfrak{c}}(\det \rho_k/F_n, 2s-1)\ L(\mathbf{f}_E, \mathbf{g}_{\rho_k/F_n}, s)$$

with the twisted L-function $L(E, \rho_k/F_n, s)$. Considering the Euler products of both, it is clear they agree at each factor except possibly at the bad primes. In fact, Dokchitser and Bouganis state in [BD07] that the Euler factors can only differ at primes at which both $H^1_l(E)$ and ρ_k/F_n are ramified. Therefore, if we assume that $(N_E, p\Delta) = 1$ we have the equality

$$L_{\mathfrak{c}}(\det \rho_k/F_n, 2s-1)\ L(\mathbf{f}_E, \mathbf{g}_{\rho_k/F_n}, s)\ =\ L(E, \rho_k/F_n, s)$$

Therefore, we can study the twisted L-functions of E using results on Rankin convolutions of Hilbert modular forms.

Chapter 4

Non-abelian Congruences

In this chapter we will prove a set of K_1-congruences for the abelian p-adic L-functions $\mathcal{L}_p(E, \rho_i)$, for Artin representations ρ_i factoring through a false Tate curve extension of $\mathbb{Q}$. Unfortunately, our congruences are not strong enough to prove the existence of the non-abelian p-adic L-function $\mathcal{L}_{E/\mathbb{Q}_{FT}}$.

The main reference for this chapter is the book [Pan91], in which Panchishkin constructs an algebraic-valued measure associated to the Rankin convolution $L(\mathbf{f}, \mathbf{g}, s)$ of two Hilbert modular forms. However, Panchishkin's results require the assumption that p and $\mathfrak{c}(\mathbf{g})$ are coprime, and additionally that $C(\mathfrak{c}(\mathbf{g}), \mathbf{g}) \neq 0$. Neither of these conditions holds when $\mathbf{g} = \mathbf{g}_{\rho_n}$, so we must give the construction of the measure again in our case. Our results hold provided the elliptic curve E is semistable, and are subject to two technical hypotheses.

The material in this chapter is joint work with my PhD supervisor, Daniel Delbourgo; a version of it appears in [DW08]. We thank Vladimir Dokchitser and Thanasis Bouganis for their very helpful comments, and in particular thank Vladimir for the argument which proves Claim $(\star)$ in Section 4.6.

4.1 Main Results

Throughout we fix an odd prime p. Let $\Delta > 1$ denote a p-power free integer. We suppose that Δ is coprime to p, which ensures all the primes above Δ are tamely ramified in the false Tate curve tower.

Recall the false Tate curve extension:

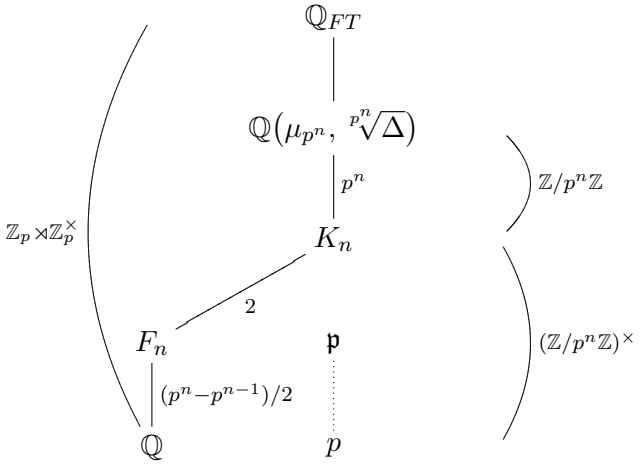
$$\mathbb{Q}_{FT} = \bigcup_{n \geq 1} \mathbb{Q}\big(\mu_{p^n},\, \sqrt[p^n]{\Delta}\big).$$

Basic Galois theory informs us that

$$\mathrm{Gal}(\mathbb{Q}_{FT}/\mathbb{Q}) \;\cong\; \begin{pmatrix} \mathbb{Z}_p^{\times} & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix} \lhd\; \mathrm{GL}_2(\mathbb{Z}_p).$$

In other words, the Galois group is a semi-direct product of two p-adic Lie groups of dimension one.

Throughout this chapter we use the following notation: for each integer $n \geq 0$, we set $K_n = \mathbb{Q}(\mu_{p^n})$ and write $F_n = \mathbb{Q}(\mu_{p^n})^+$ for the maximal real subfield. When the value of n is clear, we simply write $\mathfrak{p}$ for the unique prime of F_n above p. In terms of a field diagram,



In this situation the representation theory is very well understood. It is proved in [Dok05] that $\mathrm{Gal}(\mathbb{Q}_{FT}/\mathbb{Q})$ has a unique self-dual representation of dimension

$p^k - p^{k-1}$, which we denote by $\rho_{k,\mathbb{Q}}$ for each $k \geq 1$. This may be written

$$\rho_{k,\mathbb{Q}} \;=\; \mathrm{Ind}_{K_k}^{\mathbb{Q}}\, \chi_{\rho_k}$$

for a character χ_{ρ_k} of $\mathrm{Gal}(\mathbb{Q}_{FT}/K_k)$. Putting $\rho_{0,\mathbb{Q}} = \mathbf{1}$, every irreducible representation of $\mathrm{Gal}(\mathbb{Q}_{FT}/\mathbb{Q})$ has the form $\rho_{k,\mathbb{Q}} \otimes \psi$ for some $k \geq 0$, and some character

$$\psi : \mathrm{Gal}\left(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}\right) \longrightarrow \mathbb{C}^\times.$$

For the rest of this section, we set $G = \mathrm{Gal}(\mathbb{Q}_{FT}/\mathbb{Q})$.

Let E be an elliptic curve over $\mathbb{Q}$. As part of the general GL_2 main conjecture, Coates et al [CFK$^+$05] predict the existence of a non-abelian p-adic L-function

$$\mathcal{L}_{E/\mathbb{Q}_{FT}} \in K_1(\mathbb{Z}_p[[G]]_{\mathcal{S}^*})$$

whose evaluation at an Artin representation $\rho : G \longrightarrow \mathrm{GL}(V)$ yields essentially the ρ-twisted L-value $L(E, \rho, 1)$. Here $\mathbb{Z}_p[[G]]_{\mathcal{S}^*}$ is the localisation of $\mathbb{Z}_p[[G]]$ at a certain Ore set $\mathcal{S}^* = \bigcup_{n\geq 0} p^n \mathcal{S}$.

We always assume that E has good ordinary reduction at p, and that Δ and N_E are coprime. We also assume that E is semistable (otherwise our distributions turn out to be identically zero).

Wiles et al have shown that all elliptic curves over $\mathbb{Q}$ are modular, so we may write f_E for the newform of weight two and conductor N_E associated to E. In order to state our full results, we are forced to impose two other hypotheses.

Hypothesis (I, n) For each integer $0 \leq j \leq n$, the Conjecture IV of Stevens [Ste89] §4 holds at all $\rho_j \otimes \psi$-twists of the f_E-isotypic component in $H_1\big(X_1(N_E), \mathbb{Z}\big)$.

Hypothesis (II) The $(p-1)$ branches of the Mazur-Tate-Teitelbaum p-adic L-function of $E/\mathbb{Q}$ each have a trivial μ-invariant.

Condition **(I, n)** implies that the p-adic L-functions $\mathcal{L}_p(E, \rho_0)$, $\mathcal{L}_p(E, \rho_1), \ldots$ $\mathcal{L}_p(E, \rho_n)$

(defined in Theorem 4.1.1 below) take p-integral values. Although we are unable to verify it for any elliptic curves, it is expected to hold quite generally; for instance, if the ρ_j-twisted main conjectures hold for $j \in \{0, \ldots, n\}$, every $\mathcal{L}_p(E, \rho_j)$ is the characteristic power series of a corresponding Selmer group, and Hypothesis **(I,** n**)** follows.

The Mazur-Tate-Teitelbaum p-adic L-function mentioned in condition **(II)** essentially interpolates the value $L(E, \chi, 1)$ at each finite order character $\chi : \mathbb{Z}_p^\times \to \mathbb{C}_p^\times$ (details are given in [MTT86]). Hypothesis **(II)** implies that the norm of $\mathcal{L}_p(E, \rho_0)$ has μ-invariant equal to zero, which ensures that the congruences we prove are non-trivial. This condition is conjectured to hold true for all E and p, and one may be able to verify it numerically by computing the L-values $L(E, \omega^i, 1)$ for each branch ω^i. We have done this for a specific example in Section 4.7.

The first of our main results is an integral version of a theorem of Shai Haran from [Har87], concerning the existence of abelian p-adic L-functions which are attached to the special values $L(E, \rho_n \otimes \psi, 1)$. To be precise, these are p-adic L-functions associated to the motives $h^1(E) \otimes_{\mathbb{Z}} M(\rho_n)$; but we will not discuss motives at all in this thesis.

Theorem 4.1.1. *Let* $\mathfrak{p}$ *denote the unique prime of* F_n *above* p*, and let* $\mathbf{f}$ *denote the base change of* f_E *to the field* F_n*. We define the automorphic period*

$$\Omega^{\mathrm{aut}}_{E/F_n} \;:=\; (2\pi)^{\phi(p^n)} \left\langle \mathbf{f}_{/F_n}, \mathbf{f}_{/F_n} \right\rangle_{\mathfrak{c}(\mathbf{f})}.$$

If there is no non-trivial congruence modulo $\mathfrak{p}$ *between* $\mathbf{f}$ *and another modular form in* $\mathcal{M}_2(\mathfrak{c}(\mathbf{f}))$*, then there exists a unique element* $\mathcal{L}_p^{\mathrm{aut}}(E, \rho_n)$ *of* $\mathbb{Z}_p[[U^{(n)}]]$ *such that*

$$\begin{aligned} \psi\Big(\mathcal{L}_p^{\mathrm{aut}}(E, \rho_n)\Big) \;&=\; \frac{\epsilon_{F_n,\mathfrak{p}}(\rho_n \otimes \psi)}{\alpha_p^{f(\rho_n \otimes \psi, \mathfrak{p})}} \;\times\; \frac{P_{\mathfrak{p}}\big(\rho_n \otimes \psi, \alpha_p^{-[F_n:\mathbb{Q}]}\big)}{P_{\mathfrak{p}}\big(\rho_n \otimes \psi^{-1}, \alpha_p'^{-[F_n:\mathbb{Q}]}\big)} \\ &\times\; \frac{L_S(E, \rho_n \otimes \psi^{-1}, 1)}{\Omega^{\mathrm{aut}}_{E/F_n}} \end{aligned}$$

for all finite characters ψ *of* $U^{(n)}$*.*

Here, $P_{\mathfrak{p}}(\rho, T)$ is the local polynomial of ρ at $\mathfrak{p}$, and α_p denotes the p-adic unit root of

$$1 - a_p(E)T + pT^2$$

with α_p' being the non-unit root. Also, S denotes the set of primes of F_n which divide $p\Delta$, and $\epsilon_{F_{n,\mathfrak{p}}}(\rho_n \otimes \psi)$ denotes the local ϵ-factor at $\mathfrak{p}$. This ϵ-factor depends on the choice of a local Haar measure and an additive character at p (see [Tat79] for details). Over $\mathbb{Q}$, we follow [CFK$^+$05] and choose the Haar measure dx which gives $\mathbb{Z}_p$ measure 1, and the additive character $\tau : (\mathbb{Q}_p, +) \to \mathbb{C}^\times$ given by $\tau(ap^{-m}) = \exp(-2\pi ia/p^m)$ with $a \in \mathbb{Z}_p$.

Recall from Chapter 2 that Kato's paper [Kat05] reduces the existence of $\mathcal{L}_{E/\mathbb{Q}_{FT}}$ to a set of congruences. We put $a_n = \mathcal{L}_p(E, \rho_n)$, and consider both

$$b_n = a_n / N_{0,n}(a_0) \quad \text{and} \quad c_n = b_n / \phi(b_{n-1}).$$

As in Chapter 2,

$$N_{i,j} : \mathbb{Z}_p[[U^{(i)}]]^\times \longrightarrow \mathbb{Z}_p[[U^{(j)}]]^\times$$

denotes the homomorphism induced by the norm map, and

$$\phi : \mathbb{Z}_p[[\mathbb{Z}_p^\times]] \longrightarrow \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$$

is the ring homomorphism induced by the p-power map on $\mathbb{Z}_p^\times$. Kato's calculations of the image of K_1 predict that

$$\prod_{i=1}^{n} N_{i,n}(c_i)^{p^i} \equiv 1 \mod p^{2n}.$$

Theorem 4.1.2. *Assume that both Hypotheses* **(I,n)** *and* **(II)** *are satisfied. Then the non-abelian congruences*

$$\prod_{i=1}^{n} N_{i,n}(c_i)^{p^i} \equiv 1 \mod p^{n+1}$$

hold true.

When $n > 1$ these congruences are conjecturally not the best possible. For example, if $n = 2$ we expect a congruence modulo p^4 not p^3, if $n = 3$ we expect one modulo p^6 not p^4, and so on. However when $n = 1$, we have proved the congruences found numerically by Tim and Vladimir Dokchitser in [DD07].

Theorem 4.1.3. *Under the same hypotheses, the congruences computed in* [DD07] *always hold, i.e.*

$$a_1 \equiv N_{0,1}(a_0) \mod p.$$

Remark 4.1.4. Theorem 4.1.3 was proved in the case $p = 3$ by A. Bouganis in [Bou05], using properties of the 3-adic Eisenstein measure. Likewise, Bouganis had a non-integral version of Theorem 4.1.1.

Remark 4.1.5. When proving these results, we encounter a period ratio

$$\frac{(2\pi)^{\phi(p^n)} \left\langle \mathbf{f}_{/F_n}, \mathbf{f}_{/F_n} \right\rangle_{\mathfrak{c}(\mathbf{f})}}{(\Omega_E^+ \Omega_E^-)^{\phi(p^n)/2}} \in \overline{\mathbb{Q}}$$

which measures the discrepancy between the motivic p-adic L-function associated to $E \otimes \rho_n$, and its automorphic counterpart. When we submitted our article [DW08], we believed that the conjectures of Doi, Hida and Ishii from [DHI98] imply that this ratio is a p-adic unit. We have since realised that this is possibly not true; however this is not a problem, if one accepts Conjecture IV of Stevens [Ste89], which implies that the p-adic L-functions $\mathcal{L}_p(E, \rho_i)$ are all p-integral.

Remark 4.1.6. In [Kat05], Kato formulates a more general set of congruences for the case in which the Iwasawa algebra is localised (see Remark 2.9.2). We are confident that the method we use to prove Theorem 4.1.2 could be adapted to prove similar weakened versions of these congruences, provided Hypotheses **(I,** n**)** and **(II)** hold.

4.2 Integrality of Special Values

Let $\rho_k := \mathrm{Ind}_{K_k}^{F_k} \chi_{\rho_k}$ denote the two-dimensional Artin representation of $\mathrm{Gal}(\mathbb{Q}_{FT}/F_k)$, and write $\rho_k/F_n := \mathrm{Res}_{F_n} \rho_k$ for its restriction to $\mathrm{Gal}(\mathbb{Q}_{FT}/F_n)$. As before, we consider the finite set of primes

$$S = \{v \ : \ v \text{ is a prime of } F_n, \ \ v|p\Delta\}\,.$$

Our first goal in this chapter is to show that for every integer $n \geq k$, there exists a $\overline{\mathbb{Q}}$-valued distribution interpolating

$$\text{simple factors} \ \times \ \frac{L_S(E, \rho_k/F_n \otimes \psi^{-1}, 1)}{\text{a period}}$$

for a suitable family of Hecke characters ψ (see Theorem 4.5.2 for the precise statement). To do this, we will study the value at $s = 1$ of the completed Rankin-Selberg product

$$\Psi(\mathbf{f}, \mathbf{g}_\rho, s) \ = \ \left(\frac{\Gamma(s)}{(2\pi)^s}\right)^{2[F:\mathbb{Q}]} \ L_{\mathfrak{c}}(2s-1, (\det \rho)^\dagger)\, L(\mathbf{f}, \mathbf{g}_\rho, s)$$

where $\mathfrak{c} = \mathfrak{c}(\mathbf{f})\mathfrak{c}(\mathbf{g}_\rho)$, and

$$L(\mathbf{f}, \mathbf{g}_\rho, s) \ = \ \sum_{\mathfrak{a}} C(\mathfrak{a}, \mathbf{f})\, C(\mathfrak{a}, \mathbf{g}_\rho)\, N_{F/\mathbb{Q}}(\mathfrak{a})^{-s}.$$

In this section, our aim is to prove the following integrality result.

Theorem 4.2.1. *Let $F = F_n$ and let ρ be an Artin representation over F_n induced from a character over K_n. Let $\mathbf{g} = \mathbf{g}_\rho$, and let $\mathbf{f} \in \mathcal{M}_2(\mathfrak{c}(\mathbf{f}))$ be a Hilbert modular form with p-integral Fourier coefficients and level $\mathfrak{c}(\mathbf{f})$ prime to $\mathfrak{c}(\mathbf{g})$.*

Let $\mathfrak{p}$ denote the unique prime of F above p. If there exists no non-trivial congruence modulo $\mathfrak{p}$ between $\mathbf{f}$ and another modular form in $\mathcal{M}_2(\mathfrak{c}(\mathbf{f}))$, then the algebraic number

$$\epsilon_F(\rho) \cdot \frac{\Psi(\mathbf{f}, \mathbf{g}^\iota, 1)}{\langle \mathbf{f}, \mathbf{f} \rangle_{\mathfrak{c}(\mathbf{f})}}$$

is p-integral, where we write $\epsilon_F(\rho) = \epsilon_F(\rho, 0)$.

Remark 4.2.2. In our paper [DW08], we required Theorem 4.2.1 to prove the integrality of the motivic p-adic L-function $\mathcal{L}_p(E, \rho_n)$. Now that we assume Hypothesis **(I,n)**, we do not actually need it. However, we still include the result to show explicitly the connection between the integrality of the automorphic p-adic L-values, and congruence properties of the Hilbert modular form $\mathbf{f}$. One can compare this to the appearance of the congruence module $\mathbf{H}_\lambda(\mathcal{P})$ in Chapter 5, in the integrality statement for Hida's p-adic L-function.

The proof of Theorem 4.2.1 is given at the end of this section; let us first consider the epsilon factor $\epsilon_F(\rho, s)$. The Artin L-function $L(\rho, s)$ is known to obey the functional equation

$$\Gamma_\infty(s)\, L(\rho, s) \;=\; \epsilon_F(\rho, s)\, \Gamma_\infty(1-s)\, L(\rho^\vee, 1-s)$$

where $\rho^\vee$ is the contragredient representation, and $\Gamma_\infty(s) := ((2\pi)^{-s}\Gamma(s))^{[F:\mathbb{Q}]}$. The global ϵ-factor at zero may be decomposed into an infinite product

$$\epsilon_F(0, \rho) \;=\; \prod_{\text{all places } v} \epsilon_{F_v}(\rho_v, \tau_v, dx_v).$$

Each local factor depends on the normalisation of additive characters τ_v of F_v, and Haar measures dx_v, however the product does not (see Tate [Tat79] for a summary of local ϵ-factors).

Lemma 4.2.3. *Setting $\epsilon_F(\rho) = \epsilon_F(\rho, 0)$, we have*

$$\Lambda(\mathbf{g}_\rho) \;=\; i^{-[F:\mathbb{Q}]}\, N_{F/\mathbb{Q}}(\mathfrak{c}\mathfrak{d}_F^2)^{-1/2}\, \epsilon_F(\rho).$$

Proof. Following Shimura in [Shi78], we define

$$R(\mathbf{g}, s) := N_{F/\mathbb{Q}}(\mathfrak{c}\mathfrak{d}_F^2)^{s/2}\Gamma_\infty(s)L(\mathbf{g}, s)$$

where $\mathbf{g}$ is a Hilbert modular form of parallel weight 1 and conductor $\mathfrak{c}$. Then from [Shi78] (2.48) there is a functional equation

$$R(\mathbf{g}, s) = i^{[F:\mathbb{Q}]} R(\mathbf{g}|J_\mathfrak{c}, 1-s).$$

Supposing $\mathbf{g}$ is primitive, we have $\mathbf{g}|J_{\mathfrak{c}} = \Lambda(\mathbf{g})\mathbf{g}^{\iota}$, so the functional equation becomes

$$R(\mathbf{g}, s) = i^{[F:\mathbb{Q}]}\Lambda(\mathbf{g})R(\mathbf{g}^{\iota}, 1-s).$$

However, taking $\mathbf{g} = \mathbf{g}_{\rho}$ we have $L(\rho, s) = L(\mathbf{g}, s)$ and $L(\rho^{\vee}, s) = L(\mathbf{g}^{\iota}, s)$. Therefore

$$\Gamma_{\infty}(s)L(\rho, s) = \epsilon_F(\rho, s)\Gamma_{\infty}(1-s)L(\rho^{\vee}, 1-s)$$

can be rewritten as

$$R(\mathbf{g}, s) = \epsilon_F(\rho, s)N_{F/\mathbb{Q}}(\mathfrak{c}\mathfrak{d}_F^2)^{s-1/2}R(\mathbf{g}^{\iota}, 1-s).$$

Substituting $R(\mathbf{g}, s) = i^{[F:\mathbb{Q}]}R(\mathbf{g}|J_{\mathfrak{c}}, 1-s)$ from the functional equation above, one obtains an equality

$$i^{[F:\mathbb{Q}]}\Lambda(\mathbf{g}) = \epsilon_F(\rho, s)N_{F/\mathbb{Q}}(\mathfrak{c}\mathfrak{d}_F^2)^{s-1/2}$$

for all values of s such that $R(1-s, \mathbf{g}^{\iota}) \neq 0$. The result follows from putting $s = 0$. □

We will need the following integral representation, a special case of [Shi78], (4.32).

Proposition 4.2.4.

$$\Psi(\mathbf{f}, \mathbf{g}^{\iota}, 1) = D_F^{1/2}\pi^{-[F:\mathbb{Q}]}\big\langle \mathbf{f}^{\iota}, V(0)\big\rangle_{\mathfrak{c}}$$

where D_F is the discriminant of $F/\mathbb{Q}$ and

$$V(0) \;=\; \mathbf{g}^{\iota}\,.\,K_1^0\big(0; \mathfrak{c}, \mathcal{O}_F; (\det\rho)^{\dagger\,-1}\big),$$

with K_1^0 the Eisenstein series introduced in Chapter 3 *(defined in* (4.5) *of* [Pan91]*).*

Let us recall the results on Eisenstein series from Chapter 3: we can apply the involution $J_{\mathfrak{c}}$ to convert K_1^0 to the Eisenstein series E_1, for which the Fourier exapnsion is known explicitly. To be precise, we have

$$K_1^0\big(0; \mathfrak{c}, \mathcal{O}_F; (\det\rho)^{\dagger\,-1}\big)\Big|J_{\mathfrak{c}} \;=\; \frac{(4\pi i)^{[F:\mathbb{Q}]}}{D_F^{1/2}\,N_{F/\mathbb{Q}}(\mathfrak{c}\mathfrak{d}_F^2)^{1/2}}\;\; E_1\big(0, (\det\rho)^{\dagger\,-1}\big)$$

where E_1 is the Eisenstein series (4.13) in [Pan91], whose λ-components have the Fourier expansion

$$E_1\big(0,(\det\rho)^{\dagger\,-1}\big)_\lambda(z) \;=\; N_{F/\mathbb{Q}}(\tilde{t}_\lambda)^{-1/2}\sum_{0\ll\xi\in\tilde{t}_\lambda} a_\lambda(\xi)e_F(\xi z)$$

where

$$a_\lambda(\xi) \;=\; \sum_{\substack{\tilde{\xi}=\tilde{b}\tilde{c},\\ c\in\mathcal{O}_F,\\ b\in\tilde{t}_\lambda}} (\det\rho)^{\dagger\,-1}(\tilde{c}).$$

We are now in a position to prove our integrality result.

Proof of Theorem 4.2.1. Let $\mathfrak{c}=\mathfrak{c}(\mathbf{f})\mathfrak{c}(\mathbf{g})$. By Proposition 4.2.4,

$$\Psi(\mathbf{f},\mathbf{g}^\iota,1) = D_F^{1/2}\pi^{-[F:\mathbb{Q}]}\,\langle \mathbf{f}^\iota, V(0)\rangle_{\mathfrak{c}}$$

where $V(0)=\mathbf{g}^\iota\,.\,K_1^0(0;\mathfrak{c},\mathcal{O}_F;(\det\rho)^{\dagger\,-1})$. Consider $V(0)\big|J_{\mathfrak{c}}$; by our earlier formula for $K_1^0\big|J_{\mathfrak{c}}$ we have

$$\begin{aligned} V(0)|J_{\mathfrak{c}} &= (\mathbf{g}^\iota\big|J_{\mathfrak{c}})\,.\,(K_1^0\big|J_{\mathfrak{c}}) \\ &= \Lambda(\mathbf{g}^\iota)N_{F/\mathbb{Q}}(\mathfrak{c}(\mathbf{f}))^{1/2}(\mathbf{g}\big|\mathfrak{c}(\mathbf{f}))\,.\,(K_1^0\big|J_{\mathfrak{c}}) \\ &= \Lambda(\mathbf{g}^\iota)(4\pi i)^{[F:\mathbb{Q}]}D_F^{-1/2}N_{F/\mathbb{Q}}(\mathfrak{c}(\mathbf{f}))^{1/2}N_{F/\mathbb{Q}}(\mathfrak{c}(\mathbf{g})\mathfrak{d}_F^2)^{-1/2} \\ &\quad\times\ (\mathbf{g}\big|\mathfrak{c}(\mathbf{f}))\,.\,E_1(0,\,\mathfrak{c},\,(\det\rho)^{\dagger\,-1}). \end{aligned}$$

Now, $\mathfrak{c}=\mathfrak{c}(\mathbf{f})\mathfrak{c}(\mathbf{g})$, so we may employ the trace map

$$\mathrm{Tr}^{\mathfrak{c}}_{\mathfrak{c}(\mathbf{f})}\,:\,\mathcal{M}_2(\mathfrak{c},\psi)\longrightarrow\mathcal{M}_2(\mathfrak{c}(\mathbf{f}),\psi),$$

which was defined in Chapter 3. Recall that it satisfies

$$\langle\mathbf{F},\mathbf{H}\rangle_{\mathfrak{c}} \;=\; \Big\langle\mathbf{F},\mathbf{H}\big|\mathrm{Tr}^{\mathfrak{c}}_{\mathfrak{c}(\mathbf{f})}\Big\rangle_{\mathfrak{c}(\mathbf{f})}$$

and the identity

$$\mathbf{H}\big|\mathrm{Tr}^{\mathfrak{c}}_{\mathfrak{c}(\mathbf{f})} = \mathbf{H}\big|J_{\mathfrak{c}}\circ U(\mathfrak{c}(\mathbf{g}))\circ J_{\mathfrak{c}(\mathbf{f})}.$$

Setting $\Theta = (\mathbf{g}|\mathfrak{c}(\mathbf{f}))\,.\,E_1(0,(\det\rho)^{\dagger\,-1})$, we calculate

$$\begin{aligned}
\Psi(\mathbf{f},\mathbf{g}^\iota,1) &= D_F^{1/2}\pi^{-[F:\mathbb{Q}]}\,\langle \mathbf{f}^\iota, V(0)\rangle_{\mathfrak{c}} \\
&= D_F^{1/2}\pi^{-[F:\mathbb{Q}]}\,\Big\langle \mathbf{f}^\iota, V(0)\big|\mathrm{Tr}^{\mathfrak{c}}_{\mathfrak{c}(\mathbf{f})}\Big\rangle_{\mathfrak{c}(\mathbf{f})} \\
&= D_F^{1/2}\pi^{-[F:\mathbb{Q}]}\,\big\langle \mathbf{f}^\iota, V(0)\big|J_{\mathfrak{c}}\circ U(\mathfrak{c}(\mathbf{g}))\circ J_{\mathfrak{c}(\mathbf{f})}\big\rangle_{\mathfrak{c}(\mathbf{f})} \\
&= \Lambda(\mathbf{g}^\iota)(4i)^{[F:\mathbb{Q}]}\,N_{F/\mathbb{Q}}(\mathfrak{c}(\mathbf{f}))^{1/2}\,N_{F/\mathbb{Q}}(\mathfrak{c}(\mathbf{g})\mathfrak{d}_F^2)^{-1/2} \\
&\quad\times\ \big\langle \mathbf{f}^\iota, \Theta\big|U(\mathfrak{c}(\mathbf{g}))\circ J_{\mathfrak{c}(\mathbf{f})}\big\rangle_{\mathfrak{c}(\mathbf{f})}\,.
\end{aligned}$$

Observe that $\Lambda(\mathbf{g}^\iota)(4i)^{[F:\mathbb{Q}]}N_{F/\mathbb{Q}}(\mathfrak{c}(\mathbf{f}))^{1/2}$ is a p-adic unit, as $\Lambda(\mathbf{g}^\iota)$ is a root of unity and $\gcd(\mathfrak{p},4\mathfrak{c}(\mathbf{f}))=1$. Also, from Lemma 4.2.3 we know that $\mathrm{ord}_{\mathfrak{p}}(N_{F/\mathbb{Q}}(\mathfrak{c}(\mathbf{g})\mathfrak{d}_F^2)^{1/2}) = \mathrm{ord}_{\mathfrak{p}}(\epsilon_F(\rho))$. Therefore,

$$\mathrm{ord}_{\mathfrak{p}}\left(\epsilon_F(\rho).\frac{\Psi(\mathbf{f},\mathbf{g}^\iota,1)}{\langle\mathbf{f},\mathbf{f}\rangle_{\mathfrak{c}(\mathbf{f})}}\right) \;=\; \mathrm{ord}_{\mathfrak{p}}\left(\frac{\big\langle \mathbf{f}^\iota, \Theta\big|U(\mathfrak{c}(\mathbf{g}))\circ J_{\mathfrak{c}(\mathbf{f})}\big\rangle_{\mathfrak{c}(\mathbf{f})}}{\langle\mathbf{f},\mathbf{f}\rangle_{\mathfrak{c}(\mathbf{f})}}\right)$$

so it suffices to prove the p-integrality of the quantity on the right hand side. As the operator J is an involution, we have

$$\big\langle \mathbf{F},\mathbf{H}\big|J_{\mathfrak{c}}\big\rangle_{\mathfrak{c}} \;=\; \big\langle \mathbf{F}\big|J_{\mathfrak{c}},\mathbf{H}\big\rangle_{\mathfrak{c}}$$

for any $\mathbf{H}\in\mathcal{M}_2(\mathfrak{c},\psi)$ and any $\mathbf{F}\in\mathcal{S}_2(\mathfrak{c},\psi)$. Therefore

$$\begin{aligned}
\big\langle \mathbf{f}^\iota, \Theta\big|U(\mathfrak{c}(\mathbf{g}))\circ J_{\mathfrak{c}(\mathbf{f})}\big\rangle_{\mathfrak{c}(\mathbf{f})} &= \big\langle \mathbf{f}^\iota\big|J_{\mathfrak{c}(\mathbf{f})}, \Theta|U(\mathfrak{c}(\mathbf{g}))\big\rangle_{\mathfrak{c}(\mathbf{f})} \\
&= \Lambda(\mathbf{f}^\iota)\,\big\langle \mathbf{f}, \Theta\big|U(\mathfrak{c}(\mathbf{g}))\big\rangle_{\mathfrak{c}(\mathbf{f})}\,.
\end{aligned}$$

By choosing a basis for the finite dimensional vector space $\mathcal{M}_2(\mathfrak{c}(\mathbf{f}))$ which includes $\mathbf{f}$, we may write

$$\Theta\big|U(\mathfrak{c}(\mathbf{g})) \;=\; c\,\mathbf{f} \;+\; \sum_{\mathbf{f}_i\neq\mathbf{f}} c_i\;\mathbf{f}_i\big|\mathfrak{b}_i$$

for algebraic numbers c_i (which are almost all zero), where each form $\mathbf{f}_i$ is primitive of level $\mathfrak{a}_i$, such that $\mathfrak{a}_i\mathfrak{b}_i$ divides $\mathfrak{c}(\mathbf{f})$. We deduce that

$$\frac{\big\langle \mathbf{f}^\iota, \Theta\big|U(\mathfrak{c}(\mathbf{g}))\circ J_{\mathfrak{c}(\mathbf{f})}\big\rangle_{\mathfrak{c}(\mathbf{f})}}{\langle\mathbf{f},\mathbf{f}\rangle_{\mathfrak{c}(\mathbf{f})}} \;=\; \Lambda(\mathbf{f}^\iota)\left(c+\sum_{\mathbf{f}_i\neq\mathbf{f}} c_i\,\frac{\big\langle \mathbf{f},\mathbf{f}_i\big|\mathfrak{b}_i\big\rangle_{\mathfrak{c}(\mathbf{f})}}{\langle\mathbf{f},\mathbf{f}\rangle_{\mathfrak{c}(\mathbf{f})}}\right).$$

It is a simple consequence of Proposition 4.13 of Shimura [Shi78] that

$$\left\langle \mathbf{f}, \mathbf{f}_i \middle| \mathfrak{b}_i \right\rangle_{\mathfrak{c}(\mathbf{f})} = \left. \frac{L(\mathbf{f}, \mathbf{f}_i^\iota | \mathfrak{b}_i, s)}{L(\mathbf{f}, \mathbf{f}_i^\iota, s)} \right|_{s=2} \times \left\langle \mathbf{f}, \mathbf{f}_i \right\rangle_{\mathfrak{c}(\mathbf{f})}$$

One may therefore write

$$\frac{\left\langle \mathbf{f}, \mathbf{f}_i \middle| \mathfrak{b}_i \right\rangle_{\mathfrak{c}(\mathbf{f})}}{\left\langle \mathbf{f}, \mathbf{f} \right\rangle_{\mathfrak{c}(\mathbf{f})}} = \left. \frac{L(\mathbf{f}, \mathbf{f}_i^\iota | \mathfrak{b}_i, s)}{L(\mathbf{f}, \mathbf{f}_i^\iota, s)} \right|_{s=2} \times \frac{\left\langle \mathbf{f}, \mathbf{f}_i \right\rangle_{\mathfrak{c}(\mathbf{f})}}{\left\langle \mathbf{f}, \mathbf{f} \right\rangle_{\mathfrak{c}(\mathbf{f})}}.$$

But $\left\langle \mathbf{f}, \mathbf{f}_i \right\rangle_{\mathfrak{c}(\mathbf{f})} = 0$ as $\mathbf{f}$ and $\mathbf{f}_i$ are distinct primitive forms, whence

$$\frac{\left\langle \mathbf{f}, \mathbf{f}_i \middle| \mathfrak{b}_i \right\rangle_{\mathfrak{c}(\mathbf{f})}}{\left\langle \mathbf{f}, \mathbf{f} \right\rangle_{\mathfrak{c}(\mathbf{f})}} = 0$$

for each i. It follows that

$$\frac{\left\langle \mathbf{f}^\iota, \Theta | U(\mathfrak{c}(\mathbf{g})) \circ J_{\mathfrak{c}(\mathbf{f})} \right\rangle_{\mathfrak{c}(\mathbf{f})}}{\left\langle \mathbf{f}, \mathbf{f} \right\rangle_{\mathfrak{c}(\mathbf{f})}} = \Lambda(\mathbf{f}^\iota)\, c.$$

Since $\Lambda(\mathbf{f}^\iota)$ is a root of unity, it suffices to prove that c is p-integral.

Suppose not; then $c^{-1} \equiv 0 \mod \mathfrak{p}$. We have an explicit formula for the Fourier coefficients of $E_1(0, (\det \rho)^{\dagger\,-1})$, and they are easily seen to be p-integral. Also, we wrote down the Fourier coefficients of $\mathbf{g}_\rho$ in Chapter 3: they are p-integral too. Therefore $\Theta = (\mathbf{g}_\rho | \mathfrak{c}(\mathbf{f}))\, . E_1(0, \mathfrak{c}, (\det \rho)^{\dagger\,-1})$ must have p-integral Fourier coefficients, implying

$$c^{-1}\, \Theta \big| U \equiv 0 \mod \mathfrak{p},$$

by our assumption that $c^{-1} \equiv 0 \mod \mathfrak{p}$. So,

$$\begin{aligned} \mathbf{f} &= c^{-1}\, \Theta \big| U - \sum_{\mathbf{f}_i \neq \mathbf{f}} c^{-1} c_i\, \mathbf{f}_i \big| \mathfrak{b}_i \\ &\equiv -\sum_{\mathbf{f}_i \neq \mathbf{f}} c^{-1} c_i\, \mathbf{f}_i \big| \mathfrak{b}_i \qquad \mod \mathfrak{p}. \end{aligned}$$

It follows that $\mathbf{f}$ is congruent modulo $\mathfrak{p}$ to a distinct modular form in $\mathcal{M}_2(\mathfrak{c}(\mathbf{f}))$, contradicting the hypothesis of the theorem. This completes the proof of Theorem 4.2.1. $\square$

4.3 Constructing the Distribution

Having established our integrality result, we go on to construct the distribution. We continue to write $F = \mathbb{Q}(\mu_{p^n})^+$, and we write $\mathbf{f}$ for the base change of f_E to F, where $E_{/\mathbb{Q}}$ is our semistable elliptic curve (this base change is guaranteed to exist as the field F is abelian over $\mathbb{Q}$).

For a finite place $v \neq \mathfrak{p}$ of F, we label roots $\alpha(v)$, $\alpha'(v)$ of the polynomial

$$1 - C(v, \mathbf{f})X + N_{F/\mathbb{Q}}(v)X^2 \;=\; (1 - \alpha(v)X)(1 - \alpha'(v)X).$$

We also define $\alpha(\mathfrak{p})$ and $\alpha'(\mathfrak{p})$ to be the roots of

$$1 - C(\mathfrak{p}, \mathbf{f})X + pX^2 \;=\; (1 - \alpha(\mathfrak{p})X)(1 - \alpha'(\mathfrak{p})X).$$

where $\alpha(\mathfrak{p})$ is the $\mathfrak{p}$-adic unit, and $\alpha'(\mathfrak{p})$ is the non-unit root. From these definitions, we extend the expressions $\alpha(\mathfrak{m})$, $\alpha'(\mathfrak{m})$ multiplicatively to all ideals $\mathfrak{m}$ of $\mathcal{O}_F$.

Definition 4.3.1. *Set* $\mathfrak{l}_0 := \prod_{\mathfrak{q}|\Delta} \mathfrak{q}$. *Then the* $\mathfrak{p}\mathfrak{l}_0$*-stabilisation of* $\mathbf{f}$ *is defined to be*

$$\mathbf{f}_0 \;:=\; \sum_{\mathfrak{a}|\mathfrak{p}\mathfrak{l}_0} M(\mathfrak{a})\alpha'(\mathfrak{a}).\mathbf{f}\big|\mathfrak{a}$$

where M *is the Möbius function on ideals.*

As Panchishkin points out in [Pan91], this definition is equivalent to the identity

$$L(\mathbf{f}_0, s) \;=\; L(\mathbf{f}, s) \;\times\; \prod_{\mathfrak{q}|\mathfrak{p}\mathfrak{l}_0} (1 - \alpha'(\mathfrak{q})N_{F/\mathbb{Q}}(\mathfrak{q})^{-s})$$

i.e. we have removed the α'-part of the Euler factors at the primes dividing $\mathfrak{p}\mathfrak{l}_0$. One can check that the level of $\mathbf{f}_0$ is $\mathfrak{p}\mathfrak{l}_0\mathfrak{c}(\mathbf{f})$.

Lemma 4.3.2. *Suppose* $\mathfrak{m}$ *is an integral ideal dividing* $\mathfrak{p}\mathfrak{l}_0$. *Then*

$$\mathbf{f}_0\big|U\big(\mathfrak{c}(\mathbf{f})\mathfrak{m}\big) \;=\; \alpha(\mathfrak{m})\; C\big(\mathfrak{c}(\mathbf{f}), \mathbf{f}\big)\; \mathbf{f}_0.$$

Proof. This result follows easily from the definition of $\mathbf{f}_0$ and the effect of the operators $\big|U(\mathfrak{m})$ and $\big|\mathfrak{m}$ on Fourier coefficients. □

Following (3.14) of [Pan91], we also define

$$\mathbf{g}_{\rho,\mathfrak{p}\mathfrak{l}_0} := \sum_{\mathfrak{n}|\mathfrak{p}\mathfrak{l}_0} M(\mathfrak{n}).\, \mathbf{g}_\rho \big| U(\mathfrak{n}) \circ \mathfrak{n}.$$

This definition is equivalent to the identity

$$L(\mathbf{g}_{\rho,\mathfrak{p}\mathfrak{l}_0}, s) \;=\; L(\mathbf{g}, s) \;\times\; \prod_{\mathfrak{q}|\mathfrak{p}\mathfrak{l}_0} (1 - \beta(\mathfrak{q}) N_{F/\mathbb{Q}}(\mathfrak{q})^{-s})\,(1 - \beta'(\mathfrak{q}) N_{F/\mathbb{Q}}(\mathfrak{q})^{-s})$$

i.e. we have completely removed the Euler factors at the primes dividing $\mathfrak{p}\mathfrak{l}_0$. We modify $\mathbf{g}_\rho$ in this way to ensure the Euler factor in our special value is the correct one.

Set $\mathfrak{c}_0 = \mathfrak{p}\mathfrak{l}_0\mathfrak{c}(\mathbf{f})$. We shall choose ideals $\mathfrak{m}'$ and $\mathfrak{l}'$ such that $\mathfrak{m}'$ is a power of $\mathfrak{p}$, $\mathrm{supp}(\mathfrak{l}') = \mathrm{supp}(\mathfrak{l}_0)$, and that $\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2 | \mathfrak{m}'\mathfrak{l}'$. We have

$$\mathbf{f}_0 \;\in\; \mathcal{S}_{\mathbf{2}}(\mathfrak{c}_0) \;\subset\; \mathcal{S}_{\mathbf{2}}(\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}')$$

and

$$\mathbf{g}_{\rho,\mathfrak{p}\mathfrak{l}_0} \;\in\; \mathcal{M}_{\mathbf{1}}(\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2,\, (\det\rho)^\dagger) \;\subset\; \mathcal{M}_{\mathbf{1}}(\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}', (\det\rho)^\dagger).$$

Then the contragredient Euler factor is given by

$$\begin{aligned}\mathrm{Eul}_{\mathfrak{p}\mathfrak{l}_0}(\rho^\vee, s) \;:=\; & \prod_{v|\mathfrak{p}\mathfrak{l}_0} (1 - \alpha'(v)\hat{\beta}(v)N(v)^{-s})(1 - \alpha'(v)\hat{\beta}'(v)N(v)^{-s}) \\ & \times (1 - \alpha^{-1}(v)\beta(v)N(v)^{s-1})(1 - \alpha^{-1}(v)\beta'(v)N(v)^{s-1}).\end{aligned}$$

Here we have factorised the Hecke polynomial as

$$1 - C(v, \mathbf{g}_\rho)X + (\det\rho)^\dagger(v)X^2 \;=\; (1 - \beta(v)X)(1 - \beta'(v)X),$$

and the dual Hecke polynomial as

$$1 - \overline{C(v, \mathbf{g}_\rho)}X + (\det\rho)^{\dagger\,-1}(v)X^2 \;=\; (1 - \hat{\beta}(v)X)(1 - \hat{\beta}'(v)X).$$

Remark 4.3.3. Since we assumed that E is semistable over $\mathbb{Q}$, we have

$$C\big(\mathfrak{c}(\mathbf{f}), \mathbf{f}\big) \;=\; (-1)^{\#\mathcal{T}_F^{ns}}$$

where $\mathcal{T}_F^{ns}$ denotes the set of finite places of F where E has non-split multiplicative reduction. In particular, $C\big(\mathfrak{c}(\mathbf{f}), \mathbf{f}\big) \neq 0$.

Lemma 4.3.4. *We have the following identity:*

$$\Psi(\mathbf{f}_0, \mathbf{g}_{\rho,\mathfrak{p}\mathfrak{l}_0}\big|J_{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}, s) \;=\; N_{F/\mathbb{Q}}\left(\frac{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)}\right)^{1/2-s} \Lambda(\mathbf{g}_\rho)\;\alpha\left(\frac{\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)}\right) C\big(\mathfrak{c}(\mathbf{f}), \mathbf{f}\big)$$
$$\times\;\mathrm{Eul}_{\mathfrak{p}\mathfrak{l}_0}(\rho^\vee, s)\quad \Psi(\mathbf{f}, \mathbf{g}_\rho^\iota, s).$$

Proof. Recall the formula $\mathbf{f}|J_{\mathfrak{m}\mathfrak{c}} = N_{F/\mathbb{Q}}(\mathfrak{m})^{k/2}(\mathbf{f}\big|J_{\mathfrak{c}})\big|\mathfrak{m}$ from Chapter 3. Since $\mathfrak{c}(\mathbf{g}_{\rho,\mathfrak{p}\mathfrak{l}_0}) = \mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2$, it follows that

$$\mathbf{g}_{\rho,\mathfrak{p}\mathfrak{l}_0}\big|J_{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'} = N_{F/\mathbb{Q}}\left(\frac{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}\right)^{1/2}\cdot\left(\mathbf{g}_{\rho,\mathfrak{p}\mathfrak{l}_0}\big|J_{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}\right)\Big|\frac{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}\quad.$$

For brevity, we will write

$$\mathbf{h} = \mathbf{g}_{\rho,\mathfrak{p}\mathfrak{l}_0}\big|J_{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}\quad.$$

Then

$$\begin{aligned}\Psi(\mathbf{f}_0, \mathbf{g}_{\rho,\mathfrak{p}\mathfrak{l}_0}\big|J_{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}, s) \;&=\; N_{F/\mathbb{Q}}\left(\frac{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}\right)^{1/2}\;\Psi\left(\mathbf{f}_0, \mathbf{h}\middle|\frac{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}, s\right)\\ &=\; N_{F/\mathbb{Q}}\left(\frac{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}\right)^{1/2-s}\;\Psi\left(\mathbf{f}_0\middle|U\left(\frac{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}\right), \mathbf{h}, s\right)\\ &=\; N_{F/\mathbb{Q}}\left(\frac{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}\right)^{1/2-s}\;\alpha\left(\frac{\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}\right)\;C\big(\mathfrak{c}(\mathbf{f}), \mathbf{f}\big)\;\Psi\left(\mathbf{f}_0, \mathbf{h}, s\right).\end{aligned}$$

Here we have exploited the fact that

$$L\left(s, \mathbf{f}_0, \mathbf{g}_\rho^\iota|\mathfrak{a}\right) \;=\; N_{F/\mathbb{Q}}(\mathfrak{a})^{-s}\;L\left(s, \mathbf{f}_0|U(\mathfrak{a}), \mathbf{g}_\rho^\iota\right)$$

for any ideal $\mathfrak{a}$ (which is clear from the definition of the operators $|\mathfrak{a}$ and $|U(\mathfrak{a})$), and also the formula

$$\mathbf{f}_0|U\left(\frac{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}\right) \;=\; \alpha\left(\frac{\mathfrak{m}'\mathfrak{l}'}{\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{p}^2\mathfrak{l}_0^2}\right)\;C\big(\mathfrak{c}(\mathbf{f}), \mathbf{f}\big)\;\mathbf{f}_0$$

which follows from Lemma 4.3.2. Furthermore,

$$\Psi(\mathbf{f}_0, \mathbf{h}, s) \;=\; N_{F/\mathbb{Q}}(\mathfrak{p}^2\mathfrak{l}_0^2)^{1-2s}\;\alpha(\mathfrak{p}^2\mathfrak{l}_0^2)\;\Lambda(\mathbf{g}_\rho)\;\mathrm{Eul}_{\mathfrak{p}\mathfrak{l}_0}(\rho^\vee, s)\;\Psi(\mathbf{f}, \mathbf{g}_\rho^\iota, s).$$

This is proved in [Pan91] Section 3.6. Combining the two equations together yields the required result. □

Definition 4.3.5. *We define the complex linear functional $\mathcal{L}_F$ on the vector space $\mathcal{M}_{\mathbf{2}}(\mathfrak{c}_0)$ by*

$$\mathcal{L}_F \ : \ \Theta \longmapsto \frac{\left\langle \mathbf{f_0}^{\iota}, \Theta \middle| J_{\mathfrak{c}_0} \right\rangle_{\mathfrak{c}_0}}{\langle \mathbf{f}, \mathbf{f} \rangle_{\mathfrak{c}(\mathbf{f})}}.$$

We shall now consider the modular form

$$\Phi \ = \ \Phi(\rho/F,\, \mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}') \ := \ \mathbf{g}_{\rho,\mathfrak{p}\mathfrak{l}_0} \,.\, E_1(0,\, \mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}',\, (\det \rho)^{\dagger\,-1})$$

where E_1 refers to the Eisenstein series of Section 3.7.

Corollary 4.3.6. *We have the formula*

$$\begin{aligned} & \frac{N_{F/\mathbb{Q}}(\mathfrak{c}(\mathbf{g}_\rho)\mathfrak{d}_F^2)^{1/2}\Lambda(\mathbf{g}_\rho)}{\alpha(\mathfrak{c}(\mathbf{g}_\rho))} \quad \mathrm{Eul}_{\mathfrak{p}\mathfrak{l}_0}(\rho^\vee, 1) \quad \frac{\Psi(\mathbf{f}, \mathbf{g}_\rho^\iota, 1)}{\langle \mathbf{f}, \mathbf{f} \rangle_{\mathfrak{c}(\mathbf{f})}} \\ = \quad & \frac{(-4i)^{[F:\mathbb{Q}]}}{\alpha(\mathfrak{m}'\mathfrak{l}')C\big(\mathfrak{c}(\mathbf{f}), \mathbf{f}\big)} \quad \mathcal{L}_F\left(\Phi \middle| U(\mathfrak{m}'\mathfrak{l}'\mathfrak{p}^{-1}\mathfrak{l}_0^{-1})\right). \end{aligned}$$

Proof. Applying the integral representation from Proposition 4.2.4, then using the trace map $\mathrm{Tr}_{\mathfrak{c}_0}^{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}$ as we did to prove Theorem 4.2.1, we obtain

$$\frac{\Psi(\mathbf{f}_0, \mathbf{g}_{\rho,\mathfrak{p}\mathfrak{l}_0} \big| J_{\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'}, 1)}{\langle \mathbf{f}, \mathbf{f} \rangle_{\mathfrak{c}(\mathbf{f})}} \ = \ \frac{(-4i)^{[F:\mathbb{Q}]}}{N_{F/\mathbb{Q}}(\mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}'\mathfrak{d}_F^2)^{1/2}} \quad \mathcal{L}_F\left(\Phi \middle| U(\mathfrak{m}'\mathfrak{l}'\mathfrak{p}^{-1}\mathfrak{l}_0^{-1})\right).$$

Combining this formula with Lemma 4.3.4 gives the desired result. □

This result implies an important distribution property: let us fix our representation ρ over F and consider the set of finite-order Hecke characters ψ such that $\mathrm{supp}(\mathfrak{c}(\psi)) = \mathrm{supp}(\mathfrak{p}\mathfrak{l}_0\mathfrak{c}(\mathbf{f}))$. Then we set

$$\begin{aligned} \tilde{\mu}_{\mathfrak{m}'\mathfrak{l}'}(\psi_{\mathfrak{m}'\mathfrak{l}'}) \ &= \ \frac{(-4i)^{[F:\mathbb{Q}]}}{N_{F/\mathbb{Q}}(\mathfrak{d}_F)\alpha(\mathfrak{m}'\mathfrak{l}')C\big(\mathfrak{c}(\mathbf{f}), \mathbf{f}\big)} \\ &\times \ \mathcal{L}_F\left(\Phi(\rho \otimes \psi/F,\, \mathfrak{c}(\mathbf{f})\mathfrak{m}'\mathfrak{l}') \,\middle|\, U(\mathfrak{m}'\mathfrak{l}'\mathfrak{p}^{-1}\mathfrak{l}_0^{-1})\right) \end{aligned}$$

for each ψ and each $\mathfrak{m}', \mathfrak{l}'$ such that $\mathfrak{c}(\mathbf{g}_{\rho\otimes\psi})\,\mathfrak{p}^2\mathfrak{l}_0^2 \,|\, \mathfrak{m}'\mathfrak{l}'$. However, Corollary 4.3.6 shows that the left-hand side does not depend on $\mathfrak{m}'$ or $\mathfrak{l}'$, so neither does the right hand side. That is, $\tilde{\mu}_{\mathfrak{m}'\mathfrak{l}'}(\psi_{\mathfrak{m}'\mathfrak{l}'})$ is independent of the choice of $\mathfrak{m}'\mathfrak{l}'$. This condition

is equivalent to the fact that the family of functions $\{\tilde{\mu}_{\mathfrak{m}'\mathfrak{l}'} : \mathfrak{m}'\mathfrak{l}'\}$ constitutes a distribution on $\mathcal{G} = \mathrm{Gal}(F_S^{\mathrm{ab}}/F)$. We will proceed to show that this distribution gives an integral-valued p-adic measure on $\mathcal{G}$.

We now consider the Hilbert modular form $\mathbf{g}_{\rho_k/F_n}$, the base change of $\mathbf{g}_{\rho_k}$ to F_n. Recall from Chapter 3 that this modular form corresponds to the induced representation $\mathrm{Res}_{F_n}\rho_k = \mathrm{Ind}_{K_n}^{F_n}(\mathrm{Res}_{K_n}\chi_{\rho_k})$, for which we write ρ_k/F_n as a shorthand.

Let us denote by $\mathcal{G}_n$ the topological group $\mathrm{Gal}(F_{n,S}^{\mathrm{ab}}/F_n)$ where $F_{n,S}^{\mathrm{ab}}$ is the maximal abelian extension of F_n unramified outside the set $S = \{v : v|\mathfrak{p}\mathfrak{l}_0\}$ and the infinite places. For the remainder of this section, $\psi : \mathcal{G}_n \longrightarrow \mathbb{C}^\times$ will be a continuous character with conductor $\mathfrak{f}_\psi$. We shall apply our earlier results to $\mathbf{g}_\rho = \mathbf{g}_{\rho_k/F_n\otimes\psi}$, as the representation $\rho_k/F_n\otimes\psi$ over F_n is clearly induced by the character $\mathrm{Res}_{K_n}(\chi_{\rho_k}\otimes\psi)$ over K_n. It is simple to check that

$$\mathrm{Res}_{K_n}(\chi_{\rho_k}\otimes\psi)^\dagger \;=\; (\chi_{\rho_k}^\dagger\otimes\psi^\dagger)\circ N_{K_n/K_k}.$$

Also, the character of $\mathbf{g}_{\rho_k/F_n\otimes\psi}$ is $(\mathrm{Res}_{F_n}\det\rho_k)^\dagger\otimes\psi^{\dagger\,2}$, and we have

$$(\mathrm{Res}_{F_n}(\det\rho_k)\otimes\psi^2)^\dagger = ((\det\rho_k)^\dagger\circ N_{F_n/F_k})\otimes\psi^{\dagger\,2}.$$

Definition 4.3.7. *The parallel weight 2 Hilbert modular form $\Phi_\psi^{n,k}$ is given by*

$$\begin{aligned}\Phi_\psi^{n,k} &= \Phi_\psi^{n,k}(\rho_k/F_n\otimes\psi,\, \mathfrak{c}(\mathbf{f}_{/F_n})\mathfrak{m}'\mathfrak{l}')\\ &:= (\mathbf{g}_{\rho_k/F_n\otimes\psi,\mathfrak{p}\mathfrak{l}_0})\,.\,E_1(0,\,\mathfrak{c}(\mathbf{f}_{/F_n})\mathfrak{m}'\mathfrak{l}',\,(\mathrm{Res}_{F_n}\det\rho_k)^{-1}\otimes\psi^{-2})\end{aligned}$$

where we assume that $\mathfrak{m}'\,\mathfrak{l}'$ is divisible by $\mathfrak{c}(\mathbf{g}_{\rho_k/F_n})(\mathfrak{p}\mathfrak{l}_0\mathfrak{f}_\psi)^2$.

Applying Corollary 4.3.6 directly to $\mathbf{g}_{\rho_k/F_n\otimes\psi}$, we deduce the following result.

Corollary 4.3.8. *For all $n \geq k$,*

$$\begin{aligned}&\frac{(-4i)^{\phi(p^n)/2}}{\alpha(\mathfrak{m}'\mathfrak{l}')C\big(\mathfrak{c}(\mathbf{f}),\mathbf{f}\big)}\,\mathcal{L}_{F_n}\left(\Phi_\psi^{n,k}\big|U(\mathfrak{m}'\mathfrak{l}'\mathfrak{p}^{-1}\mathfrak{l}_0^{-1})\right) \;=\; \frac{N_{F_n/\mathbb{Q}}(\mathfrak{c}(\mathbf{g}_{\rho_k/F_n\otimes\psi})\mathfrak{d}_{F_n}^2)^{1/2}}{\alpha(\mathfrak{c}(\mathbf{g}_{\rho_k/F_n\otimes\psi}))}\\ &\times\;\Lambda(\mathbf{g}_{\rho_k/F_n\otimes\psi})\;\times\;\mathrm{Eul}_{\mathfrak{p}\mathfrak{l}_0}(\rho_k/F_n\otimes\psi^{-1},1)\;\times\;\frac{\Psi(\mathbf{f}_{/F_n},\mathbf{g}^\iota_{\rho_k/F_n\otimes\psi},1)}{\big\langle\mathbf{f}_{/F_n},\mathbf{f}_{/F_n}\big\rangle_{\mathfrak{c}(\mathbf{f})}}\,.\end{aligned}$$

Furthermore, the Fourier coefficients of the λ-component of $\Phi_\psi^{n,k}$ are given by

$$\begin{aligned}\phi_{\psi,\lambda}^{n,k}(\xi) &= \sum_{\xi=\xi_1+\xi_2} \sum_{\substack{\mathfrak{a}\lhd\mathcal{O}_{K_n},\\ \mathfrak{a}\bar{\mathfrak{a}}=\xi_1\tilde{t}_\lambda^{-1}}} (\chi_{\rho_k}^\dagger \circ N_{K_n/K_k})(\mathfrak{a})\,\psi^\dagger(\xi_1\tilde{t}_\lambda^{-1}) \\ &\times \sum_{\substack{\tilde{\xi}_2=\tilde{b}\tilde{c},\\ c\in\mathcal{O}_{F_n},\\ b\in\tilde{t}_\lambda}} \left((\det\rho_k)^\dagger \circ N_{F_n/F_k}\right)^{-1}(\tilde{c})\,\psi^\dagger(\tilde{c})^{-2}.\end{aligned}$$

4.4 The Connection with Elliptic Curves

We need to interpret the values from Corollary 4.3.8 back in terms of the arithmetic of $E_{/\mathbb{Q}}$.

First, we will find an expression for the α-term from the formula. Recall that we already made a choice of $\alpha(\mathfrak{q})$ for each $\mathfrak{q}$ dividing $\mathfrak{pl}_0$, in order to define the $\mathfrak{pl}_0$-stabilisation $\mathbf{f}_0$. For an Artin representation ρ over a field F, we denote its conductor by $\mathfrak{f}_\rho$. This is an ideal of $\mathcal{O}_F$, and we write $f(\rho,\mathfrak{q})$ for the exponent of the prime $\mathfrak{q}$ in $\mathfrak{f}_\rho$.

Lemma 4.4.1. ***(i)*** *For each prime $q|p\Delta$, there exists a root α_q of the polynomial $1-a_q(E)T+qT^2$ such that*

$$\alpha(\mathfrak{c}(\mathbf{g}_{\rho_k/F_n}\otimes\psi)) \;=\; \alpha_p^{f(\rho_k/F_n\otimes\psi,\mathfrak{p})}\cdot\prod_{q|\Delta}\alpha_q^{\mathrm{ord}_q(A_{\tilde{\chi}})}$$

where $\tilde{\chi}=\mathrm{Res}_{K_n}(\chi_{\rho_k}\otimes\psi)$ and $A_{\tilde{\chi}}=N_{K_n/\mathbb{Q}}(\mathfrak{f}_{\tilde{\chi}})$.

(ii) *Furthermore, if we make the stronger assumption that ψ is a character of $\mathrm{Gal}(F_{n,\{\mathfrak{p}\}}^{\mathrm{ab}}/F_n)$ i.e. ψ is ramified only at the prime above p, then*

$$\mathrm{ord}_q(A_{\tilde{\chi}})=p^n-p^{n-1}\qquad \textit{for all } q|\Delta.$$

In particular, $\alpha(\mathfrak{c}(\mathbf{g}_{\rho_k/F_n}\otimes\psi))$ is always a p-adic unit.

Proof. For $\mathfrak{q}\neq\mathfrak{p}$, $\alpha(\mathfrak{q})$ is one of the eigenvalues of $\mathrm{Frob}_\mathfrak{q}^{-1}$ acting on the Tate module $T_p(E)$. However, $\mathrm{Frob}_\mathfrak{q}^{-1}=\mathrm{Frob}_q^{-[f_{n,\mathfrak{q}}:\mathbb{F}_q]}$ where $f_{n,\mathfrak{q}}$ denotes the residue field of F_n

at $\mathfrak{q}$. Therefore

$$\alpha(\mathfrak{q}) \;=\; \alpha_q^{[f_{n,\mathfrak{q}}:\mathbb{F}_q]}$$

for one of the roots α_q of $1 - a_q(E)T + qT^2$.

For $\mathfrak{q} = \mathfrak{p}$, we instead consider $T_p(\tilde{E})$ where $\tilde{E}$ denotes the reduction of E over $f_{n,\mathfrak{p}}$. In this case, $\mathrm{rank}_{\mathbb{Z}_p} T_p(\tilde{E}) = 1$ because we have assumed E has good ordinary reduction at p, so $\alpha(\mathfrak{p})$ is the unique eigenvalue of $\mathrm{Frob}_{\mathfrak{p}}^{-1}$ acting on $T_p(\tilde{E})$. Applying the same argument as above, $\alpha(\mathfrak{p}) = \alpha_p$.

Set $\mathfrak{c} = \mathfrak{c}(\mathbf{g}_{\rho_k/F_n} \otimes \psi)$ for brevity. Then $\alpha(\mathfrak{c})$ is defined multiplicatively, so

$$\alpha(\mathfrak{c}) \;=\; \prod_{\substack{\mathfrak{q}\in \mathrm{Spec}(\mathcal{O}_{F_n}),\\ \mathfrak{q}\,|\,\mathfrak{c}}} \alpha(\mathfrak{q})^{\mathrm{ord}_{\mathfrak{q}}(\mathfrak{c})} \;=\; \prod_{q | N_{F_n/\mathbb{Q}}(\mathfrak{c})} \alpha_q^{\mathrm{ord}_q(N_{F_n/\mathbb{Q}}(\mathfrak{c}))}.$$

Because $\rho_k/F_n \otimes \psi = \mathrm{Ind}_{K_n}^{F_n} \tilde{\chi}$, we have

$$\mathfrak{c}(\mathbf{g}_{\rho_k/F_n} \otimes \psi) \;=\; N_{K_n/F_n}(\mathfrak{f}_{\tilde{\chi}})\,\mathrm{Disc}(K_n/F_n)$$

by Shimura's formula for the level of $\mathbf{g}_\rho$ from [Shi78] section 5. However $\mathrm{Disc}(K_n/F_n) = \mathfrak{p}$, which means

$$N_{F_n/\mathbb{Q}}(\mathfrak{c}) \;=\; p.N_{K_n/\mathbb{Q}}(\mathfrak{f}_{\tilde{\chi}}).$$

The primes dividing $N_{K_n/\mathbb{Q}}(\mathfrak{f}_{\tilde{\chi}})$ are those dividing $p\Delta$, whence

$$\alpha(\mathfrak{c}(\mathbf{g}_{\rho_k/F_n} \otimes \psi)) \;=\; \alpha_p^{1+\mathrm{ord}_p(A_{\tilde{\chi}})} \,.\, \prod_{q|\Delta} \alpha_q^{\mathrm{ord}_q(A_{\tilde{\chi}})}.$$

Now, p is completely ramified in the extension $K_n/\mathbb{Q}$, so if $\mathfrak{P}$ denotes the unique prime of K_n above p, we have $N_{K_n/\mathbb{Q}}(\mathfrak{P}) = p$. From this we deduce

$$\begin{aligned} 1 + \mathrm{ord}_p(A_{\tilde{\chi}}) &= 1 + \mathrm{ord}_{\mathfrak{P}}(\mathfrak{f}_{\tilde{\chi}}) \\ &= f(\rho_k/F_n \otimes \psi, \mathfrak{p}) \end{aligned}$$

by the usual formula for the induced conductor, and this proves **(i)**.

It remains to prove assertion **(ii)**. We now assume ψ is ramified only above p, and that $q|\Delta$. We then obtain

$$\mathrm{ord}_q(N_{K_n/\mathbb{Q}}(\mathfrak{f}_{\tilde{\chi}})) = \sum_{\mathfrak{q}|q} f(\tilde{\chi},\mathfrak{q})[k_{n,\mathfrak{q}}:\mathbb{F}_q]$$

where the sum is taken over the primes of K_n above q, and $k_{n,\mathfrak{q}}$ denotes the residue field of K_n at $\mathfrak{q}$. Under our additional assumption on ψ, we can say

$$f(\tilde{\chi},\mathfrak{q}) = f(\mathrm{Res}_{K_n}\chi_{\rho_k},\mathfrak{q})$$

and the character $\mathrm{Res}_{K_n}\chi_{\rho_k}$ factors through the extension $K_n(\sqrt[p^n]{\Delta})/K_n$. The prime $\mathfrak{q}$ is totally yet tamely ramified in this extension. Therefore $\mathrm{Res}_{K_n}\chi_{\rho_k}$ is non-trivial on the inertia group, but is trivial on all the higher ramification groups. By definition of the Artin conductor, this implies $f(\tilde{\chi},\mathfrak{q}) = 1$. Therefore,

$$\begin{aligned}\mathrm{ord}_q(N_{K_n/\mathbb{Q}}(\mathfrak{f}_{\tilde{\chi}})) &= \sum_{\mathfrak{q}|q}[k_{n,\mathfrak{q}}:\mathbb{F}_q] \\ &= [k_{n,\mathfrak{q}}:\mathbb{F}_q] \ \times \ \text{number of primes of } K_n \text{ above } q \\ &= [K_n:\mathbb{Q}]\end{aligned}$$

as q is unramified in $K_n/\mathbb{Q}$. Observing that $[K_n:\mathbb{Q}] = p^n - p^{n-1}$ completes the demonstration of **(ii)**.

Finally, as α_p was chosen to be a p-adic unit and either choice of α_q is a p-adic unit when $q \neq p$, it is clear $\alpha(\mathfrak{c}(\mathbf{g}_{\rho_k/F_n}\otimes\psi))$ is always a p-adic unit. □

Now we can relate the Hilbert modular form $\Phi_\psi^{n,k}$ to Artin-twists of the L-function of $E_{/F_n}$. It is neccessary to use the following automorphic period:

$$\Omega^{\mathrm{aut}}_{E/F_n} \ := \ (2\pi)^{\phi(p^n)}\left\langle \mathbf{f}_{/F_n}, \mathbf{f}_{/F_n}\right\rangle_{\mathfrak{c}(\mathbf{f})}.$$

Theorem 4.4.2. *Let $\tilde{\chi} = \mathrm{Res}_{K_n}(\chi_{\rho_k}\otimes\psi)$, and $A_{\tilde{\chi}} = N_{K_n/\mathbb{Q}}(\mathfrak{f}_{\tilde{\chi}})$. Then*

$$\begin{aligned}\frac{4^{\phi(p^n)/2}}{\alpha(\mathfrak{m}'\mathfrak{l}')C\big(\mathfrak{c}(\mathbf{f}),\mathbf{f}\big)}\,\mathcal{L}_{F_n}\left(\Phi_\psi^{n,k}\big|U(\mathfrak{m}'\mathfrak{l}'\mathfrak{p}^{-1}\mathfrak{l}_0^{-1})\right) &= \frac{\epsilon_{F_n}(\rho_k/F_n\otimes\psi)}{\alpha_p^{f(\rho_k/F_n\otimes\psi,\mathfrak{p})}\prod_{q|\Delta}\alpha_q^{\mathrm{ord}_q(A_{\tilde{\chi}})}} \\ \times \quad \prod_{v|\mathfrak{p}\mathfrak{l}_0}\frac{P_v(\rho_k/F_n\otimes\psi,\alpha_{q_v}^{-[f_{n,v}:\mathbb{F}_{q_v}]})}{P_v(\rho_k/F_n\otimes\psi^{-1},\alpha_{q_v}'^{-[f_{n,v}:\mathbb{F}_{q_v}]})} \quad &\times \quad \frac{L_S(1,E,\rho_k/F_n\otimes\psi^{-1})}{\Omega^{\mathrm{aut}}_{E/F_n}}.\end{aligned}$$

Proof. By its very definition,

$$P_v\big(\rho_k/F_n \otimes \psi, X\big) \;=\; \big(1-\psi^\dagger(v)\beta_n(v)X\big)\big(1-\psi^\dagger(v)\beta'_n(v)X\big).$$

Since $\alpha(v), \alpha'(v)$ are the roots of the polynomial $1-C(v,\mathbf{f})X+N_{F_n/\mathbb{Q}}(v)X^2$, clearly $\alpha'(v)N_{F_n/\mathbb{Q}}(v)^{-1} = \alpha(v)^{-1}$ and

$$\begin{aligned} &P_v(\rho_k/F_n\otimes\psi, \alpha(v)^{-1}) \;\; = \\ &\big(1-\psi^\dagger(v)\beta_n(v)\alpha'(v)N_{F_n/\mathbb{Q}}(v)^{-1}\big)\,\big(1-\psi^\dagger(v)\beta'_n(v)\alpha'(v)N_{F_n/\mathbb{Q}}(v)^{-1}\big). \end{aligned}$$

Applying a similar formula for $P_v(\rho_k/F_n\otimes\psi, \alpha'(v)^{-1})$, we obtain

$$\mathrm{Eul}_{\mathfrak{pl}_0}(\rho_k/F_n\otimes\psi^{-1},1) = \prod_{v|\mathfrak{pl}_0} P_v(\rho_k/F_n\otimes\psi,\alpha(v)^{-1})\,P_v(\rho_k/F_n\otimes\psi^{-1},\alpha(v)^{-1}).$$

The Euler factor of $\Psi(\mathbf{f}_{/F_n}, \mathbf{g}_{\rho_k/F_n}\otimes\psi, 1)$ at the primes in S is

$$\prod_{v|\mathfrak{pl}_0} P_v(\rho_k/F_n\otimes\psi,\alpha(v)^{-1})^{-1}\;\; P_v(\rho_k/F_n\otimes\psi,\alpha'(v)^{-1})^{-1}$$

therefore

$$\begin{aligned} &\mathrm{Eul}_{\mathfrak{pl}_0}(\rho_k/F_n\otimes\psi^{-1},1) \;\;.\;\; \Psi(\mathbf{f}_{/F_n}, \mathbf{g}_{\rho_k/F_n}\otimes\psi^{-1},1) \quad = \\ &\prod_{v|\mathfrak{pl}_0}\frac{P_v(\rho_k/F_n\otimes\psi,\alpha(v))}{P_v(\rho_k/F_n\otimes\psi^{-1},\alpha'(v))} \;\;\times\;\; \Psi_S(\mathbf{f}_{/F_n}, \mathbf{g}_{\rho_k/F_n}\otimes\psi^{-1},1). \end{aligned}$$

We showed earlier that $\alpha(v) = \alpha_{q_v}^{[f_{n,v}:\mathbb{F}_q]}$ and $\alpha'(v) = \alpha_{q_v}'^{[f_{n,v}:\mathbb{F}_q]}$ where q_v denotes the unique rational prime below v. This gives us the required factor

$$\prod_{v|\mathfrak{pl}_0}\frac{P_v(\rho_k/F_n\otimes\psi,\alpha_{q_v}^{-[f_{n,v}:\mathbb{F}_{q_v}]})}{P_v(\rho_k/F_n\otimes\psi^{-1},\alpha_{q_v}'^{-[f_{n,v}:\mathbb{F}_{q_v}]})} \;\;.$$

Further, as mentioned in Chapter 3 there is an equality

$$L_{\mathfrak{c}}(\det\rho_k/F_n\otimes\psi^{-1},2s-1)\;L(\mathbf{f}_E,\mathbf{g}_{\rho_k/F_n\otimes\psi^{-1}},s) \;=\; L(E,\rho_k/F_n\otimes\psi^{-1},s),$$

and completing the convolution we obtain

$$\Psi_S(\mathbf{f}_{/F_n},\,\mathbf{g}_{\rho_k/F_n\otimes\psi^{-1}},1) \;=\; (2\pi)^{-\phi(p^n)}\;L_S(E,\rho_k/F_n\otimes\psi^{-1},1).$$

By the definition of our automorphic period $\Omega^{\mathrm{aut}}_{E/F_n}$, we have

$$\frac{\Psi_S(\mathbf{f}_{/F_n},\, \mathbf{g}_{\rho_k/F_n\otimes\psi^{-1}},1)}{\big\langle \mathbf{f}_{/F_n},\mathbf{f}_{/F_n}\big\rangle_{\mathfrak{c}(\mathbf{f})}} \;=\; \frac{L_S(E,\,\rho_k/F_n\otimes\psi^{-1},1)}{\Omega^{\mathrm{aut}}_{E/F_n}}.$$

One concludes that

$$\begin{aligned}&\mathrm{Eul}_{\mathfrak{p}\mathfrak{l}_0}(\rho_k/F_n\otimes\psi^{-1},1) \quad\times\quad \frac{\Psi(\mathbf{f}_{/F_n},\mathbf{g}_{\rho_k/F_n}\otimes\psi^{-1},1)}{\big\langle \mathbf{f}_{/F_n},\mathbf{f}_{/F_n}\big\rangle_{\mathfrak{c}(\mathbf{f})}}\\ =\quad &\prod_{v|\mathfrak{p}\mathfrak{l}_0}\frac{P_v(\rho_k/F_n\otimes\psi,\alpha_{q_v}^{-[f_{n,v}:\mathbb{F}_{q_v}]})}{P_v(\rho_k/F_n\otimes\psi^{-1},\alpha_{q_v}'^{-[f_{n,v}:\mathbb{F}_{q_v}]})}\quad\times\quad\frac{L_S(E,\rho_k/F_n\otimes\psi^{-1},1)}{\Omega^{\mathrm{aut}}_{E/F_n}}\,.\end{aligned}$$

Applying Corollary 4.3.8 to this we obtain

$$\frac{(-4i)^{\phi(p^n)/2}}{\alpha(\mathfrak{m}'\mathfrak{l}')C\big(\mathfrak{c}(\mathbf{f}),\mathbf{f}\big)}\quad\mathcal{L}_{F_n}\Big(\Phi_\psi^{n,k}\big|U(\mathfrak{m}'\mathfrak{l}'\mathfrak{p}^{-1}\mathfrak{l}_0^{-1})\Big)\;=\;\frac{N_{F_n/\mathbb{Q}}(\mathfrak{c}(\mathbf{g}_{\rho_k/F_n\otimes\psi})\mathfrak{d}_{F_n}^2)^{1/2}}{\alpha(\mathfrak{c}(\mathbf{g}_{\rho_k/F_n\otimes\psi^{-1}}))}\;\times$$

$$\Lambda(\mathbf{g}_{\rho_k/F_n\otimes\psi^{-1}})\;\times\;\prod_{v|\mathfrak{p}\mathfrak{l}_0}\frac{P_v(\rho_k/F_n\otimes\psi,\alpha_{q_v}^{-[f_{n,v}:\mathbb{F}_{q_v}]})}{P_v(\rho_k/F_n\otimes\psi^{-1},\alpha_{q_v}'^{-[f_{n,v}:\mathbb{F}_{q_v}]})}\;\times\;\frac{L_S(E,\rho_k/F_n\otimes\psi^{-1},1)}{\Omega^{\mathrm{aut}}_{E/F_n}}\;.$$

Then using Lemmas 4.2.3 and 4.4.1 to convert the $\Lambda(\mathbf{g})$ and $\alpha(\mathfrak{c}(\mathbf{g}))$ terms respectively, we arrive at the desired result. □

4.5 The Kummer Congruences

Let $S=\mathrm{supp}(\mathfrak{p}\mathfrak{l}_0)$, and ψ be a character of $\mathcal{G}_n=\mathrm{Gal}(F_{n,S}^{\mathrm{ab}}/F_n)$. Consider the algebraic distribution on $\mathcal{G}_n$ given by

$$\int_{x\in\mathcal{G}_n}\psi(x)d\mu(x)\;:=\;\frac{4^{\phi(p^n)/2}}{\alpha(\mathfrak{m}'\mathfrak{l}')C\big(\mathfrak{c}(\mathbf{f}),\mathbf{f}\big)}\quad\mathcal{L}_{F_n}\Big(\Phi_\psi^{n,k}\big|U(\mathfrak{m}'\mathfrak{l}'\mathfrak{p}^{-1}\mathfrak{l}_0^{-1})\Big)$$

where we put

$$\begin{aligned}\Phi_\psi^{n,k}\quad&=\quad\Phi^{n,k}(\rho_k/F_n\otimes\psi,\,\mathfrak{c}(\mathbf{f}_{/F_n})\mathfrak{m}'\mathfrak{l}')\\ &=\quad(\mathbf{g}_{\rho_k/F_n\otimes\psi})\times E_1\Big(0,\,\mathfrak{c}(\mathbf{f}_{/F_n})\mathfrak{m}'\mathfrak{l}',\,(\mathrm{Res}_{F_n}\det\rho_k)^{\dagger\,-1}\otimes\psi^{\dagger\,-2}\Big)\end{aligned}$$

as in the previous section.

Proposition 4.5.1. *The distribution μ is a bounded p-adic measure on $\mathcal{G}_n$.*

Proof. To prove this, we need to show there exists a fixed constant $B \in \mathbb{Z}$ with the following property: for any set of coefficients $b_\psi \in \mathbb{C}_p$ (with only finitely many b_ψ non-zero) satisfying

$$\sum_\psi b_\psi \ \psi(x) \ \in \ p^m \mathcal{O}_{\mathbb{C}_p}$$

for all $x \in \mathcal{G}_n$, we have

$$\sum_\psi B \ b_\psi \int_{x \in \mathcal{G}_n} \psi(x) d\mu(x) \ \in \ p^m \mathcal{O}_{\mathbb{C}_p}.$$

Here the sums range over all continuous characters ψ of $\mathcal{G}_n$.

Using Atkin-Lehner theory, it can be shown that the linear functional $\mathcal{L}_{F_n}$ decomposes into a finite linear combination of the Fourier coefficients. So there exist finitely many ideals $\mathfrak{n}_i$ and fixed algebraic numbers $l(\mathfrak{n}_i) \in \overline{\mathbb{Q}}$ such that

$$\mathcal{L}_{F_n}(\Theta) = \sum_i C(\mathfrak{n}_i, \Theta) l(\mathfrak{n}_i)$$

for all $\Theta \in \mathcal{M}_2(\mathfrak{c}_0)$. Let us put

$$u = \frac{4^{\phi(p^n)/2}}{C\big(\mathfrak{c}(\mathbf{f}), \mathbf{f}\big)\alpha(\mathfrak{m}'\mathfrak{l}')}$$

which is a p-adic unit. Then for any $B \in \mathbb{Z}$ we have

$$\begin{aligned}
\sum_\psi B\, b_\psi \int_{x \in \mathcal{G}_n} \psi(x) d\mu(x) &= uB \sum_\psi b_\psi \ \mathcal{L}_{F_n}\left(\Phi_\psi^{n,k} \big| U(\mathfrak{m}'\mathfrak{l}'\mathfrak{p}^{-1}\mathfrak{l}_0^{-1})\right) \\
&= uB \sum_\psi b_\psi \sum_i C(\mathfrak{n}_i, \Phi_\psi^{n,k} \big| U(\mathfrak{m}'\mathfrak{l}'\mathfrak{p}^{-1}\mathfrak{l}_0^{-1})) l(\mathfrak{n}_i) \\
&= u \sum_i \left(\sum_\psi b_\psi \, C(\mathfrak{n}_i \mathfrak{p} \mathfrak{l}_0 \mathfrak{m}'^{-1} \mathfrak{l}'^{-1}, \Phi_\psi^{n,k}) \right) B\, l(\mathfrak{n}_i).
\end{aligned}$$

So, if we choose $B \in \mathbb{Z}$ so that $l(\mathfrak{n}_i)\, B \in \mathcal{O}_{\mathbb{C}_p}$ for all i, we see that it suffices to prove $\sum_\psi b_\psi \, C(\mathfrak{n}, \Phi_\psi^{n,k}) \ \in \ p^m \mathcal{O}_{\mathbb{C}_p}$ for all $\mathfrak{n}$.

From Corollary 4.3.8, we know that the λ-component of $\Phi_\psi^{n,k}$ has Fourier coeffi-

cients

$$\begin{aligned}\phi^{n,k}_{\psi,\lambda}(\xi) &= \sum_{\xi=\xi_1+\xi_2} \sum_{\substack{\mathfrak{a}\lhd\mathcal{O}_K,\\ \mathfrak{a}\bar{\mathfrak{a}}=\xi_1\tilde{t}_\lambda^{-1}}} (\chi^\dagger_{\rho_k}\circ N_{K_n/K_k})(\mathfrak{a})\,\psi^\dagger(\xi_1\tilde{t}_\lambda^{-1}) \\ &\qquad \sum_{\substack{\tilde{\xi}_2=\tilde{b}\tilde{c},\\ c\in\mathcal{O}_{F_n},\\ b\in\tilde{t}_\lambda}} \Big((\det\rho_k)^\dagger\circ N_{F_n/F_k}\Big)^{-1}(\tilde{c})\,\psi^\dagger(\tilde{c})^{-2}.\end{aligned}$$

Recall that $C(\mathfrak{n},\Phi^{n,k}_\psi) = N_{F_n/\mathbb{Q}}(\tilde{t}_\lambda)^{-1}\phi^{n,k}_{\psi,\lambda}(\xi)$ when $\mathfrak{n}=\xi\tilde{t}_\lambda^{-1}$. Therefore

$$\begin{aligned}\sum_\psi b_\psi\, C(\mathfrak{n},\Phi^{n,k}_\psi) &= N_{F_n/\mathbb{Q}}(\tilde{t}_\lambda)^{-1}\sum_\psi b_\psi \sum_{\xi_1,\xi_2}\sum_{\mathfrak{a}}(\chi^\dagger_{\rho_k}\circ N_{K_n/K_k})(\mathfrak{a})\,\psi^\dagger(\xi_1\tilde{t}_\lambda^{-1}) \\ &\qquad \sum_c \Big((\det\rho_k)^\dagger\circ N_{F_n/F_k}\Big)^{-1}(\tilde{c})\,\psi^\dagger(\tilde{c})^{-2} \\ &= N_{F_n/\mathbb{Q}}(\tilde{t}_\lambda)^{-1}\sum_{\xi_1,\xi_2}\sum_{\mathfrak{a}}(\chi^\dagger_{\rho_k}\circ N_{K_n/K_k})(\mathfrak{a}) \\ &\qquad \sum_c \Big((\det\rho_k)^\dagger\circ N_{F_n/F_k}\Big)^{-1}(\tilde{c})\,\left(\sum_\psi b_\psi\ \psi^\dagger(\xi_1\tilde{t}_\lambda^{-1}\tilde{c}^{-2})\right).\end{aligned}$$

By assumption, $\sum_\psi b_\psi\ \psi^\dagger(\xi_1\tilde{t}_\lambda^{-1}\tilde{c}^{-2}) \in p^m\mathcal{O}_{\mathbb{C}_p}$, and t_λ is always chosen so that $N_{F_n/\mathbb{Q}}(\tilde{t}_\lambda)$ is prime to p. Therefore $\sum_\psi b_\psi\, C(\mathfrak{n},\Phi^{n,k}_\psi)\in p^m\mathcal{O}_{\mathbb{C}_p}$. □

Theorem 4.5.2. *If the base change $\mathbf{f}_{/F_n}$ of f_E to the field F_n is not congruent modulo $\mathfrak{p}$ to a distinct element of $\mathcal{M}_2(\mathfrak{c}(\mathbf{f}_{/F_n}))$, then there exists an abelian p-adic L-function $\mathcal{L}_{p,\Delta}(E,\rho_k/F_n,\boldsymbol{\alpha})$ in $\mathcal{O}_{\mathbb{C}_p}[[\mathcal{G}_n]]$ interpolating the special values*

$$\begin{aligned}&\frac{\epsilon_{F_n}(\rho_k/F_n\otimes\psi)}{\alpha_p^{f(\rho_k/F_n\otimes\psi,\mathfrak{p})}\prod_{q|\Delta}\alpha_q^{\mathrm{ord}_q(A_{\tilde{\chi}})}} \\ \times\quad &\prod_{v|\mathfrak{p}\mathfrak{l}_0}\frac{P_v(\rho_k/F_n\otimes\psi,\alpha_{q_v}^{-[f_{n,v}:\mathbb{F}_{q_v}]})}{P_v(\rho_k/F_n\otimes\psi^{-1},\alpha_{q_v}'^{-[f_{n,v}:\mathbb{F}_{q_v}]})}\quad\times\quad\frac{L_S(1,E,\rho_k/F_n\otimes\psi^{-1})}{\Omega^{\mathrm{aut}}_{E/F_n}}\end{aligned}$$

at all finite characters ψ of $\mathcal{G}_n=\mathrm{Gal}(F^{\mathrm{ab}}_{n,S}/F_n)$.

Here $\tilde{\chi}=\mathrm{Res}_{K_n}(\chi_{\rho_k}\otimes\psi)$, $A_{\tilde{\chi}}=N_{K_n/\mathbb{Q}}(\mathfrak{f}_{\tilde{\chi}})$, and $\boldsymbol{\alpha}=(\alpha_{q_1},...,\alpha_{q_r})$ denotes our choice of α_q for each prime $q|\Delta$.

Proof. The measure μ on $\mathcal{G}_n$ corresponds to an element

$$\mathcal{L}_{p,\Delta}(E, \rho_k/F_n, \boldsymbol{\alpha}) \ \in \ \mathcal{O}_{\mathbb{C}_p}[[\mathcal{G}_n]] \otimes_{\mathbb{Z}} \mathbb{Q}$$

which has special values $\int_{x\in\mathcal{G}_n} \psi(x)d\mu(x)$ at all characters ψ of $\mathcal{G}_n$. We will show that these special values are in fact p-integral. We have

$$\begin{aligned}\int_{x\in\mathcal{G}_n} \psi(x)d\mu(x) &= \frac{4^{\phi(p^n)/2}}{C\big(\mathfrak{c}(\mathbf{f}),\mathbf{f}\big)\alpha(\mathfrak{m}'\mathfrak{l}')} \quad \mathcal{L}_{F_n}\left(\Phi_{\psi}^{n,k}\big|U(\mathfrak{m}'\mathfrak{l}'\mathfrak{p}^{-1}\mathfrak{l}_0^{-1})\right) \\ &= (\ p\text{-adic unit }) \times \mathrm{Eul}_{\mathfrak{p}\mathfrak{l}_0}(\rho_k/F_n \otimes \psi^{-1}, 1) \\ &\quad \times \epsilon_{F_n}(\rho_{k/F_n} \otimes \psi) \ \times \ \frac{\Psi(\mathbf{f}_{/F_n}, (\mathbf{g}_{\rho_k/F_n\otimes\psi})^{\iota}, 1)}{\big\langle \mathbf{f}_{/F_n}, \mathbf{f}_{/F_n}\big\rangle_{\mathfrak{c}(\mathbf{f})}}\end{aligned}$$

by Corollary 4.3.8. Recall that

$$\begin{aligned}\mathrm{Eul}_{\mathfrak{p}\mathfrak{l}_0}(\rho_k/F_n \otimes \psi^{-1}, 1) &= \prod_{v|\mathfrak{p}\mathfrak{l}_0} P_v(\rho_k/F_n \otimes \psi, \alpha_{q_v}^{-[f_{n,v}:\mathbb{F}_{q_v}]}) \\ &\quad \times \ P_v(\rho_k/F_n \otimes \psi^{-1}, \alpha_{q_v}^{-[f_{n,v}:\mathbb{F}_{q_v}]}).\end{aligned}$$

The polynomials $P_{\mathfrak{q}}(\rho_k/F_n \otimes \psi^{-1}, X)$ all have p-integral coefficients, and α_q is a p-unit for any $q \neq p$, hence

$$P_{\mathfrak{q}}\big(\rho_k/F_n \otimes \psi, \alpha_q^{-[f_{n,\mathfrak{q}}:\mathbb{F}_q]}\big) \in \mathcal{O}_{\mathbb{C}_p}$$

when $\mathfrak{q} \neq \mathfrak{p}$. Also α_p was chosen to be the unit root, thus we also have

$$P_{\mathfrak{p}}(\rho_k/F_n \otimes \psi, \alpha_p^{-1}) \in \mathcal{O}_{\mathbb{C}_p}.$$

The same applies when ψ is replaced by ψ^{-1}, thus $\mathrm{Eul}_{\mathfrak{p}\mathfrak{l}_0}(\rho_k/F_n\otimes\psi^{-1}, 1)$ is p-integral. Lastly, using Theorem 4.2.1 with $\rho = (\rho_k/F_n) \otimes \psi$ yields

$$\epsilon_{F_n}(\rho_{k/F_n} \otimes \psi) \ \frac{\Psi(\mathbf{f}_{/F_n}, (\mathbf{g}_{\rho_k/F_n\otimes\psi})^{\iota}, s)}{\big\langle \mathbf{f}_{/F_n}, \mathbf{f}_{/F_n}\big\rangle_{\mathfrak{c}(\mathbf{f})}} \ \in \ \mathcal{O}_{\mathbb{C}_p}.$$

Therefore, all the special values of our p-adic L-function lie in $\mathcal{O}_{\mathbb{C}_p}$, so $\mathcal{L}_{p,\Delta}(E, \rho_k/F_n, \boldsymbol{\alpha}) \in \mathcal{O}_{\mathbb{C}_p}[[\mathcal{G}_n]]$. □

4.6 The Weak Form of Kato's Congruences

In this section we will use our distributions to prove a final set of congruences. We do this as evidence for the stronger congruences from Kato's paper [Kat05], which imply the existence of a non-abelian p-adic L-function.

For all $n \geq 0$, we write

$$a_n = \mathcal{L}_p(E, \rho_n/F_n) \ \in \ \mathbb{Z}_p[[U^{(n)}]]^\times$$

for the p-adic L-function defined in Theorem 4.1.1. It may be constructed from the element $\mathcal{L}_{p,\Delta}(E, \rho_k/F_n, \boldsymbol{\alpha})$ as we show in this section, and its integrality follows from Hypothesis **(I,n)**.

We then put $b_n = a_n/N_{0,n}(a_0)$ and $c_n = b_n/\phi(b_{n-1})$ as in Section 4.1. Ideally we want to prove that

$$\prod_{i=1}^{n} N_{i,n}(c_i)^{p^i} \equiv 1 \mod p^{2n}$$

for all $n \geq 1$. We are unable to prove this congruence modulo p^{2n}, but we will at least prove it modulo p^{n+1}; the result is a straightforward consequence of the following lemma.

Lemma 4.6.1. *Assume Hypothesess* **(I,n)** *and* **(II)** *hold true for an integer $n \geq 1$. For each $0 \leq i \leq n$, we have*

$$a_n \equiv N_{i,n}(a_i) \mod p\, \mathbb{Z}_p[[U^{(n)}]].$$

Remark 4.6.2. In fact, Lemma 4.6.1 is true even if Hypothesis **(II)** is false, but in this case both sides of the congruence are zero.

Recall that the 'automorphic' p-adic L-function $\mathcal{L}_{p,\Delta}(E, \rho_k/F_n, \boldsymbol{\alpha})$ is an element of $\mathcal{O}_{\mathbb{C}_p}[[\mathcal{G}_n]]$, but we abuse notation slightly and also write $\mathcal{L}_{p,\Delta}(E, \rho_i/F_n, \boldsymbol{\alpha})$ for its image under the projection

$$\mathcal{O}_{\mathbb{C}_p}[[\mathcal{G}_n]] \twoheadrightarrow \mathcal{O}_{\mathbb{C}_p}[[U^{(n)}]].$$

We need to relate this to the motivic p-adic L-function $a_i = \mathcal{L}_p(E, \rho_i)$. By defnition, the element $N_{i,n}(a_i) \in \mathcal{O}_{\mathbb{C}_p}[[U^{(n)}]]$ has special values

$$\begin{aligned}\psi(N_{i,n}(a_i)) \;=\; \frac{\epsilon_{F_n}(\rho_i/F_n \otimes \psi)_{\mathfrak{p}}}{\alpha_p^{f(\rho_i/F_n \otimes \psi, \mathfrak{p})}} \;&\times\; \frac{P_{\mathfrak{p}}(\rho_i/F_n \otimes \psi, \alpha_p^{-[F_n:\mathbb{Q}]})}{P_{\mathfrak{p}}(\rho_i/F_n \otimes \psi^{-1}, \alpha_p^{'-[F_n:\mathbb{Q}]})} \\ &\times\; \frac{L_S(1, E, \rho_i/F_n \otimes \psi)}{(\Omega_E^+ \Omega_E^-)^{\phi(p^n)/2}}\end{aligned}$$

at all finite-order characters ψ of $U^{(n)}$. A formula for the special values of $\mathcal{L}_{p,\Delta}(E, \rho_k/F_n, \boldsymbol{\alpha})$ was given in Theorem 4.5.2, but now we have projected it down to $\mathcal{O}_{\mathbb{C}_p}[[U^{(n)}]]$ we may simplify it.

Lemma 4.6.3. *Suppose ψ is a character of $U^{(n)}$, and v is a finite prime of F_n which divides Δ. Then the local polynomial $P_v(\rho_k/F_n \otimes \psi, T)$ is trivial unless $k = 0$.*

Proof. The representation $\rho_k/F_n \otimes \psi$ factors through M/F_n for some field M that depends on the character ψ. Let us write $\bar{v}$ for a place of M dividing v and $I_{\bar{v}} \subseteq \mathrm{Gal}(M/F_n)_{\bar{v}}$ for the corresponding inertia subgroup. Then by definition $P_v(\rho_k/F_n \otimes \psi, X)$ is the characteristic polynomial of Frob_v^{-1} acting on the inertia invariant subspace $(\rho_k/F_n \otimes \psi)^{I_{\bar{v}}}$.

However, ψ factors through $U^{(n)}$ and so ψ is only ramified above p. Since $(v, p) = 1$ we have $\mathrm{Res}_{I_{\bar{v}}} \psi = \mathbf{1}$ and

$$(\rho_k/F_n \otimes \psi)^{I_{\bar{v}}} = (\rho_k/F_n)^{I_{\bar{v}}}.$$

Because ρ_k/F_n is induced from a character χ_{ρ_k} over K_n, and v is unramified in K_n/F_n, one easily checks that $\mathrm{Res}_{I_{\bar{v}}} \rho_k/F_n$ decomposes into two copies of χ_{ρ_k}. If $k > 0$, χ_{ρ_k} is non-trivial and thus $\chi_{\rho_k}^{I_{\bar{v}}} = 0$. This implies $(\rho_k/F_n)^{I_{\bar{v}}} = 0$ which completes the proof. □

Having established Lemma 4.6.3, we can simplify our Euler factor when ψ is a character of $U^{(n)}$:

$$\prod_{v|\mathfrak{p}\mathfrak{l}_0} \frac{P_v(\rho_k/F_n \otimes \psi, \alpha_{q_v}^{-[f_{n,v}:\mathbb{F}_{q_v}]})}{P_v(\rho_k/F_n \otimes \psi^{-1}, \alpha_{q_v}^{'-[f_{n,v}:\mathbb{F}_{q_v}]})} \;=\; \frac{P_{\mathfrak{p}}(\rho_k/F_n \otimes \psi, \alpha_p^{-[F_n:\mathbb{Q}]})}{P_{\mathfrak{p}}(\rho_k/F_n \otimes \psi^{-1}, \alpha_p^{'-[F_n:\mathbb{Q}]})}\,.$$

Comparing the special values of $N_{i,n}(a_i)$ and $\mathcal{L}_{p,\Delta}(E,\rho_i/F_n,\boldsymbol{\alpha})$, one finds

$$N_{i,n}(a_i) \;=\; \frac{\Omega^{\mathrm{aut}}_{E/F_n}}{(\Omega^+_E\Omega^-_E)^{\phi(p^n)/2}} \;\times\; \gamma_E^{i,n} \;\times\; \mathcal{L}_{p,\Delta}(E,\rho_i/F_n,\boldsymbol{\alpha})$$

where $\gamma_E^{i,n} \in \mathcal{O}_{\mathbb{C}_p}[[U^{(n)}]]$ satisfies

$$\psi(\gamma_E^{i,n}) \;=\; \frac{\prod_{q|\Delta}\alpha_q^{p^n-p^{n-1}}}{\prod_{v\neq\mathfrak{p}}\epsilon_{F_{n,v}}(\rho_i/F_n\otimes\psi^{-1})}.$$

Let $\mathfrak{M}_{\mathbb{C}_p}$ denote the maximal ideal of $\mathcal{O}_{\mathbb{C}_p}$.

Claim ($\star$): $\quad \gamma_E^{0,n} \equiv \gamma_E^{1,n} \equiv \ldots \equiv \gamma_E^{n,n} \mod \mathfrak{M}_{\mathbb{C}_p}[[U^{(n)}]] \quad$ for each $n \in \mathbb{N}$.

We will prove this claim at the end of this section (c.f. Lemma 4.6.8).

Remark 4.6.4. One can check easily that the element $\gamma_E^{0,n}$ is a unit of $\mathcal{O}_{\mathbb{C}_p}[[U^{(n)}]]$, so Claim ($\star$) implies that each $\gamma_E^{i,n}$ is a unit. In particular we have an integral p-adic L-function

$$\mathcal{L}_p^{\mathrm{aut}}(E,\rho_i/F_n) \;:=\; \gamma_E^{i,n} \;\times\; \mathcal{L}_{p,\Delta}(E,\rho_i/F_n,\boldsymbol{\alpha}) \;\in\; \mathcal{O}_{\mathbb{C}_p}[[U^{(n)}]]$$

which has the interpolation property claimed in Theorem 4.1.1.

Definition 4.6.5. *We define the period error term associated to E and the field $F_n = \mathbb{Q}(\mu_{p^n})^+$ to be*

$$\mathbf{Err}_{F_n}(E) \;:=\; \frac{\big(\Omega^+_E\Omega^-_E\big)^{\phi(p^n)/2}}{\Omega^{\mathrm{aut}}_{E/F_n}} \;\in\; \overline{\mathbb{Q}}.$$

So we may write

$$\mathbf{Err}_{F_n}(E) \;\times\; N_{i,n}\big(\mathcal{L}(E,\rho_i)\big) \;=\; \gamma_E^{i,n} \;\times\; \mathcal{L}_{p,\Delta}(E,\rho_i/F_n,\boldsymbol{\alpha}).$$

If Hypothesis **(I,** n**)** holds then the norm of the motivic p-adic L-function $\mathcal{L}(E,\rho_i)$ is p-integral; further, under Hypothesis **(II)** the μ-invariant of $N_{0,n}\big(\mathcal{L}(E,\rho_0)\big)$ is trivial. Since $\gamma_E^{0,n}$ is a unit, we have

$$\mathrm{ord}_p\big(\mathbf{Err}_{F_n}(E)\big) \;=\; \mu\text{-invariant of } \mathcal{L}_{p,\Delta}(E,\rho_0/F_n,\boldsymbol{\alpha}).$$

Lemma 4.6.6. *For all $n \in \mathbb{N}$ and $0 \leq i \leq n$,*

$$\mathcal{L}_{p,\Delta}(E, \rho_i/F_n, \boldsymbol{\alpha}) \;\equiv\; \mathcal{L}_{p,\Delta}(E, \rho_n/F_n, \boldsymbol{\alpha}) \mod \mathbf{Err}_{F_n}(E)\,.\,\mathfrak{M}_{\mathbb{C}_p}[[U^{(n)}]].$$

Proof. Let us write $H_n = \mathrm{Gal}\left(K_n(\sqrt[p^n]{\Delta})/K_n\right)$, so that $\mathrm{Res}_{K_n}\chi_{\rho_i}$ factors through H_n for each i. We claim that there is a bounded measure on the group $H_n \times U^{(n)}$ given by

$$(\chi, \psi) \;\longmapsto\; \psi\left(\mathcal{L}_{p,\Delta}(E, \mathrm{Ind}_{K_n}^{F_n}\chi, \boldsymbol{\alpha})\right)$$

for any pair of characters $\chi : H_n \to \mathbb{C}^\times$ and $\psi : U^{(n)} \to \mathbb{C}^\times$.

If one accepts this claim, the result follows easily: we know that the μ-invariant of this measure is at least $\mathrm{ord}_p\big(\mathbf{Err}_{F_n}(E)\big)$, meaning that all its power series coefficients lie in $\mathbf{Err}_{F_n}(E).\mathcal{O}_{\mathbb{C}_p}$. Since each character $\mathrm{Res}_{K_n}\chi_{\rho_i}$ takes values in μ_{p^∞}, we have a congruence

$$\mathrm{Res}_{K_n}\chi_{\rho_i} \;\equiv\; \chi_n \mod \mathfrak{M}_{\mathbb{C}_p};$$

so the values of this measure at $(\mathrm{Res}_{K_n}\chi_{\rho_i}, \psi)$ and (χ_{ρ_n}, ψ) must be congruent modulo $\mathbf{Err}_{F_n}(E).\mathfrak{M}_{\mathbb{C}_p}$, i.e.

$$\psi\Big(\mathcal{L}_{p,\Delta}(E, \rho_i/F_n, \boldsymbol{\alpha})\Big) \;\equiv\; \psi\Big(\mathcal{L}_{p,\Delta}(E, \rho_n, \boldsymbol{\alpha})\Big) \mod \mathbf{Err}_{F_n}(E).\mathfrak{M}_{\mathbb{C}_p}$$

for all ψ, which is precisely the assertion of the lemma.

Now we will prove the claim: we must check the appropriate Kummer congruences for the values of this distribution. We have already checked them as ψ varies (in the proof of Proposition 4.5.1), so it suffices to prove the following: for any coefficients $b_\chi \in \mathbb{C}_p$ satisfying

$$\sum_{\chi \in \widehat{H}_n} b_\chi\,\chi(h) \;\in\; p^m\mathcal{O}_{\mathbb{C}_p}$$

for all $h \in H_n$, we have

$$\sum_{\chi \in \widehat{H}_n} B\,b_\chi\,\psi\left(\mathcal{L}_{p,\Delta}(E, \mathrm{Ind}_{K_n}^{F_n}\chi, \boldsymbol{\alpha})\right) \;\in\; p^m\mathcal{O}_{\mathbb{C}_p}.$$

for any character ψ of $U^{(n)}$, where $B \in \mathbb{Z}$ is fixed.

We prove this in the same way that we proved Proposition 4.5.1. By Panchishkin's Atkin-Lehner theory argument, we can write these values as linear combinations of the Fourier coefficients of a Hilbert modular form:

$$\psi\left(\mathcal{L}_{p,\Delta}(E, \mathrm{Ind}_{K_n}^{F_n}\chi, \boldsymbol{\alpha})\right) \;=\; \sum_{\mathfrak{m}} C(\mathfrak{m}, \Phi_{\chi,\psi})\; l(\mathfrak{m})$$

for algebraic numbers $l(\mathfrak{m})$, almost all zero. Therefore it suffices to prove the Kummer congruence for the Fourier coefficients $C(\mathfrak{m}, \Phi_{\chi,\psi})$. The Hilbert modular form $\Phi_{\chi,\psi}$ is given by

$$\Phi_{\chi,\psi} \;:=\; \mathbf{g}_{\rho\otimes\psi} \;\times\; E_1\Big(0,\, \mathfrak{c}(\mathbf{f}_{/F_n})\mathfrak{m}'\mathfrak{l}',\, (\det\rho)^{\dagger\,-1}\otimes\psi^{\dagger\,-2}\Big)$$

where $\rho = \mathrm{Ind}_{K_n}^{F_n}\chi$. From [Pan91] we know that that its Fourier coefficients are

$$\begin{aligned} C(\mathfrak{m}, \Phi_{\chi,\psi}) \;&=\; N_{F_n/\mathbb{Q}}(\tilde{t}_\lambda)^{-1} \sum_{\xi=\xi_1+\xi_2} \sum_{\substack{\mathfrak{a}\lhd\mathcal{O}_K,\\ \mathfrak{a}\bar{\mathfrak{a}} \,=\, \xi_1\tilde{t}_\lambda^{-1}}} \chi^\dagger(\mathfrak{a})\,\psi^\dagger(\xi_1\tilde{t}_\lambda^{-1}) \\ &\times \sum_{\substack{\tilde{\xi_2}=\tilde{b}\tilde{c},\\ c\in\mathcal{O}_{F_n},\\ b\in\tilde{t}_\lambda}} (\det\rho)^\dagger(\tilde{c})^{-1}\,\psi^\dagger(\tilde{c})^{-2}. \end{aligned}$$

where $\mathfrak{m} = \xi\tilde{t}_\lambda^{-1}$. Recall from Section 3.11 that the character $\det\rho$ is given on ideals by

$$(\det\rho)^\dagger(\mathfrak{b}) \;=\; \theta_{K_n/F_n}(\mathfrak{b})\;\chi^\dagger(\mathfrak{b}\mathcal{O}_{K_n}),$$

so we may write

$$C(\mathfrak{m}, \Phi_{\chi,\psi}) \;=\; N_{F_n/\mathbb{Q}}(\tilde{t}_\lambda)^{-1} \sum_{\xi_1,\mathfrak{a},c} \psi^\dagger(\xi_1\tilde{t}_\lambda^{-1}\,\tilde{c}^{-2})\;\theta_{K_n/F_n}(\tilde{c})\;\chi^\dagger\big(\mathfrak{a}(c\,\mathcal{O}_{K_n})^{-1}\big).$$

Therefore we have

$$\begin{aligned} \sum_\chi b_\chi\, C(\mathfrak{m}, \Phi_{\chi,\psi}) \;&=\; N_{F_n/\mathbb{Q}}(\tilde{t}_\lambda)^{-1} \sum_{\xi_1,\mathfrak{a},c} \psi^\dagger(\xi_1\tilde{t}_\lambda^{-1}\,\tilde{c}^{-2})\;\theta_{K_n/F_n}(\tilde{c}) \\ &\times \sum_\chi b_\chi\,\chi^\dagger\big(\mathfrak{a}(c\,\mathcal{O}_{K_n})^{-1}\big). \end{aligned}$$

By assumption, $\sum_\chi b_\chi \, \chi^\dagger\big(\mathfrak{a}(c\,\mathcal{O}_{K_n})^{-1}\big)$ lies in $p^m\mathcal{O}_{\mathbb{C}_p}$, and $N_{F_n/\mathbb{Q}}(\tilde{t}_\lambda)$ is always a p-adic unit; so we conclude

$$\sum_\chi b_\chi \, C(\mathfrak{m}, \Phi_{\chi,\psi}) \;\; \in \;\; p^m\mathcal{O}_{\mathbb{C}_p}.$$

for any choice of ψ. This implies the full Kummer congruences for this measure, and proves the claim. □

Now we are able to prove Lemma 4.6.1.

Proof of Lemma 4.6.1: Recall that we want to show

$$N_{i,n}(a_i) \;\equiv\; a_n \mod p\,\mathbb{Z}_p[[U^{(n)}]].$$

for all $0 \le i \le n$, and that $N_{i,n}(a_i)$ is related to $\mathcal{L}_{p,\Delta}(E, \rho_i/F_n, \boldsymbol{\alpha})$ by

$$N_{i,n}(a_i) \;=\; \mathbf{Err}_{F_n}(E)^{-1} \,\times\, \gamma_E^{i,n} \,\times\, \mathcal{L}_{p,\Delta}(E, \rho_i/F_n, \boldsymbol{\alpha}).$$

By Lemma 4.6.6 we know that

$$\mathbf{Err}_{F_n}(E)^{-1} \;\mathcal{L}_{p,\Delta}(E, \rho_i/F_n, \boldsymbol{\alpha}) \mod \mathfrak{M}_{\mathbb{C}_p}[[U^{(n)}]]$$

is independent of i, and Claim $(\star)$ asserts that

$$\gamma_E^{i,n} \;\equiv\; \gamma_E^{n,n} \mod \mathfrak{M}_{\mathbb{C}_p}[[U^{(n)}]]\,,$$

so we have

$$N_{i,n}(\mathcal{L}_p(E, \rho_i)) \;\equiv\; \mathcal{L}_p(E, \rho_n) \mod \mathfrak{M}_{\mathbb{C}_p}[[U^{(n)}]].$$

This is almost the congruence we require, except that we need it modulo p rather than modulo $\mathfrak{M}_{\mathbb{C}_p}$. To complete the proof we use the algebraicity result of Bouganis and V. Dokchitser (Theorem 4.2 of [BD07]) which states that

$$\epsilon_{F_n}(\rho) \;\; \frac{L_S(1, E, \rho)}{(\Omega_E^+)^{\dim \rho^+}(\Omega_E^-)^{\dim \rho^-}} \;\in\; \mathbb{Q}(\rho)$$

where $\mathbb{Q}(\rho)$ denotes the field of definition of the Artin representation ρ. However as V. Dokchitser comments in [Dok05], the representations ρ_i may all be realised over $\mathbb{Q}$, so we have

$$\mathcal{L}_p(E,\rho_i) \ \in \ \mathbb{Z}_p[[U^{(i)}]] \otimes \mathbb{Q} \quad \text{for all } i.$$

Further, our integrality result (Theorem 4.2.1) implies that the special values of

$$\mathcal{L}_p(E,\rho_i) \ = \ \frac{\Omega^{\mathrm{aut}}_{E/F_i}}{(\Omega^+_E\Omega^-_E)^{\phi(p^i)/2}} \ \times \ \gamma_E^{i,i} \ \times \ \mathcal{L}_{p,\Delta}(E,\rho_i,\boldsymbol{\alpha})$$

are all p-integral; we deduce that

$$\mathcal{L}_p(E,\rho_i) \ \in \ \mathbb{Z}_p[[U^{(i)}]] \quad \text{for all } i.$$

In conclusion

$$N_{i,n}(\mathcal{L}_p(E,\rho_i)) \equiv \mathcal{L}_p(E,\rho_n) \mod \left(\mathfrak{M}_{\mathbb{C}_p}[[U^{(n)}]] \cap \mathbb{Z}_p[[U^{(n)}]]\right),$$

i.e.

$$N_{i,n}(\mathcal{L}_p(E,\rho_i)) \equiv \mathcal{L}_p(E,\rho_n) \mod p\,\mathbb{Z}_p[[U^{(n)}]]$$

which is the desired congruence. □

Having finally proved Lemma 4.6.1, it is straightforward to prove the main result of this section.

Theorem 4.6.7. *Let $a_n = \mathcal{L}_p(E,\rho_n/F_n)$ for all n, and write*

$$b_n = a_n/N_{0,n}(a_0) \quad \textit{and} \quad c_n = b_n/\phi(b_{n-1}).$$

Then the congruence

$$\prod_{i=1}^{n} N_{i,n}(c_i)^{p^i} \equiv 1 \mod p^{n+1}$$

holds for all $n \geq 1$.

Proof. From the definitions of c_i and b_i, this congruence can be rearranged into the form

$$\prod_{i=1}^{n} N_{i,n}(a_i \,.\, \phi \circ N_{0,i-1}(a_0))^{p^i} \equiv \prod_{i=1}^{n} N_{i,n}(\phi(a_{i-1}) \,.\, N_{0,i}(a_0))^{p^i} \mod p^{n+1}.$$

We prove this result by induction on n.

Base Case: When $n = 1$ we need to prove

$$(\phi(a_0) \,.\, a_1)^p \equiv (\phi(a_0) \,.\, N_{0,1}(a_0))^p \mod p^2.$$

First note that $x \equiv y \mod p$ implies $x^p \equiv y^p \mod p^2$, so it suffices to show

$$a_1 \equiv N_{0,1}(a_0) \mod p$$

which is a consequence of Lemma 4.6.1 (this also proves Theorem 4.1.3).

Induction Step: Our induction hypothesis is

$$\prod_{i=1}^{n-1} N_{i,n-1}(a_i \,.\, \phi \circ N_{0,i-1}(a_0))^{p^i} \equiv \prod_{i=1}^{n-1} N_{i,n-1}(\phi(a_{i-1}) \,.\, N_{0,i}(a_0))^{p^i} \mod p^n.$$

Note that if $x_n \equiv y_n \mod p^r$ for $x_n, y_n \in \mathbb{Z}_p[[U^{(n)}]]$, then

$$N_{n-1,n}(x_n) \equiv N_{n-1,n}(y_n) \mod p^{r+1}.$$

Therefore our induction hypothesis implies

$$\begin{aligned} & N_{n-1,n}\left(\prod_{i=1}^{n-1} N_{i,n-1}(a_i \,.\, \phi \circ N_{0,i-1}(a_0))^{p^i}\right) \\ \equiv \quad & N_{n-1,n}\left(\prod_{i=1}^{n-1} N_{i,n-1}(\phi(a_{i-1}) \,.\, N_{0,i}(a_0))^{p^i}\right) \mod p^{n+1} \end{aligned}$$

which can be rewritten as

$$(\dagger) \quad \prod_{i=1}^{n-1} N_{i,n}(a_i \,.\, \phi \circ N_{0,i-1}(a_0))^{p^i} \equiv \prod_{i=1}^{n-1} N_{i,n}(\phi(a_{i-1}) \,.\, N_{0,i}(a_0))^{p^i} \mod p^{n+1}.$$

Now, from Lemma 4.6.1 we know

$$a_{n-1} \equiv N_{0,n-1}(a_0) \mod p$$

implying that

$$\phi(a_{n-1}) \equiv \phi(N_{0,n-1}(a_0)) \mod p.$$

Combining this with the congruence

$$a_n \equiv N_{0,n}(a_0) \mod p$$

(which also comes from Lemma 4.6.1), we obtain

$$N_{0,n}(a_0)\ \phi(a_{n-1}) \ \equiv\ a_n\ \phi(N_{0,n-1}(a_0)) \mod p.$$

Finally, raising both sides to the p^n-th power yields

$$(\ N_{0,n}(a_0)\ \phi(a_{n-1})\ )^{p^n} \ \equiv\ (\ a_n\ \phi(N_{0,n-1}(a_0))\ )^{p^n} \mod p^{n+1}.$$

This provides the factor at $i = n$; multiplying by the congruence (†) above we get

$$\prod_{i=1}^{n} N_{i,n}(a_i\,.\,\phi \circ N_{0,i-1}(a_0))^{p^i} \equiv \prod_{i=1}^{n} N_{i,n}(\phi(a_{i-1})\,.\,N_{0,i}(a_0))^{p^i} \mod p^{n+1}$$

which completes the induction step. □

It remains to prove Claim (⋆).

Lemma 4.6.8. *For each $n \geq 0$,*

$$\gamma_E^{0,n} \ \equiv\ \gamma_E^{1,n} \equiv ... \equiv\ \gamma_E^{n,n} \mod \mathfrak{M}_{\mathbb{C}_p}[[U^{(n)}]]$$

where $\gamma_E^{k,n} \in \mathcal{O}_{\mathbb{C}_p}[[U^{(n)}]]$ takes special values

$$\psi(\gamma_E^{k,n}) \ =\ \frac{\prod_{q|\Delta} \alpha_q^{p^n - p^{n-1}}}{\prod_{v \neq \mathfrak{p}} \epsilon_{F_{n,v}}(\rho_k/F_n \otimes \psi^{-1})}\ .$$

Proof. We will show that the special values of these elements are congruent modulo $\mathfrak{M}_{\mathbb{C}_p}$. Let $M_n = K_n(\sqrt[p^n]{\Delta})$, so that the representation ρ_k/F_n factors through $G = \mathrm{Gal}(M_n/F_n)$. We need to verify

$$\epsilon_{F_{n,v}}(\rho_k/F_n \otimes \psi) \ \equiv\ \epsilon_{F_{n,v}}(\rho_n \otimes \psi) \mod \mathfrak{M}_{\mathbb{C}_p}$$

for all places v of F_n such that $v|\Delta$. First we will show that suffices to prove the congruence

$$\epsilon_{K_{n,w}}(\mathrm{Res}_{K_n}\,\chi_{\rho_k} \otimes \psi) \ \equiv\ \epsilon_{K_{n,w}}(\chi_{\rho_n} \otimes \psi) \mod \mathfrak{M}_{\mathbb{C}_p}$$

for all places w above v.

Case 1: v splits in K_n/F_n.
Let $\bar{v}$ be a place of M_n above v; in this case, the decomposition group $G_{\bar{v}}$ is contained in $\mathrm{Gal}(M_n/K_n)$. Therefore, the representation splits:

$$\mathrm{Res}_{G_{\bar{v}}}(\rho_k/F_n \otimes \psi) \;\cong\; (\mathrm{Res}_{G_{\bar{v}}}\, \chi_{\rho_k} \otimes \psi) \,\oplus\, (\mathrm{Res}_{G_{\bar{v}}}\, \chi_{\rho_k} \otimes \psi)^{-1}.$$

Thus it suffices to check that the epsilon-factors of the characters themselves are congruent.

Case 2: v is inert in K_n/F_n.
In this case we apply the inductivity of local epsilon factors in degree zero (see [Tat79] (3.4.8)). This gives us

$$\frac{\epsilon_{F_{n,v}}(\rho_k/F_n \otimes \psi)}{\epsilon_{F_{n,v}}(\mathbf{1} \oplus \eta)} \;=\; \frac{\epsilon_{K_{n,w}}(\mathrm{Res}_{K_n}\, \chi_{\rho_k} \otimes \psi)}{\epsilon_{K_{n,w}}(\mathbf{1})}$$

where w is a prime of K_n above v, and η is the quadratic character of K_n/F_n, so in fact $\mathrm{Ind}_{K_n}^{F_n}\, \mathbf{1} = \mathbf{1} \oplus \eta$. It can be shown that the ratio $\epsilon_{F_n}(\mathbf{1} \oplus \eta)_v / \epsilon_{K_n}(\mathbf{1})_w$ is a p-adic unit. Therefore we may write

$$\begin{aligned} \epsilon_{F_{n,v}}(\rho_k/F_n \otimes \psi) &= \frac{\epsilon_{F_{n,v}}(\mathbf{1} \oplus \eta)}{\epsilon_{K_{n,w}}(\mathbf{1})} \;\times\; \epsilon_{K_{n,w}}(\mathrm{Res}_{K_n}\, \chi_{\rho_k} \otimes \psi)_w \\ &= (\,p\text{-adic unit}) \;\times\; \epsilon_{K_{n,w}}(\mathrm{Res}_{K_n}\, \chi_{\rho_k} \otimes \psi)\,, \end{aligned}$$

and we are again reduced to proving the congruence for the epsilon factors of the characters.

It will be enough to prove for each place $w|q$ that

$$\epsilon_{K_{n,w}}(\chi) \;\equiv\; \epsilon_{K_{n,w}}(\chi') \mod \mathfrak{M}_{\mathbb{C}_p}$$

where χ and χ' are two characters over K_n, both tamely ramified at w and satisfying $\chi \equiv \chi' \mod \mathfrak{M}_{\mathbb{C}_p}$. Recall that these local ϵ-factors depend on a choice of

Haar measure dx and a choice of additive character $\tau : (K_{n,w}, +) \longrightarrow \mathbb{C}^\times$. Then $\epsilon_{K_{n,w}}(\chi) = \epsilon_{K_{n,w}}(\chi, \tau, dx)$ in the notation of Tate [Tat79], and we have the Gauss sum expression

$$\epsilon_{K_{n,w}}(\chi, \tau, dx) \;=\; \chi(\pi^{a(\chi)+n(\tau)})\, q^{n(\tau)-\delta/2} \sum_{u \in \mathcal{O}_w^\times \bmod \pi^{a(\chi)}} \chi(u)\; \tau\left(\frac{u}{\pi^{a(\chi)+n(\tau)}}\right)$$

and similarly

$$\epsilon_{K_{n,w}}(\chi', \tau, dx) = \chi'(\pi^{a(\chi')+n(\tau)})\, q^{n(\tau)-\delta/2} \sum_{u \in \mathcal{O}_w^\times \bmod \pi^{a(\chi')}} \chi(u)\tau\left(\frac{u}{\pi^{a(\chi')+n(\tau)}}\right).$$

Here, π is a uniformiser for $K_{n,w}$, q is the number of elements in the residue field of w, δ is the exponent of w in the different of K_n, $a(\chi)$ is the exponent of w in the conductor of χ, and $n(\tau)$ is an integer depending on the additive character τ.

Since we assumed that χ and χ' are both tamely ramified at w, we have $a(\chi) = a(\chi')$. Therefore, since we also assume that χ and χ' are congruent modulo $\mathfrak{M}_{\mathbb{C}_p}$, the two sums are congruent term-by-term. □

4.7 A Short Example

Consider the semistable elliptic curve

$$E \;:\; y^2 + xy + y \;=\; x^3 - x^2 - x - 14$$

which is labelled 17A1 in Cremona's tables; it possesses good ordinary reduction at $p = 7$. In the paper [DD07], Tim and Vladimir Dokchitser compute the value

$$\mathbf{1}\big(N_{0,1}(a_0)\big) \;=\; 5.7^0 + 2.7^1 + 2.7^2 + \ldots$$

This implies that $N_{0,1}(a_0) \in \mathbb{Z}_7[[U^{(1)}]]^\times$, confirming that Hypothesis **(II)** holds in this case. If the conjecture of Stevens holds for E over F_n for some integer $n \geq 1$, Hypothesis **(I,n)** is also true, and our system of congruences

$$a_n \equiv N_{0,n}(a_0) \mod 7$$

confirms $a_n \in \mathbb{Z}_7[[U^{(n)}]]^\times$ for this example. Granted Stevens' conjecture holds, one obtains the K_1-congruence

$$\prod_{i=1}^{n} N_{i,n}(c_i)^{7^i} \equiv 1 \mod 7^{n+1}$$

by Theorem 4.1.2.

Chapter 5

Hecke Characters and CM-fields

In this chapter, we review some results on the p-adic interpolation of Hecke L-functions over a CM-field. These will be necessary to tackle the K_1-congruences for elliptic curves with complex multiplication in the next chapter.

We first recall the definition of a Hecke character, its L-series and its p-adic avatar. Then we introduce two p-adic L-functions, the first constructed by Katz in [Kat78] and the second by Hida in [Hid91]; the relation between these distributions is explored in the key paper [HT93].

The material in these articles is lengthy and technical; since we will only use the theory in a very specific case, we do not give the full details of all the objects involved.

5.1 Hecke Characters

Let M be a number field, and let $M_{\mathbb{A}}$ denote the adele ring of M. The multiplicative group $M^\times$ embeds diagonally into the idele group $M_{\mathbb{A}}^\times$, and we call the quotient $M_{\mathbb{A}}^\times / M^\times$ the idele class group.

Definition 5.1.1. *A Hecke character is a continuous homomorphism*

$$\psi \ : \ \frac{M_{\mathbb{A}}^{\times}}{M^{\times}} \longrightarrow \mathbb{C}^{\times}$$

i.e. a continuous idele class character.

For an integer $n \geq 1$ and a finite place $\mathfrak{p}$ of M, we write $U_{\mathfrak{p}}^{(n)}$ for the n-th group of higher units in $\mathcal{O}_{\mathfrak{p}}^{\times}$, so that $U_{\mathfrak{p}}^{(n)} = 1 + \mathfrak{p}^n$ (we also put $U_{\mathfrak{p}}^{(0)} = \mathcal{O}_{\mathfrak{p}}$). Then for an integral ideal $\mathfrak{m}$ of $\mathcal{O}_M$, we put

$$J^{\mathfrak{m}} \ = \ \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \ \subset \ M_{\mathbb{A}}^{\times}$$

where $n_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})$ and the product is taken over all finite places. We say that a Hecke character ψ has *module of definition* $\mathfrak{m}$ if $\psi(J^{\mathfrak{m}}) = \{1\}$, and we define the conductor $\mathfrak{f}_{\psi}$ of ψ to be the smallest module of definition for ψ.

If x_{∞} denotes the infinite part of $x \in M_{\mathbb{A}}^{\times}$, we may write

$$\psi(x_{\infty}) \ = \ \prod_{\sigma \in \mathrm{Hom}(M, \overline{\mathbb{Q}})} x_{\sigma}^{\xi_{\sigma}}$$

for integers ξ_{σ}, where $\mathrm{Hom}(M, \overline{\mathbb{Q}})$ is the set of field embeddings of M into $\overline{\mathbb{Q}}$. We will refer to the linear combination

$$\sum_{\sigma} \xi_{\sigma} \, \sigma \ \in \ \mathbb{Z}\big[\,\mathrm{Hom}(M, \overline{\mathbb{Q}})\big]$$

as the *infinity-type* of ψ.

We can also view Hecke characters as characters of ideals. Let $\mathfrak{m}$ be a non-zero integral ideal of $\mathcal{O}_M$, and denote by $\mathcal{I}_M(\mathfrak{m})$ the multiplicative group of fractional ideals of $\mathcal{O}_M$ which are prime to $\mathfrak{m}$. We also write

$$\mathrm{Prin}(\mathfrak{m}) = \Big\{\text{principal ideals } (\alpha) \text{ of } \mathcal{O}_M : \ \alpha \equiv 1 \mod \mathfrak{m}, \ \alpha \text{ totally positive}\Big\}.$$

Here we refer to an element of $\alpha \in M$ as totally positive if $\alpha^{\sigma} > 0$ for all real embeddings $\sigma : M \hookrightarrow \mathbb{R}$ (although M is not assumed to be a totally real field here).

Definition 5.1.2. *Let*

$$T \;=\; \sum_{\sigma} \eta_\sigma\, \sigma \;\in\; \mathbb{Z}\big[\,\mathrm{Hom}(M, \overline{\mathbb{Q}})\big]$$

be a $\mathbb{Z}$-linear combination of embeddings. An algebraic Grossencharacter modulo $\mathfrak{m}$ of infinity type T is defined to be a homomorphism

$$\varphi \;:\; \mathcal{I}_M(\mathfrak{m}) \longrightarrow \overline{\mathbb{Q}}^{\times}$$

such that for any $(\alpha) \in \mathrm{Prin}(\mathfrak{m})$ we have

$$\varphi\big((\alpha)\big) \;=\; \alpha^{-T} \;=\; \prod_{\sigma} (\alpha^\sigma)^{-\eta_\sigma}.$$

If $\mathfrak{m}'$ is another ideal with $\mathfrak{m}|\mathfrak{m}'$, a Grossencharacter modulo $\mathfrak{m}$ naturally gives rise to another modulo $\mathfrak{m}'$ by restriction from $\mathcal{I}_M(\mathfrak{m})$ to $\mathcal{I}_M(\mathfrak{m}')$. If $\mathfrak{f}_\varphi$ is the smallest ideal such that φ extends to a Grossencharacter modulo $\mathfrak{f}_\varphi$, we call $\mathfrak{f}_\varphi$ the *conductor* of φ. If φ is a Grossencharacter modulo $\mathfrak{m}$ such that $\mathfrak{m} = \mathfrak{f}_\varphi$ we say that φ is *primitive*.

These Grossencharacters are equivalent to Hecke characters as defined above. If $\psi : M_{\mathbb{A}}^{\times}/M^{\times} \longrightarrow \mathbb{C}^{\times}$ is a Hecke character with module of definition $\mathfrak{m}$, we can define a Grossencharacter φ_ψ modulo $\mathfrak{m}$ by setting

$$\varphi_\psi(\mathfrak{p}) \;=\; \psi(\hat{\varpi}_{\mathfrak{p}})$$

for all prime ideals $\mathfrak{p}$ such that $(\mathfrak{p}, \mathfrak{m}) = 1$, where

$$\hat{\varpi}_{\mathfrak{p}} \;=\; (\ldots 1, \varpi_{\mathfrak{p}}, 1, \ldots) \;\in\; M_{\mathbb{A}}^{\times}$$

and $\varpi_{\mathfrak{p}} \in M_{\mathfrak{p}}$ is a uniformiser. One can check that φ_ψ has the same conductor and infinity type as ψ. We will usually identify φ_ψ with ψ when there is no danger of confusion.

5.2 Hecke L-series

If ψ is a Grossencharacter modulo $\mathfrak{m}$, we extend it to all of $\mathcal{I}_M$ by setting $\psi(\mathfrak{a}) = 0$ for all ideals $\mathfrak{a}$ with $(\mathfrak{a}, \mathfrak{m}) \neq 1$. Then we define the *Hecke L-series* associated to ψ

to be

$$L(\psi, s) \ := \sum_{\mathfrak{a} \lhd \mathcal{O}_M} \psi(\mathfrak{a})\ N_{M/\mathbb{Q}}(\mathfrak{a})^{-s}.$$

This L-series is known to converge absolutely and uniformly on the domain $\mathrm{Re}(s) \geq 1 + \delta$ for any $\delta > 0$, and has the Euler product representation

$$L(\psi, s) \ = \ \prod_{\mathfrak{p}} \left(1 - \psi(\mathfrak{p})\ N_{M/\mathbb{Q}}(\mathfrak{p})^{-s}\right)^{-1},$$

where the product is taken over all prime ideals $\mathfrak{p}$ of $\mathcal{O}_M$.

The Hecke L-function $L(\psi, s)$ can be meromorphically continued to the entire complex plane, and satsfies a functional equation of the following form: we define the completed Hecke L-function

$$\tilde{L}(\psi, s) \ := \ c(\psi)^{s/2}\ L_\infty(\psi, s)\ L(\psi, s)$$

where $L_\infty(s, \psi)$ is a prescribed gamma factor, and $c(\psi) = |D_M|\, N_{M/\mathbb{Q}}(\mathfrak{f}_\psi)$. Then we have a functional equation

$$\tilde{L}(\psi, s) \ = \ W(\psi)\ \ \tilde{L}(\overline{\psi}, 1 - s),$$

where $W(\psi) \in \mathbb{C}$ is known as the *root number* of ψ, and has absolute value 1.

5.3 The p-adic Avatar of a Hecke Character

We choose an odd prime p, and fix two embeddings of $\overline{\mathbb{Q}}$:

$$\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C} \qquad \text{and} \qquad \iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p.$$

Given any embedding $\sigma : M \hookrightarrow \overline{\mathbb{Q}}$, composing σ with ι_p induces a p-adic place of M. We will denote the corresponding prime ideal over p by $\mathfrak{P}_\sigma$.

Consider an algebraic Hecke character $\psi : M_{\mathbb{A}}^\times / M^\times \longrightarrow \mathbb{C}^\times$, with infinite part

$$\psi(x_\infty) \ = \ \prod_{\sigma \in \mathrm{Hom}(M, \overline{\mathbb{Q}})} x_\sigma^{\xi_\sigma}.$$

We define a character $\hat{\psi} : M_{\mathbb{A}_f}^\times / M^\times \longrightarrow \overline{\mathbb{Q}}_p^\times$ by

$$\hat{\psi}(x) \;=\; \psi(x) \prod_{\sigma \in \mathrm{Hom}(M,\overline{\mathbb{Q}})} (x_{\mathfrak{P}_\sigma})^{\xi_\sigma}$$

where $M_{\mathbb{A}_f}^\times$ is the group of finite ideles. Following [HT93] we call $\hat{\psi}$ the *p-adic avatar of* ψ. By definition it has the property that $\psi(x) = \hat{\psi}(x)$ for any idele $x \in M_{\mathbb{A}}^\times$ with $x_p = x_\infty = 1$. Also, if $y \in M_{\mathbb{A}}^\times$ has p-component sufficiently close to 1 (i.e. $|y_p - 1|_p$ is small enough) we have

$$\hat{\psi}(y_p) \;=\; \prod_{\sigma \in \mathrm{Hom}(M,\overline{\mathbb{Q}})} (y_{\mathfrak{P}_\sigma})^{\xi_\sigma} \,.$$

If ψ is defined modulo $\mathfrak{C}p^n$, then as a character of ideals $\hat{\psi}$ is given by composing the Grossencharacter ψ with the embedding ι_p. The Artin map gives an isomorphism

$$\frac{\mathcal{I}_M(\mathfrak{C}p^n)}{\mathrm{Prin}(\mathfrak{C}p^n)} \;\xrightarrow{\sim}\; \mathrm{Gal}\left(M(\mathfrak{C}p^n)/M\right),$$

so it allows us to regard $\hat{\psi}$ as a character of $\mathrm{Gal}(M(\mathfrak{C}p^n)/M)$. In fact we can pass to the projective limit over n and view $\hat{\psi}$ as a continuous character

$$\hat{\psi} \;:\; \mathrm{Gal}\left(M(\mathfrak{C}p^\infty)/M\right) \longrightarrow \overline{\mathbb{Q}}_p^\times$$

where $M(\mathfrak{C}p^\infty)$ is the maximal ray class field modulo $\mathfrak{C}p^\infty$ over M.

5.4 CM-fields

Let F be a totally real number field, and M/F a totally imaginary quadratic extension. Such a field M is called a *CM-field*.

As above, we fix an odd prime p and two embeddings of $\overline{\mathbb{Q}}$:

$$\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C} \qquad \text{and} \qquad \iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p.$$

Hypothesis: *Throughout we assume that every prime of F above p splits in M/F .*

This hypothesis allows us to choose a set Σ of embeddings of M into $\overline{\mathbb{Q}}$ such that:

(i) $\Sigma \cap \overline{\Sigma} = \emptyset$ *and* $\Sigma \cup \overline{\Sigma}$ *is the set of all embeddings* $\sigma : M \hookrightarrow \overline{\mathbb{Q}}$;

(ii) *the p-adic place induced by any element of* Σ *composed with* ι_p *is distinct from that induced by any element of* $\overline{\Sigma}$.

The set Σ is called a *p-ordinary CM-type for* M. We have the corresponding set of primes over p:

$$S \ := \ \big\{ \mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_M) \ : \ \mathfrak{P} \text{ induced by some } \sigma \in \Sigma \ \big\}.$$

By definition of Σ, the set of prime factors of p in M may be written as the disjoint union $S \cup \overline{S}$ where $\mathfrak{P} \in S$ if and only if $\overline{\mathfrak{P}} \in \overline{S}$.

We fix a prime-to-p ideal $\mathfrak{C}$, and write $\mathbf{G}_\infty(\mathfrak{C}) = \mathrm{Gal}\left(M(\mathfrak{C}p^\infty)/M\right)$. We may decompose this Galois group as a product

$$\mathbf{G}_\infty(\mathfrak{C}) \ = \ \mathbf{G}_{\mathrm{tor}}(\mathfrak{C}) \times \mathbf{W}$$

where $\mathbf{G}_{\mathrm{tor}}(\mathfrak{C})$ is a finite group and $\mathbf{W}$ is a $\mathbb{Z}_p$-free module of finite rank. In fact, $\mathbf{W}$ is determined independently of the prime-to-p conductor $\mathfrak{C}$ (see [HT93]).

For the rest of this chapter, we will write $\mathcal{O} = \mathcal{O}_{\mathbb{C}_p}$. We consider the completed group ring

$$\Lambda \ = \ \mathcal{O}[[\mathbf{W}]] \ := \ \varprojlim_a \mathcal{O}\left[\mathbf{W}/\mathbf{W}^{p^a}\right].$$

By choosing a basis of $\mathbf{W}$, we can make identifications

$$\mathbf{W} \ \cong \ \mathbb{Z}_p^r \qquad \text{and} \qquad \Lambda \ \cong \ \mathcal{O}[[X_1, \ldots, X_r]].$$

We may also write $\mathcal{O}[[\mathbf{G}_\infty(\mathfrak{C})]] \ = \ \Lambda[\mathbf{G}_{\mathrm{tor}}(\mathfrak{C})]$. If we are given a character λ :

$\mathbf{G}_{\mathrm{tor}}(\mathfrak{C}) \longrightarrow \mathcal{O}^\times$, we have a natural projection

$$\begin{aligned} \lambda_* \quad : \quad \mathcal{O}[[\mathbf{G}_\infty(\mathfrak{C})]] \quad &\longrightarrow \quad \Lambda \\ (g, w) \quad &\longmapsto \quad \lambda(g)[w] \end{aligned}$$

where $(g, w) \in \mathbf{G}_{\mathrm{tor}}(\mathfrak{C}) \times \mathbf{W}$, and $[w]$ is the image of $w \in \mathbf{W}$ in $\Lambda = \mathcal{O}[[\mathbf{W}]]$.

For $G = \mathbf{G}_\infty(\mathfrak{C})$ or $\mathbf{W}$, we write $\mathfrak{X}(G)$ for the set of continuous characters $G \longrightarrow \overline{\mathbb{Q}}_p^\times$. Any character $\mathcal{P} \in \mathfrak{X}(G)$ induces an $\mathcal{O}$-algebra homomorphism $\mathcal{P} : \mathcal{O}[[G]] \longrightarrow \overline{\mathbb{Q}}_p$, such that $\mathcal{P}\big|_G$ is the original character of G. This means we have an isomorphism

$$\mathfrak{X}(G) \;\cong\; \mathrm{Hom}_{\mathcal{O}-\mathrm{alg}}\big(\mathcal{O}[[G]], \overline{\mathbb{Q}}_p\big).$$

As stated in [HT93], the set $\mathfrak{X}(G)$ can also be identified with the $\overline{\mathbb{Q}}_p$-valued points of $\mathrm{Spec}(\mathcal{O}[[G]]))$.

An element $\Phi \in \mathcal{O}[[G]]$ can be thought of as an analytic function on $\mathfrak{X}(G)$ by setting $\Phi(\mathcal{P}) := \mathcal{P}(\Phi)$ for all $\mathcal{P} \in \mathfrak{X}(G)$. It can also be viewed as a measure on G by setting

$$\int_G \mathcal{P}(g)\, d\Phi(g) \;=\; \mathcal{P}(\Phi).$$

Recall our fixed projection $\lambda_* : \mathcal{O}[[\mathbf{G}_\infty(\mathfrak{C})]] \longrightarrow \Lambda$. For a point $P \in \mathfrak{X}(\mathbf{W})$, we define a specialisation

$$\lambda_{\mathcal{P}} = \mathcal{P} \circ \lambda_* \;:\; \mathcal{O}[[\mathbf{G}_\infty(\mathfrak{C})]] \longrightarrow \overline{\mathbb{Q}}_p,$$

so $\lambda_{\mathcal{P}}$ is a p-adic character of $\mathbf{G}_\infty(\mathfrak{C})$. If there exists an algebraic Hecke character ψ such that $\lambda_{\mathcal{P}}$ is equal to the p-adic avatar $\hat{\psi}$, we say $\mathcal{P}$ is *arithmetic*.

5.5 The Katz Measure

Let M be a CM-field as before, with complex CM-type Σ. We are interested in the p-adic interpolation of values of Hecke L-functions over M. In [Kat78], Katz

constructs a measure μ_{Katz} on $\mathbf{G}_\infty(\mathfrak{C})$ with the property

$$\frac{\displaystyle\int \hat{\lambda}\, d\mu_{\mathrm{Katz}}}{p\text{-adic period}} \;=\; \text{explicit factors} \;\times\; \frac{L(\lambda,0)}{\text{complex period}}$$

for every Hecke character λ over M, whose conductor divides $\mathfrak{C}p^\infty$ and which satisfies a certain criticality condition. In fact, Katz's original construction was only for characters modulo p^∞, but this was generalised by Hida and Tilouine in [HT93] to the case of a non-trivial prime-to-p conductor $\mathfrak{C}$.

We will briefly state the interpolation properties of this measure, and we refer the reader to [HT93] for the full details. We also follow the notation of [HT93] where possible.

In [Kat78], Katz defines a complex period $\Omega_\infty \in \mathbb{C}^\Sigma$, and a p-adic period $\Omega_p \in (\mathcal{O}_{\mathbb{C}_p}^\times)^\Sigma$. They are defined using differentials on Hilbert-Blumenthal abelian varieties, but the details are beyond the scope of this thesis.

We denote by δ a purely imaginary element of M, which is a suitable generator of the ideal $\mathfrak{C}\,\mathfrak{d}_M$. We write $\mathbf{e}_M$ for the standard additive character $M_{\mathbb{A}}/M \to \mathbb{C}^\times$ which is normalised by $\mathbf{e}_M(x_\infty) = \exp(2\pi i \operatorname{Tr}_{M/\mathbb{Q}}(x_\infty))$. Then we define a local factor:

$$W_p(\lambda) \;:=\; \prod_{\mathfrak{P}\in S} N_{M/\mathbb{Q}}(\mathfrak{P})^{-f}\;\; \lambda(\varpi_{\mathfrak{P}}^{-f}) \sum_{u\in\mathcal{O}_{\mathfrak{P}}^\times \bmod \mathfrak{P}^f} \lambda_{\mathfrak{P}}(u)\;\, \mathbf{e}_M\left(\frac{u}{d_{\mathfrak{P}}\,\varpi_{\mathfrak{P}}^f}\right)$$

where $\varpi_{\mathfrak{P}}$ is a uniformiser for $M_{\mathfrak{P}}$, $f = f(\lambda,\mathfrak{P})$ is the power of $\mathfrak{P}$ dividing the conductor of λ, and $d_{\mathfrak{P}} \in \mathcal{O}_{\mathfrak{P}}$ generates the local different $\mathfrak{d}_{M,\mathfrak{P}}$.

Now we can state the interpolation property of the Katz measure, as given in Theorem II of [HT93].

Proposition 5.5.1. *There exists an integral-valued measure μ_{Katz} on $\mathbf{G}_\infty(\mathfrak{C})$ which*

has the property

$$\frac{1}{\Omega_p^{m_0\Sigma+2d}}\int_{\mathbf{G}_\infty(\mathfrak{C})}\hat{\lambda}\,d\mu_{\mathrm{Katz}} \;=\; [\mathcal{O}_M^\times:\mathcal{O}_F^\times]\,W_p(\lambda)\,\frac{(-1)^{m_0\Sigma}\,\pi^d\,\Gamma_\Sigma(m_0\Sigma+d)}{\sqrt{|D_F|}\,\mathrm{Im}(\delta)^d}$$
$$\times\;\prod_{\mathfrak{L}|\mathfrak{C}}\big(1-\lambda(\mathfrak{L})\big)\;\times\;\prod_{\mathfrak{P}\in S}\big(1-\lambda(\overline{\mathfrak{P}})\big)\big(1-\lambda^*(\overline{\mathfrak{P}})\big)\;\times\;\frac{L(\lambda,0)}{\Omega_\infty^{m_0\Sigma+2d}}$$

for all Hecke characters λ modulo $\mathfrak{C}p^\infty$ such that:

(i) *the conductor of λ is divisible by all the prime factors of $\mathfrak{C}$ which are split in M/F,*

(ii) *the infinity type of λ is $m_0\Sigma + d - \overline{d}$ where $d = \sum_{\sigma\in\Sigma} d_\sigma\sigma$ for integers m_0 and d_σ satisfying either $m_0 > 0$ and $d_\sigma \geq 0$ or $m_0 \leq 1$ and $d_\sigma \geq 1 - m_0$.*

In the statement of Proposition 5.5.1, we use the following conventions: for an element $\xi \in \mathbb{Z}[\Sigma \cup \overline{\Sigma}]$ and for $x \in \mathbb{C}^\Sigma$, we write

$$x^\xi \;=\; \prod_{\sigma\in\Sigma} x_\sigma^{\xi_\sigma}\prod_{\sigma\in\Sigma}\overline{x}_\sigma^{\xi_{\overline{\sigma}}} \qquad \text{and} \qquad \Gamma_\Sigma(\xi) \;=\; \prod_{\sigma\in\Sigma}\Gamma(\xi_\sigma)\,.$$

The set Σ is identified with the formal sum $\sum_{\sigma\in\Sigma}\sigma$, and $a \in M$ is considered to be an element of $\mathbb{C}^\Sigma$ via the diagonal embedding $a \mapsto (a^\sigma)_{\sigma\in\Sigma}$. We consider π to be the diagonal element $(\pi)_{\sigma\in\Sigma} \in \mathbb{C}^\Sigma$. The L-function in the theorem is the one associated with the primitive Hecke character.

5.6 Anti-cyclotomic Projection

As in Section 5.4, we consider a character $\lambda : \mathbf{G}_{\mathrm{tor}}(\mathfrak{C}) \longrightarrow \mathcal{O}^\times$, and the projection $\lambda_* : \mathcal{O}[[\mathbf{G}_\infty(\mathfrak{C})]] \longrightarrow \Lambda$ where $\Lambda = \mathcal{O}[[\mathbf{W}]]$. Let us define another character by setting

$$\lambda^-(x) \;=\; \lambda(x)^{-1}\lambda(x^c);$$

where $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ denotes complex conjugation. We assume λ^- to be primitive of conductor $\mathfrak{C}^-$ (as a character of $\mathbf{G}_\infty(\mathfrak{C})/\mathbf{W}$), so that we may consider it as a

character of $\mathbf{G}_{\mathrm{tor}}(\mathfrak{C}^-)$. We may decompose $\mathbf{G}_\infty(\mathfrak{C}^-)$ as a product

$$\mathbf{G}_\infty(\mathfrak{C}^-) \;=\; \mathbf{G}_{\mathrm{tor}}(\mathfrak{C}^-) \times \mathbf{W}$$

since $\mathbf{W}$ is determined independently of $\mathfrak{C}$. Then, we define the anti-cyclotomic projection π_λ^- associated to λ:

$$\begin{aligned} \pi_\lambda^- \quad : \quad \mathcal{O}[[\mathbf{G}_\infty(\mathfrak{C}^-)]] \quad &\longrightarrow \quad \Lambda \\ (\zeta, w) \quad &\longmapsto \quad \lambda^-(\zeta)\, w^{-1}c^{-1}wc. \end{aligned}$$

for $(\zeta, w) \in \mathbf{G}_{\mathrm{tor}}(\mathfrak{C}^-) \times \mathbf{W}$. By definition, π_λ^- takes values in the anti-cyclotomic part $\mathcal{O}[[\mathbf{W}^-]]$ of Λ, which is defined by

$$\mathbf{W}^- \;:=\; \left\{ w \in \mathbf{W} \;:\; c^{-1}wc = w^{-1} \right\}.$$

Recall the Katz measure μ_{Katz} from Section 5.5 above. This is an integral-valued measure, and so it corresponds to a power series $\mathbb{L}_{\mathrm{Katz}} \in \mathcal{O}[[\mathbf{G}_\infty(\mathfrak{C})]]$. Therefore we may define its anti-cyclotomic projection

$$\mathbb{L}^-_{(M,\lambda)} \;:=\; \pi_\lambda^-\big(\,\mathbb{L}_{\mathrm{Katz}}\big) \;\in\; \mathcal{O}[[\mathbf{W}^-]].$$

Looking back at Proposition 5.5.1, one sees that $\mathbb{L}^-_{(M,\lambda)}$ will satisfy the interpolation property

$$\frac{\mathbb{L}^-_{(M,\lambda)}(\mathcal{P})}{p\text{-adic period}} \;=\; \text{explicit factors} \;\times\; \frac{L(\lambda_{\mathcal{P}}^c \lambda_{\mathcal{P}}^{-1}, 0)}{\text{complex period}}$$

whenever $\mathcal{P} \in \mathfrak{X}(\mathbf{W})$ is arithmetic for λ, and the Hecke character $\lambda_{\mathcal{P}}^c \lambda_{\mathcal{P}}^{-1}$ is critical.

5.7 The Theta Measure

Let φ be an algebraic Hecke character over M, defined modulo $\mathfrak{C}p^\infty$. It is known that there exists a Hilbert automorphic form $\theta(\varphi)$ over the totally real field F with the property

$$\theta(\varphi)\,\big|\,T(\mathfrak{q}) \;=\; \begin{cases} \big(\varphi(\mathfrak{Q}) + \varphi(\overline{\mathfrak{Q}})\big)\,\theta(\varphi) & \text{if } \mathfrak{q} \text{ splits as } \mathfrak{Q}\overline{\mathfrak{Q}} \text{ in } M/F \\ \varphi(\mathfrak{Q})\;\theta(\varphi) & \text{if } \mathfrak{q} \text{ ramifies in } M/F \\ 0 & \text{if } \mathfrak{q} \text{ is inert in } M/F \end{cases}$$

for each prime $\mathfrak{q}$ of $\mathcal{O}_F$ with $(\mathfrak{q}, \mathfrak{C}p) = 1$. We call $\theta(\varphi)$ the *theta series* of φ. The level of $\theta(\varphi)$ is

$$\mathfrak{c}\big(\theta(\varphi)\big) \;=\; N_{M/F}(\mathfrak{f}_\varphi)\ \mathrm{Disc}(M/F)\ p.$$

The weight of $\theta(\varphi)$ will not in general be parallel, but if the infinity type of λ can be written in the form $m_0\Sigma + d(\Sigma - \Sigma c)$ with $m_0, d \in \mathbb{Z}$ then the theta series has parallel weight $m_0 + 2d + 1$.

A Hecke eigenform of level $\mathfrak{C}p^\infty$ may be viewed as a specialisation of the Hecke algebra $\mathbf{h}(\mathfrak{C}; \mathcal{O})$, in which the Hecke operator $T(\mathfrak{q})$ is mapped to the corresponding eigenvalue. Therefore, we can reinterpret the existence of theta series as an $\mathcal{O}[[\mathbf{W}]]$-algebra homomorphism

$$\theta^* \;:\; \mathbf{h}(\mathfrak{C}; \mathcal{O}) \longrightarrow \mathcal{O}[[\mathbf{G}_\infty(\mathfrak{C})]]$$

such that

$$\theta^*\big(T(\mathfrak{q})\big) = \begin{cases} [\mathfrak{Q}] + [\overline{\mathfrak{Q}}] & \text{if } \mathfrak{q} \text{ splits as } \mathfrak{Q}\overline{\mathfrak{Q}} \text{ in } M/F \\ [\mathfrak{Q}] & \text{if } \mathfrak{q} \text{ ramifies in } M/F \\ 0 & \text{if } \mathfrak{q} \text{ is inert in } M/F \end{cases}$$

for all primes $\mathfrak{q}$ satisfying $(\mathfrak{q}, \mathfrak{C}p) = 1$. Here $[\mathfrak{Q}]$ denotes the image of the prime ideal $\mathfrak{Q}$ under the Artin symbol.

We refer to the map θ^* as the *theta measure*; by definition, the specialisation

$$\hat{\varphi} \circ \theta^* \;:\; \mathbf{h}(\mathfrak{C}; \mathcal{O}) \longrightarrow \overline{\mathbb{Q}}_p^\times$$

corresponds to the theta series $\theta(\varphi)$.

Remark 5.7.1. Here we should point out that in $\mathbf{h}(\mathfrak{C}; \mathcal{O})$ is in fact the p-adic Hecke algebra, and the specialisation $\hat{\varphi} \circ \theta^*$ corresponds to $\theta(\varphi)$ considered as a p-adic Hilbert modular form. We will not define p-adic modular forms here, but refer the reader to [HT89] and [HT93] for details. For our purposes, it is sufficient to consider $\theta(\varphi)$ as a complex Hilbert modular form with an algebraic q-expansion.

5.8 Congruence Modules

We now define a congruence module associated to λ_*, which is needed to ensure Hida's automorphic p-adic L-function is integral (see Theorem 5.9.2). Let $\Lambda = \mathcal{O}[[\mathbf{W}]]$ as before, and write $\mathbf{L}$ for the field of fractions of Λ. If $\mathbf{h} = \mathbf{h}(\mathfrak{C}; \mathcal{O})$ there exists a decomposition

$$\mathbf{h} \otimes_\Lambda \mathbf{L} \;=\; \mathbf{L} \oplus \mathbf{B}$$

such that projection to the first factor is given by $\lambda_* \circ \theta^*$.

Definition 5.8.1. *The congruence module of λ_* is defined to be*

$$C(\lambda_*; \Lambda) \;:=\; \frac{\Lambda}{(\mathbf{h} \otimes_\Lambda \Lambda) \cap \mathbf{L}}.$$

As its name suggests, this module is related to congruences between $\theta(\lambda)$ and other Hilbert modular forms, but we will not discuss this. We simply quote that $C(\lambda_*; \Lambda)$ is a torsion Λ-module of finite type, and so it has a characteristic power series $\mathbf{H}_\lambda := \mathrm{char}_\Lambda C(\lambda_*; \Lambda)$. We will refer to $\mathbf{H}_\lambda$ as the *congruence power series of* λ.

Theorem 5.8.2. [MT90, Til89, HT93] *Under the condition $\mathfrak{C} + \mathfrak{C}^c = \mathcal{O}_M$, then up to a p-adic unit we have*

$$\mathbf{H}_\lambda \quad = \quad \frac{\#\mathrm{Pic}(\mathcal{O}_M)}{\#\mathrm{Pic}(\mathcal{O}_{M^+})} \;\times\; \mathbb{L}^-_{(M,\lambda)}$$

where $\mathbb{L}^-_{(M,\lambda)}$ is the anti-cyclotomic projection of the Katz p-adic L-function as defined in Section 5.6.

This deep result forms part of the 'anti-cyclotomic main conjecture'. In the context of our work, it provides a more explicit description of the valuation of $\mathbf{H}_\lambda$ at weight two (i.e. for CM elliptic curves).

5.9 Hida's p-adic L-function

In [HT93] Section 7, Hida and Tilouine define a convolution L-series $\mathfrak{D}(\mathbf{f},\mathbf{g},s)$ for Hilbert modular forms $\mathbf{f} \in \mathcal{S}_k(\mathfrak{c}(\mathbf{f}),\psi)$ and $\mathbf{g} \in \mathcal{M}_l(\mathfrak{c}(\mathbf{g}),\eta)$. This L-series can be written as an Euler product, and is similar to the convolution

$$L_{\mathfrak{c}}(\psi\eta, 2s+2-k-l) \sum_{\mathfrak{a}\lhd\mathcal{O}_F} C(\mathfrak{a},\mathbf{f})\, C(\mathfrak{a},\mathbf{g})\, N_{F/\mathbb{Q}}(\mathfrak{a})^{-s}$$

which we studied in Chapter 3, but is normalised differently. We will now introduce a p-adic L-function constructed by Hida in [Hid91], which interpolates the special values of $\mathfrak{D}(\theta(\lambda_{\mathcal{P}}),\theta(\nu_{\mathcal{Q}}),s)$.

We fix two prime-to-p conductors $\mathfrak{C},\mathfrak{C}' \lhd \mathcal{O}_M$, and two characters

$$\lambda \;:\; \mathbf{G}_{\mathrm{tor}}(\mathfrak{C}) \longrightarrow \mathcal{O}^{\times} \qquad \text{and} \qquad \nu \;:\; \mathbf{G}_{\mathrm{tor}}(\mathfrak{C}') \longrightarrow \mathcal{O}^{\times}.$$

Since the free part $\mathbf{W}$ of $\mathbf{G}_{\infty}(\mathfrak{C})$ is determined independently of $\mathfrak{C}$, we can write

$$\mathbf{G}_{\infty}(\mathfrak{C}) \cong \mathbf{G}_{\mathrm{tor}}(\mathfrak{C}) \times \mathbf{W} \qquad \text{and} \qquad \mathbf{G}_{\infty}(\mathfrak{C}') \cong \mathbf{G}_{\mathrm{tor}}(\mathfrak{C}') \times \mathbf{W}.$$

Therefore, setting $\Lambda = \mathcal{O}[[\mathbf{W}]]$, we have associated projections as in Section 5.4:

$$\lambda_* \;:\; \mathcal{O}[[\mathbf{G}_{\infty}(\mathfrak{C})]] \longrightarrow \Lambda \qquad \text{and} \qquad \nu_* \;:\; \mathcal{O}[[\mathbf{G}_{\infty}(\mathfrak{C}')]] \longrightarrow \Lambda.$$

Suppose we have $\mathcal{P},\mathcal{Q} \in \mathfrak{X}(\mathbf{W})$ such that $\mathcal{P}$ is an arithmetic specialisation for λ_*, and $\mathcal{Q}$ is an arithmetic specialisation for ν_*. Then the compositions $\lambda_{\mathcal{P}} = \mathcal{P}\circ\lambda_*$ and $\nu_{\mathcal{Q}} = \mathcal{Q}\circ\nu_*$ are the p-adic avatars of two algebraic Hecke characters.

For any Hecke character ψ we define the *unitarisation* ψ^u of ψ by

$$\psi^u(x) \;=\; \frac{\psi(x)}{|\psi(x)|_{\infty}}.$$

Lemma 5.9.1. *Let $\mathfrak{D}_p\big(\theta(\lambda_{\mathcal{P}}),\theta(\nu_{\mathcal{Q}})^{\vee},s\big)$ denote Hida's Rankin convolution with the Euler factors at the primes above p removed. Then we have the identity*

$$\mathfrak{D}_p\left(\theta(\lambda_{\mathcal{P}}),\ \theta(\nu_{\mathcal{Q}})^{\vee},\ s\right) \;=\; E'(\mathcal{P},\mathcal{Q}\,;s)\ \times\ L_p\big(\lambda_{\mathcal{P}}^u\,\nu_{\mathcal{Q}}^{cu},s\big)\ \times\ L_p\big(\lambda_{\mathcal{P}}^u\,\nu_{\mathcal{Q}}^{[c]u},s\big),$$

where $\nu^{[c]}(x) = \nu(x^c)^c$ if $x_p = 1$, and $E'(\mathcal{P},\mathcal{Q};s)$ is the Euler factor defined in [HT93]. *The Hecke L-functions in the equation above are always the primitive ones.*

Proof. See [HT93], equation (8.5 a). □

Now let us also assume that

$$\text{infinity type of } \lambda_{\mathcal{P}} \;=\; m_0\,\Sigma \,+\, d(\Sigma - \Sigma c)$$

for some integers m_0 and d, and similarly

$$\text{infinity type of } \nu_{\mathcal{Q}} \;=\; m_0'\,\Sigma \,+\, d'(\Sigma - \Sigma c)$$

for integers m_0' and d'. Then, following [HT93] we write

$$m(\mathcal{P}) \;=\; m_0 - 1 \qquad \text{and} \qquad m(\mathcal{Q}) \;=\; m_0' - 1.$$

We can now quote the existence of the Rankin convolution p-adic L-function, which is proved by Hida in [Hid91] Theorem 5.2. We write $\Lambda\widehat{\otimes}_{\mathcal{O}}\Lambda$ for the $\mathfrak{m}$-adic completion of $\Lambda \otimes_{\mathcal{O}} \Lambda$, where $\mathfrak{m}$ is the unique maximal ideal of $\Lambda \otimes_{\mathcal{O}} \Lambda$.

Theorem 5.9.2. *There exists an element $\mathfrak{D}_{\lambda,\nu} \in \mathrm{Quot}(\Lambda\widehat{\otimes}_{\mathcal{O}}\Lambda)$ satisfying:*

(i) *We have*

$$(\mathbf{H}_\lambda \otimes 1)\,.\,\mathfrak{D}_{\lambda,\nu} \;\in\; \Lambda\widehat{\otimes}_{\mathcal{O}}\Lambda,$$

where $\mathbf{H}_\lambda$ is the characteristic power series of the congruence module $C(\lambda_*;\Lambda)$.

(ii) *For all pairs $(\mathcal{P},\mathcal{Q})$ which are critical for (λ,ν),*

$$\begin{aligned}\mathfrak{D}_{\lambda,\nu}(\mathcal{P},\mathcal{Q}) \;&=\; \frac{C(\mathcal{P},\mathcal{Q})\;W(\mathcal{P},\mathcal{Q})\;E(\mathcal{P},\mathcal{Q})}{S(\mathcal{P})} \\ &\times\; \frac{\mathfrak{D}_p\Big(\theta(\lambda_{\mathcal{P}}),\;\theta(\nu_{\mathcal{Q}})^\vee,\;1+\dfrac{m(\mathcal{Q})-m(\mathcal{P})}{2}\Big)}{\Big\langle \theta(\lambda_{\mathcal{P}})\otimes\eta'_{\mathcal{P}},\;\theta(\lambda_{\mathcal{P}})\otimes\eta'_{\mathcal{P}}\Big\rangle}\end{aligned}$$

for interpolation factors $C(\mathcal{P},\mathcal{Q}), W(\mathcal{P},\mathcal{Q}), E(\mathcal{P},\mathcal{Q})$ and $S(\mathcal{P})$ which are explicitly given in [HT93] *Section 8. Here the character $\eta'_{\mathcal{P}} : \mathcal{O}_p^\times \to \overline{\mathbb{Q}}^\times$ is defined by $\eta'_{\mathcal{P}}(y) = \hat{\lambda}_{\mathcal{P}}(y)^{-1}$.*

The condition for $(\lambda_{\mathcal{P}}, \nu_{\mathcal{Q}})$ to be critical is given in [Hid91] (5.3a); when all the weights are parallel, it reduces to the assertion $m(\mathcal{P}) - m(\mathcal{Q}) \geq 1$.

The definitions of the interpolation factors are complicated, and we will not give them in full generality. Luckily, the following remark of Hida tells us what they are in the case we are interested in.

Remark 5.9.3. In the preamble to [Hid91], Hida states that when $(\lambda_{\mathcal{P}}, \nu_{\mathcal{Q}})$ is a motivic pair, the ϵ-factors $W(\mathcal{P}, \mathcal{Q})$, the Γ-factors $C(\mathcal{P}, \mathcal{Q})$ and the Euler factors $E(\mathcal{P}, \mathcal{Q})\, S(\mathcal{P})^{-1}$ coincide exactly with those given in the general recipe for p-adic L-functions of motives given by Coates and Perrin-Riou in [CPR89]. Therefore, when we specialise to the case of CM elliptic curves, these interpolation factors will agree with those of Coates et al from [CFK$^+$05].

Chapter 6

Growth of CM Periods

In this chapter we prove weak forms of Kato's K_1-congruences for elliptic curves with complex multiplication, subject to two technical hypotheses identical to those imposed in Chapter 4.

As before, we encounter an error term measuring the failure of the Petersson inner product to coincide with the Néron period. This period ratio grows as we climb the tower of totally real fields, and we use symmetric square L-series to explicitly compute it in some cases. Finally, we show how the growth-rate can be estimated in the CM case using the arithmetic of the $\mathbb{Z}_p^2$-extension.

This chapter is joint work with my PhD supervisor, Daniel Delbourgo. We thank Thanasis Bouganis for informing us of his approach to the Heisenberg type congruences, and for many other suggestions. We are also very grateful to Neil Dummigan for his advice on computing the special values of symmetric square L-series.

6.1 Main Results

Let E be an elliptic curve defined over $\mathbb{Q}$ admitting complex multiplication by an order in the ring $\mathcal{O}_K$, where $K = \mathbb{Q}\left(\sqrt{-D}\right)$ denotes an imaginary quadratic field. Fix a prime number $p \neq 2$ which splits into $(p) = \mathfrak{p} \times \mathfrak{p}^*$ inside $\mathcal{O}_K$; this is equivalent to assuming that E possesses good ordinary reduction at p. We also pick an auxiliary p-power-free integer $\Delta > 1$ which is coprime to p, and to the conductor N_E of the elliptic curve.

We consider a false Tate curve extension of the quadratic field K: setting

$$K_{\mathrm{FT}} = \bigcup_{n \geq 1} K\left(\mu_{p^n}, \sqrt[p^n]{\Delta}\right)$$

we have

$$G_\infty \ := \ \mathrm{Gal}(K_{FT}/K) \ \cong \ \begin{pmatrix} \mathbb{Z}_p^\times & \mathbb{Z}_p \\ 0 & 1 \end{pmatrix},$$

the same non-commutative p-adic Lie group of dimension 2 that we considered in previous chapters.

The Artin representations of $\mathrm{Gal}(K_{FT}/K)$ can be described in the same way as those of $\mathrm{Gal}(\mathbb{Q}_{FT}/\mathbb{Q})$: putting $K_n = K(\mu_{p^n})$ we write

$$\rho_n \ = \ \mathrm{Ind}_{K_n}^K(\chi_n)$$

for the unique self-dual representation of G_∞ of degree $p^n - p^{n-1}$. The irreducible Artin representations of G_∞ are all of the form $\rho_n \otimes \psi$ for some $n \geq 0$, and some finite order character $\psi : \mathrm{Gal}\big(K(\mu_{p^\infty})/K\big) \to \mathbb{C}^\times$.

Lastly, the Galois group of $K(\mu_{p^\infty})$ over K_n will be abbreviated by $U^{(n)}$.

Definition 6.1.1. *The 'motivic' p-adic L-function $\mathcal{L}(E, \rho_n)$ of $E_{/K}$ twisted by ρ_n is the unique element of $\mathbb{Z}_p[\![U^{(n)}]\!] \otimes \mathbb{Q}$ satisfying*

$$\psi\big(\mathcal{L}(E, \rho_n)\big) \ = \ \frac{\epsilon(\rho_n \otimes \psi)_p}{\alpha_p^{f_\psi}} \ \times \ \text{Euler factor} \ \times \ \frac{L_{\{p\Delta\}}\big(E/K, \rho_n \otimes \psi^{-1}, 1\big)}{\big(\Omega_E^+ \, \Omega_E^-\big)^{[K_n:K]}}$$

at all Dirichlet characters $\psi : U^{(n)} \to \overline{\mathbb{Q}}_p^{\times}$ *of conductor* $\mathfrak{f}_\psi$. *Here* α_p *is the* p*-adic unit root of* $1 - a_p(E)T + pT^2$, *and* f_ψ *is the power of* p *dividing* $\mathfrak{f}_\psi$. *Also* $\epsilon(\rho_n \otimes \psi)_p$ *is the local* ϵ*-factor at* p, *normalised as in* [CFK$^+$05].

The existence of $\mathcal{L}(E, \rho_n)$ follows from interpolation properties of the Katz-Eisenstein measure, which is discussed in the next section.

To make further progress, we now impose the same two assumptions that were needed in Chapter 4.

Hypothesis (I, n**)** For each integer $j \in \{0, \ldots, n\}$, Conjecture IV of Stevens [Ste89] §4 holds at all $\rho_j \otimes \psi$-twists of the f_E-isotypic component in $H_1\big(X_1(N_E), \mathbb{Z}\big)$.

Hypothesis (II) Each analytic μ-invariant associated to the $(p-1)$ branches of the Mazur-Tate-Teitelbaum p-adic L-function for E/K, vanishes.

As stated in Chapter 4, both of these hypotheses are expected to hold in general. Hypothesis **(I,** n**)** would follow from the ρ_j-twisted main conjectures for $j \in \{0, \ldots, n\}$, and Hypothesis **(II)** may be verified numerically in certain cases. For example, we computed the value of $\mathrm{Norm}_{0,1}(\mathcal{L}_p(E, \rho_0))$ evaluated at the trivial character for some examples of E, p and Δ (see Tables 6.1, 6.2 and 6.3). For the cases in which this value is a p-adic unit, Hypothesis **(II)** is confirmed.

Recall that for all positive integers $j \leq n$, the norm map induces a homomorphism $\mathrm{Norm}_{j,n} : \mathbb{Z}_p[[U^{(j)}]] \to \mathbb{Z}_p[[U^{(n)}]]$ on the completed group rings. We now state the first main theorem of this chapter.

Theorem 6.1.2. *Assume that* **(I,** n**)** *holds for a given* $n \in \mathbb{N}$, *and also* **(II)** *is true. Then there is a family of congruences*

$$\mathcal{L}(E, \rho_n) \;\equiv\; \mathrm{Norm}_{n-1,n}\big(\mathcal{L}(E, \rho_{n-1})\big) \;\equiv\; \ldots \;\equiv\; \mathrm{Norm}_{0,n}\big(\mathcal{L}(E, \rho_0)\big) \mod p.$$

In particular, if $\omega^i\big(\mathcal{L}(E, \rho_0)\big) \in \mathbb{Z}_p^{\times}$ for all $i \in \{0, \ldots, p-2\}$ then by Definition 6.1.1,

clearly one has $L(E/K_1, 1) \neq 0$. Moreover, from Theorem 6.1.2 it follows directly

$$L(E/K, \rho_j, 1) \ \neq \ 0 \qquad \text{at every } 1 \leq j \leq n.$$

Let $\varphi : \mathbb{Z}_p[[U^{(j-1)}]] \longrightarrow \mathbb{Z}_p[[U^{(j)}]]$ be the homomorphism induced by the p-power map on $U^{(0)} \cong \mathbb{Z}_p^{\times}$. Setting $a_j = \mathcal{L}(E, \rho_j)$, one may then define

$$c_j \quad := \quad \frac{a_j \ \times \ \varphi \circ \mathrm{Norm}_{0,j-1}(a_0)}{\mathrm{Norm}_{0,j}(a_0) \ \times \ \varphi(a_{j-1})}$$

which belongs to the field of quotients $\mathrm{Frac}\left(\mathbb{Z}_p[\![U^{(j)}]\!]\right)$.

Theorem 6.1.3. *Under the same conditions as the previous result,*

$$\prod_{j=1}^{n} \mathrm{Norm}_{j,n}(c_j)^{p^j} \ \equiv \ 1 \mod p^{n+1}.\mathbb{Z}_p\big[\big[U^{(n)}\big]\big].$$

These congruences are analagous to the ones we obtained in [DW08] for semi-stable elliptic curves. As explained in Chapter 2, if these congruences hold modulo p^{2n} rather than modulo p^{n+1}, then one would establish the existence of a non-abelian p-adic L-function inside $K_1\big(\mathbb{Z}_p\big[\big[G_\infty\big]\big]_{S*}\big)$, as explained by Kato in [Kat05] §1.

Remark 6.1.4. Theorem 6.1.3 is a straightforward consequence of Theorem 6.1.2, courtesy of a strong induction argument. The details are identical to the proof of Theorem 4.6.7 in Chapter 4 and we shall not reproduce them here. This leaves us with the task of proving 6.1.2 in the next section.

Let us now consider Hida's automorphic p-adic L-function (see Definition 6.2.2). This object $\mathcal{L}^{\mathrm{Hida}}(E, \rho_n)$ interpolates exactly the same data as $\mathcal{L}(E, \rho_n)$, except that the period in its denominator is the Petersson self-product for the base-change of f_E to K_n^+, and there is an extra factor arising from the congruence module. If

$$\Omega^{\mathrm{mot}}_{K_n^+}(E) = \left(\Omega_E^+ \ \Omega_E^-\right)^{[K_n^+:\mathbb{Q}]} \qquad \text{and} \qquad \Omega^{\mathrm{aut}}_{K_n^+}(E) = \pi^{[K_n:\mathbb{Q}]}\big\langle \mathbf{f}_{/K_n^+}, \mathbf{f}_{/K_n^+}\big\rangle,$$

where $\mathbf{f}_{/K_n^+}$ denotes the base change of f_E to K_n^+, then one has the relationship

$$\mathcal{L}(E, \rho_n) \ = \ \frac{\Omega^{\mathrm{aut}}_{K_n^+}(E)}{\Omega^{\mathrm{mot}}_{K_n^+}(E)} \ \times \ \mathbf{H}_\lambda(\underline{2})^{-1} \ \times \ \mathcal{L}^{\mathrm{Hida}}(E, \rho_n) \quad \text{(up to a } p\text{-adic unit)}$$

where $\mathbf{H}_\lambda(\underline{2})$ denotes the value of the characteristic power series for the associated congruence module $C(\lambda_{E,K_n^+};\Lambda)$, evaluated at parallel weight two (see §1 for details). The p-adic L-function $\mathcal{L}^{\mathrm{Hida}}(E,\rho_n)$ arises from the Rankin convolution approach, and is heavily p-integral; but it appears to be the natural object to work with from an automorphic point of view.

Remark 6.1.5. In order to prove the full K_1-congruences of Kato, we first need to understand the analytic invariants

$$p^{\mu_{p,n}^{\mathrm{Per}}(E)} \;:=\; \left|\frac{\Omega_{K_n^+}^{\mathrm{mot}}(E)}{\Omega_{K_n^+}^{\mathrm{aut}}(E)}\right|_p^{-1} \qquad \text{and} \qquad p^{\mu_{p,n}^{\mathrm{anti}}(E)} \;:=\; \Big|\mathbf{H}_\lambda\big(2,\ldots,2\big)\Big|_p^{-1}$$

and their rate of growth as the fields K_n^+ climb up the cyclotomic $\mathbb{Z}_p$-extension.

Henceforth we shall assume that the prime p is greater than 3, and does not divide the degree of $X_0(N_E) \overset{\varphi_E}{\twoheadrightarrow} E$.

We now consider the two-variable Iwasawa module $\mathrm{Gal}\big(\mathcal{M}_\infty/K(E[p^\infty])\big)$ with $\mathcal{M}_\infty$ the maximal abelian pro-p-extension of $K\big(E[p^\infty]\big)$ unramified outside $\mathfrak{p}$. Let us define non-negative integers

$$\mu_E^{\mathrm{cy}} \;:=\; \sum_{j=0}^{p-2} \mu_{\omega^j}\big(\mathcal{Z}_{\infty,+}\big) \qquad \text{and} \qquad \lambda_E^{\mathrm{cy}} \;:=\; \sum_{j=0}^{p-2} \lambda_{\omega^j}\big(\mathcal{Z}_{\infty,+}\big)$$

where $\big(\mu_{\omega^j},\lambda_{\omega^j}\big)$ refer to the Iwasawa μ- and λ-invariants for the ω_K^j-eigenspace inside

$$\mathcal{Z}_{\infty,+} \;:=\; H^0\Big(K\big(E[p]\big)/K_1\,,\,\Big(\mathrm{Gal}\big(\mathcal{M}_\infty/K(E[p^\infty])\big)\otimes \Phi_{E,\mathfrak{p}}^{\otimes -2}\Big)_{\Gamma_-}\Big).$$

Theorem 6.1.6. *Assume the $\mu_{\omega^j}\big(\mathcal{Z}_{\infty,+}\big)$-invariants vanish at each integer $j \in \big\{0,\ldots,p-2\big\}$. For $n \gg 1$, the p-adic valuation of the ratio of motivic with the automorphic periods over K_n^+ is given by*

$$\mu_{p,n}^{\mathrm{Per}}(E) \;=\; n\big((p-1).p^{n-1} - \lambda_E^{\mathrm{cy}} + 1\big) - \Big(p^{n-1} + \nabla_{K_n^+}^{\mathrm{Sym}^2 E} + \mathrm{ord}_p\big(h^-(K_n)\big)\Big) + \; O(1)$$

where $\nabla_{K_n^+}^{\mathrm{Sym}^2 E}$ denotes the p-adic order of

$$\prod_{\text{places } \nu \mid N_E \text{ of } K_n^+} \det\left(1 - \Big(N_{K_n^+/\mathbb{Q}}(\nu)\Big)^{-s}.\,\mathrm{Frob}_\nu \Big|\, \big(\mathrm{Sym}^2 H_p^1(E)\big)^{I_\nu}\right)\Bigg|_{s=2}.$$

The demonstration of this result uses a version of the two-variable main conjecture, proved by Karl Rubin in the case of complex multiplication.

It is not difficult to calculate the terms $\nabla_{K_n^+}^{\mathrm{Sym}^2 E}$ which arise from the bad Euler factors of the symmetric square L-function. We give an algorithm for computing them in Appendix A.

Lastly we recall from [HT93] §0 that the anti-cyclotomic main conjecture over K_n^+ affirms that

$$\mathbf{H}_\lambda \ = (\text{a unit}) \ \times \ h^-(K_n) \ \times \ \mathbb{L}^-_{(K_n,\lambda)}\,,$$

where $\mathbb{L}^-_{(K_n,\lambda)}$ denotes the branch of the Katz p-adic L-function projected along the anti-cyclotomic $\mathbb{Z}_p$-extension of K_n^+, and $h^-(K_n)$ denotes the relative class number which is defined by

$$h^-(K_n) \ := \ \frac{h(K_n)}{h(K_n^+)}.$$

Therefore we have:

Corollary 6.1.7. *For all integers $n \gg 1$,*

$$\begin{aligned}\mathrm{ord}_p\left(\frac{\mathcal{L}^{\mathrm{Hida}}(E,\rho_n)}{\mathcal{L}(E,\rho_n)}\right) \ &= \ n\big((p-1).p^{n-1} - \lambda_E^{\mathrm{cy}} + 1\big) \ - \ \left(p^{n-1} + \nabla_{K_n^+}^{\mathrm{Sym}^2 E}\right) \\ &\quad + \ \mathrm{ord}_p\left(\mathbb{L}^-_{(K_n,\lambda)}\big(2,\ldots,2\big)\right) \ + \ \text{a fixed constant.}\end{aligned}$$

6.2 Elliptic Curves with Complex Multiplication

Let $E_{/\mathbb{Q}}$ be an elliptic curve with complex multiplication by an order in the ring of integers of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$. The following important result from CM theory relates the Hasse-Weil L-series of such elliptic curves to Hecke L-functions.

Proposition 6.2.1. *If F is a number field containing K, then there exists a canonical Hecke character*

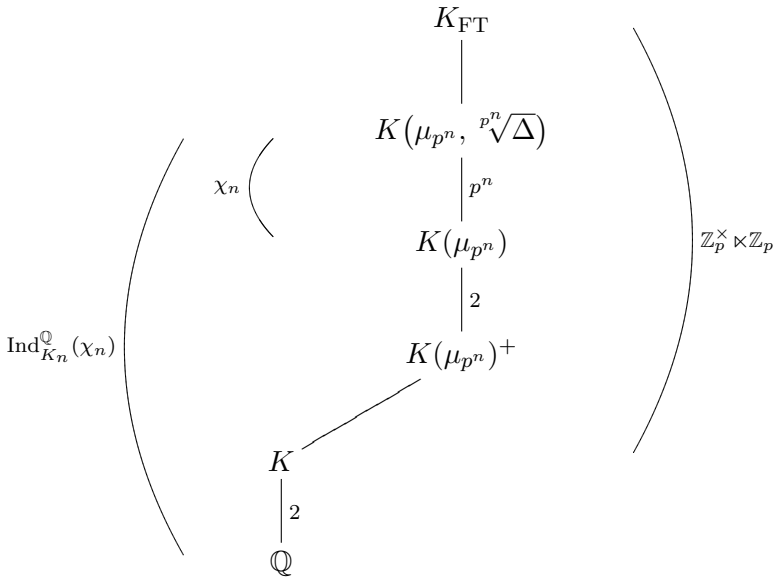
$$\Phi_{E/F} \ : \ \frac{F_{\mathbb{A}}^\times}{F^\times} \longrightarrow \overline{\mathbb{Q}}^\times$$

attached to $E_{/F}$*, such that*

$$L(E/F,s) \;=\; L(\Phi_{E/F},s)\;\; L(\overline{\Phi_{E/F}},s) \qquad \textit{and} \qquad L(E/F^{+},s) \;=\; L(\Phi_{E/F},s).$$

Proof. See Rubin's exposition [Rub99]. □

We refer to the Hecke character $\Phi_{E/F}$ as the *associated Grossencharacter* of E/F. Now, we recall our new false Tate curve tower from Section 6.1:



Remember that we always assume the prime p splits in $K/\mathbb{Q}$, which means that E has good ordinary reduction at p.

We want to specialise the results of Chapter 5 to the CM-field

$$M = K_n = \mathbb{Q}\big(\sqrt{-D},\ \mu_{p^n}\big),$$

choosing the Hecke characters $\lambda_{\mathcal{P}}$ and $\nu_{\mathcal{Q}}$ so that we obtain twisted L-values of E.

Let $\mathfrak{C} = \mathrm{cond}_{K_n}(E) \lhd \mathcal{O}_{K_n}$, and let us write $\mathbf{G}_\infty(\mathfrak{C}) = \mathrm{Gal}(K_n(\mathfrak{C}p^\infty)/K_n)$. As before, we decompose this Galois group into a product of the torsion part and the free part:

$$\mathbf{G}_\infty(\mathfrak{C}) \;=\; \mathbf{G}_{\mathrm{tor}}(\mathfrak{C}) \times \mathbf{W}.$$

The p-adic avatar of Φ_{E/K_n} factors through $\mathbf{G}_\infty(\mathfrak{C})$, so we may restrict it to $\mathbf{G}_{\rm tor}(\mathfrak{C})$; we put $\eta = \Phi_{E/K_n}\big|_{\mathbf{G}_{\rm tor}(\mathfrak{C})}$ and consider the projection

$$\eta_* \ : \ \mathcal{O}_{\mathbb{C}_p}[[\mathbf{G}_\infty(\mathfrak{C})]] \longrightarrow \Lambda_0 = \mathcal{O}_{\mathbb{C}_p}[[\mathbf{W}]].$$

Then we have the homomorphism

$$\lambda = \eta_* \circ \theta_N \ : \ \mathbf{h}(N; \mathcal{O}_{\mathbb{C}_p}) \longrightarrow \Lambda_0$$

at level $N = \mathfrak{C}\mathfrak{C}^c\,\mathrm{Disc}(K_n/K_n^+)$, which corresponds by duality to the base-change of $f_E \in \mathcal{S}_2\big(\Gamma_0(N_E)\big)$ over K_n^+.

Let us take $\mathcal{P} : \Lambda_0 \to \overline{\mathbb{Q}}_p$ to be the specialisation at weight $\underline{k} = (2, \ldots, 2)$, and put

$$\lambda_{\mathcal{P}} = \mathcal{P} \circ \eta_* \ : \ \mathbf{G}_\infty(\mathfrak{C}) \longrightarrow \overline{\mathbb{Q}}_p^\times.$$

Then the Hilbert modular form $\theta(\lambda_{\mathcal{P}})$ will be the base-change of f_E to K_n^+, and its L-series coincides with

$$L(E/K_n^+, s) \ = \ L(\Phi_{E/K_n}, s).$$

Now recall that, for j in the range $\{0, \ldots, n\}$, we have the anti-cyclotomic character

$$\chi_j \ : \ \mathrm{Gal}\left(K_j\big(\sqrt[p^j]{\Delta}\big)/K_j\right) \longrightarrow \mu_{p^j} \qquad \text{given by} \qquad \sigma \longmapsto \frac{\sigma\big(\sqrt[p^j]{\Delta}\big)}{\sqrt[p^j]{\Delta}}$$

which induces the Artin representation ρ_j over the quadratic field K. Let us also fix a character $\psi : U^{(n)} \to \overline{\mathbb{Q}}^\times$ of finite order.

Suppose that $\mathfrak{C}' \lhd \mathcal{O}_{K_n}$ is divisible by the conductor of $\mathrm{Res}_{K_n}(\chi_j) \otimes \psi$. This character will factor through the group $\mathbf{G}_\infty(\mathfrak{C}') = \mathrm{Gal}(K_n(\mathfrak{C}'p^\infty)/K_n)$, which has the same free part $\mathbf{W}$ as $\mathbf{G}_\infty(\mathfrak{C})$. So, if we put

$$\gamma \ = \ \mathrm{Res}_{K_n}(\chi_j) \otimes \psi\Big|_{\mathbf{G}_{\rm tor}(\mathfrak{C}')}$$

we have a projection

$$\gamma_* \ : \ \mathcal{O}[[\mathbf{G}_\infty(\mathfrak{C}')]] \ \xrightarrow{\gamma_*} \ \Lambda_0 = \mathcal{O}_{\mathbb{C}_p}[[\mathbf{W}]]$$

and a morphism

$$\nu = \nu(j,n,\psi) \ : \ \mathbf{h}(N';\mathcal{O}_{\mathbb{C}_p}) \ \stackrel{\gamma_*\circ\theta_{N'}}{\longrightarrow} \ \Lambda_0$$

at level $N' = \mathfrak{C}'\mathfrak{C}'^c \operatorname{Disc}(K_n/K_n^+)$. We compose this with the arithmetic specialisation $\mathcal{Q}$ at weight $\underline{k}' = (1,\ldots,1)$ with character $\operatorname{Res}_{K_n}(\chi_j)\otimes\psi\Big|_{\mathbf{W}}$, and we get a unique Hecke character

$$\nu_{\mathcal{Q}} = \mathcal{Q}\circ\gamma_* \ : \ \mathbf{G}_\infty(\mathfrak{C}') \longrightarrow \ \overline{\mathbb{Q}}_p.$$

Clearly $\nu_{\mathcal{Q}}$ is a unitary Hecke character, moreover $\theta\big(\nu_{\mathcal{Q}}(j,n,\psi)\big)$ is the primitive Hilbert modular form associated to the $\operatorname{Gal}\big(\overline{\mathbb{Q}}/K_n^+\big)$-representation

$$\operatorname{Ind}_{K_n}^{K_n^+}\big(\operatorname{Res}_{K_n}(\chi_j)\big)\otimes\psi$$

via the work of Serre (analogous to the form $\mathbf{g}_{\rho_j/K_n}$ from Chapter 3).

Now we ask the question: what L-value data does the pair $(\lambda_{\mathcal{P}},\nu_{\mathcal{Q}})$ interpolate? Recall from Theorem 5.9.2 that the value of Hida's p-adic L-function is given by

$$\mathfrak{D}_{\lambda,\nu}(\mathcal{P},\mathcal{Q}) \ = \ \frac{\mathfrak{D}_p\Big(\theta(\lambda_{\mathcal{P}}),\ \theta(\nu_{\mathcal{Q}})^\vee, 1+\dfrac{m(\mathcal{Q})-m(\mathcal{P})}{2}\Big)}{\big\langle\theta(\lambda_{\mathcal{P}})\otimes\eta'_{\mathcal{P}},\ \theta(\lambda_{\mathcal{P}})\otimes\eta'_{\mathcal{P}}\big\rangle},$$

up to certain interpolation factors defined in [HT93]. Applying standard properties of the theta-lift given in Lemma 5.9.1, we get

$$\begin{aligned}\mathfrak{D}_p\big(\theta(\lambda_{\mathcal{P}}),\theta(\nu_{\mathcal{Q}})^\vee,1/2\big) \ &= \ L_p\big(\lambda_{\mathcal{P}}^u\nu_{\mathcal{Q}}^{cu},1/2\big)\ .\ L_p\big(\lambda_{\mathcal{P}}^u\nu_{\mathcal{Q}}^{[c]u},1/2\big)\\ &= \ L_p\Big((\Phi_{E/K_n})^u\nu_{\mathcal{Q}}^c,1/2\Big)\ .\ L_p\Big((\Phi_{E/K_n})^u\nu_{\mathcal{Q}}^{[c]},1/2\Big).\end{aligned}$$

By definition of the unitarised Hecke character $(\Phi_{E/K_n})^u$, we have

$$L\big((\Phi_{E/K_n})^u,1/2\big) \ = \ L(\Phi_{E/K_n},1).$$

So, after unravelling the unitarisation and removing the Euler factor contribution coming from the $E(\mathcal{P},\mathcal{Q})$ term, we obtain the special value

$$L_{\{p\Delta\}}\big(E/K_n,\ \operatorname{Res}_{K_n}(\chi_j)^c\otimes\psi^{-1},1\big) \ = \ \prod_\beta L_{\{p\Delta\}}\big(E/K,\rho_j\otimes\beta\psi^{-1},1\big)\ ,$$

where β ranges over all characters $\operatorname{Gal}(K_n/K_j)\to\mathbb{C}^\times$. This motivates the following definition.

Definition 6.2.2. *We define the p-adic L-function* $\mathcal{L}^{\mathrm{Hida}}(E, \rho_j/K_n^+)$ *to be the unique element of* $\mathcal{O}_{\mathbb{C}_p}[[U^{(n)}]]$ *such that for all finite-order characters* $\psi : U^{(n)} \to \overline{\mathbb{Q}}^\times$ *we have*

$$\psi\left(\mathcal{L}^{\mathrm{Hida}}(E, \rho_j/K_n^+)\right) \;=\; (\mathbf{H}_\lambda(\mathcal{P}) \otimes 1)\,.\,\mathfrak{D}_{\lambda,\nu}(\mathcal{P}, \mathcal{Q})$$

for the specialisations $\lambda_{\mathcal{P}}$ *and* $\nu_{\mathcal{Q}} = \nu_{\mathcal{Q}}(j, n, \psi)$ *defined above.*

Note that we are forced to include the congruence power series term $\mathbf{H}_\lambda(\mathcal{P})$ to ensure the p-adic L-function is integral (see Theorem 5.9.2).

Comparing this p-adic L-function to the one defined in 6.1.1, the calculation of the special value above shows that

$$\begin{aligned}\psi\left(\mathcal{L}^{\mathrm{Hida}}(E, \rho_j/K_n^+)\right) \;&=\; \frac{\left(\pi^{-2}\,\Omega_E^+\,\Omega_E^-\right)^{[K_n^+:\mathbb{Q}]}}{\left\langle \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}}, \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}} \right\rangle} \;\times\; \mathbf{H}_\lambda(\mathcal{P}) \\ &\times\; \psi\Big(\mathrm{Norm}_{j,n}\big(\mathcal{L}(E, \rho_j)\big)\Big)\,.\end{aligned}$$

We know that the interpolation factors agree by Remark 5.9.3.

The first two terms in the product are non-zero scalars - in particular, they do not depend on how the character ψ is chosen, nor on the Artin representation ρ_j. We will estimate the power of p occurring in these scalars later in this chapter.

Definition 6.2.3. *We define the automorphic error term associated to* E *and the field* K_n^+ *by*

$$\mathbf{Err}_{K_n^+}(E) \;:=\; \frac{\left(\pi^{-2}\,\Omega_E^+\,\Omega_E^-\right)^{[K_n^+:\mathbb{Q}]}}{\left\langle \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}}, \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}} \right\rangle} \;\times\; \Big|\mathbf{H}_\lambda(\mathcal{P})\Big|_p^{-1}.$$

This term measures the ratio of the 'automorphic' L-function $\mathcal{L}^{\mathrm{Hida}}(E, \rho_j/K_n^+)$ with its motivic counterpart $\mathrm{Norm}_{j,n}\big(\mathcal{L}(E, \rho_j)\big)$.

We are now in a position to prove the main result of this section.

Proof of Theorem 6.1.2.

The family of automorphic L-functions

$$\mathfrak{D}_{\lambda,\nu}(\mathcal{P},-)\Big|_{\mathcal{O}_{\mathbb{C}_p}[[U^{(n)}]]} \quad \text{associated to} \quad \gamma = \mathrm{Res}_{K_n}(\chi_j)\otimes\psi\Big|_{\mathbf{G}_{\mathrm{tor}}(\mathfrak{C}')}$$

share a common μ-invariant, for all $j \in \{0,\ldots,n\}$ and fixed character $\psi\big|_{\mathbf{G}_{\mathrm{tor}}(\mathfrak{C}')}$ (as switching γ's does not change the branch of the underlying ray-class measure). This means that the elements

$$\mathcal{L}^{\mathrm{Hida}}(E,\rho_j/K_n^+) \;\in\; \mathcal{O}_{\mathbb{C}_p}[[U^{(n)}]]$$

have a common μ-invariant for $0 \le j \le n$.

Hypothesis **(I,** n**)** implies that the norm of each motivic p-adic L-function $\mathcal{L}(E,\rho_j)$ is p-integral. Moreover, under Hypothesis **(II)** the μ-invariant of $\mathrm{Norm}_{0,1}\big(\mathcal{L}(E,\rho_0)\big)$ is trivial, hence the μ-invariant of $\mathrm{Norm}_{0,n}\big(\mathcal{L}(E,\rho_0)\big)$ must also vanish for every $n \ge 1$. Since we have

$$\mathcal{L}^{\mathrm{Hida}}(E,\rho_0/K_n^+) \;=\; \mathbf{Err}_{K_n^+}(E) \;\times\; \mathrm{Norm}_{0,n}\big(\mathcal{L}(E,\rho_0)\big),$$

it follows that the quantity $\mathrm{ord}_p\Big(\mathbf{Err}_{K_n^+}(E)\Big)$ coincides with the μ-invariant of $\mathcal{L}^{\mathrm{Hida}}(E,\rho_0/K_n^+)$. It will be equal to the common μ-invariant shared by $\mathcal{L}^{\mathrm{Hida}}(E,\rho_j/K_n^+)$ for all j.

Because $\mathrm{Res}_{K_n}(\chi_j)$ takes values in μ_{p^∞}, such characters are congruent to 1 modulo $\mathfrak{M}_{\mathbb{C}_p}$, the maximal ideal of $\mathcal{O}_{\mathbb{C}_p}$. Thus each residual specialisation

$$\big(\lambda_{\mathcal{P}},\ \nu_{\mathcal{Q}}(j,n,\psi)\big)\ :\ \mathbf{h}(N;\mathcal{O}_{\mathbb{C}_p})\,\widehat{\otimes}_{\mathcal{O}_{\mathbb{C}_p}}\,\mathbf{h}(N';\mathcal{O}_{\mathbb{C}_p}) \longrightarrow \mathcal{O}_{\mathbb{C}_p} \twoheadrightarrow \mathcal{O}_{\mathbb{C}_p}/\mathbf{Err}_{K_n^+}(E)\,.\,\mathfrak{M}_{\mathbb{C}_p}$$

whilst dependent on n and ψ, is independent of the choice of $j \in \{0,\ldots,n\}$. This implies that

$$\big(\mathbf{H}_\lambda(\mathcal{P})\otimes 1\big)\,.\,\mathfrak{D}_{\lambda,\nu}(\mathcal{P},\mathcal{Q}) \mod \mathbf{Err}_{K_n^+}(E)\,.\,\mathfrak{M}_{\mathbb{C}_p}$$

must also be independent of the choice of $j \in \{0,\ldots,n\}$, for all finite order characters ψ of $U^{(n)}$. Therefore,

$$\mathcal{L}^{\mathrm{Hida}}(E,\rho_j/K_n^+) \mod \mathbf{Err}_{K_n^+}(E)\,.\,\mathfrak{M}_{\mathbb{C}_p}[[U^{(n)}]]$$

is independent of j, and we obtain the congruence

$$\mathcal{L}(E,\rho_n) \;\equiv\; \mathrm{Norm}_{j,n}\big(\mathcal{L}(E,\rho_j)\big) \mod \mathfrak{M}_{\mathbb{C}_p}[[U^{(n)}]].$$

Finally we apply the algebraicity result of Bouganis and Dokchitser ([BD07] Theorem 4.2) as we did in the semistable case. This result shows that the algebraic part of $L(E,\rho,1)$ lies in the field of definition of E and ρ, when ρ factors through a false Tate curve extension. The elliptic curve E and the self-dual representations $\mathrm{Ind}_K^{\mathbb{Q}}(\rho_n)$ are all realisable over $\mathbb{Q}$, so the above congruence strengthens to one modulo

$$\mathfrak{M}_{\mathbb{C}_p}[[U^{(n)}]] \;\cap\; \mathbb{Q}_p[[U^{(n)}]] \;=\; p\,.\,\mathbb{Z}_p[[U^{(n)}]]$$

and this completes the proof of Theorem 6.1.2. □

6.3 Calculating the Ratio of Motivic and Automorphic Periods

We now describe the numerical ratio of $\mathcal{L}(E,\rho_n)$ with its automorphic counterpart. Under the hypotheses of Theorem 6.1.2, this ratio corresponds to the μ-invariant of $\mathcal{L}^{\mathrm{Hida}}(E,\rho_j/K_n^+)$ precisely. From Definition 6.2.3, it can be written as

$$\mathrm{ord}_p\Big(\mathbf{Err}_{K_n^+}(E)\Big) \;=\; \mu_{p,n}^{\mathrm{anti}}(E) \;+\; \mu_{p,n}^{\mathrm{Per}}(E)$$

where

$$\begin{aligned}\mu_{p,n}^{\mathrm{anti}}(E) &= \mathrm{ord}_p\big(\mathbf{H}_\lambda(\mathcal{P})\big)\\ &= \mathrm{ord}_p\big(h(K_n)\big) \;-\; \mathrm{ord}_p\big(h(K_n^+)\big) \;+\; \mathrm{ord}_p\big(\mathbb{L}^-_{(K_n,\lambda)}(\mathcal{P})\big)\end{aligned}$$

by Theorem 5.8.2, and secondly

$$\mu_{p,n}^{\mathrm{Per}}(E) \;=\; \mathrm{ord}_p\left(\frac{\big(\pi^{-2}\,\Omega_E^+\,\Omega_E^-\big)^{[K_n^+:\mathbb{Q}]}}{\big\langle\theta(\lambda_\mathcal{P})\otimes\eta'_\mathcal{P},\theta(\lambda_\mathcal{P})\otimes\eta'_\mathcal{P}\big\rangle}\right).$$

Theorem 6.3.1. *In the notation of* [Kat78] §5.7.8-9*, the value* $\mathbb{L}^{-}_{(K_n,\lambda)}(\mathcal{P})$ *is given by*

$$\begin{aligned}\frac{\mathbb{L}^{-}_{(K_n,\lambda)}(\mathcal{P})}{\Omega_p^{m_0\Sigma+2d}} &= \Big[\mathcal{O}_{K_n}^{\times} : \mathcal{O}_{K_n^+}^{\times}\Big] \,.\, W_p\big((\lambda\circ c)\,.\,\lambda^{-1}\big)\,.\,\frac{(-1)^{m_0\Sigma}}{\sqrt{\mathrm{Disc}(K_n^+)}} \\ &\times \quad \frac{L_{\mathfrak{p},\mathfrak{p}^*}\Big(\big(\lambda\circ c\big)_{\mathcal{P}}.\lambda_{\mathcal{P}}^{-1},0\Big)}{\pi^{-d}\,\Omega_\infty^{m_0\Sigma+2d}}\end{aligned}$$

where $\lambda_{\mathcal{P}} = (\Phi_{E/K_n})^u$*,* W_p *is a root number, and* (Ω_∞,Ω_p) *denote the Katz periods.*

Proof. This follows directly from the interpolation formula given in Proposition 5.5.1. □

From a computational perspective, most of these terms are straightforward to work out. For example the index $\big[\mathcal{O}_{K_n}^{\times} : \mathcal{O}_{K_n^+}^{\times}\big]$ is just a power of p, and the root number W_p can be expressed as a Gauss sum. The p-adic period Ω_p is always a p-adic unit.

Let us now concentrate on computing the quantity $\mu_{p,n}^{\mathrm{Per}}(E)$ numerically. For any Dirichlet character ψ whose conductor is coprime to that of E, we will write $L^{\mathrm{imp}}(\mathrm{Sym}^2 E,\psi,s)$ for the imprimitive ψ-twisted symmetric square L-series. Recall that the imprimitive symmetric square L-series may be defined by the Euler product

$$L^{\mathrm{imp}}(\mathrm{Sym}^2 E,s) \;:=\; \prod_q \Big((1-\alpha_q^2\,q^{-s})(1-\alpha_q\,\alpha_q'\,q^{-s})(1-\alpha_q'^2\,q^{-s})\Big)^{-1}$$

where as usual $1-a_q(E)\,T+q\,T^2 \;=\; (1-\alpha_q\,T)(1-\alpha_q'\,T)$ for each rational prime q. We write

$$\tau(\psi) \;=\; \sum_{a=1}^{f_\psi}\psi(a)e^{2\pi i a/f_\psi},$$

for the standard Gauss sum of ψ, and define

$$\xi(E/K_n^+) \quad := \prod_{\psi:\mathrm{Gal}(K_n^+/\mathbb{Q})\to\mathbb{C}^\times} \frac{\tau(\psi^{-2})L^{\mathrm{imp}}(\mathrm{Sym}^2E,\psi,2)}{\pi^3\langle f_E,f_E\rangle_{N_E}}$$

which is $\mathrm{Aut}(\mathbb{C})$-invariant (and hence rational) due to results of Sturm [Stu80, Stu89].

Proposition 6.3.2. *If the prime $p \neq 2$ does not divide the degree of the modular parametrisation $X_0(N_E) \overset{\varphi_E}{\twoheadrightarrow} E$ or the Manin constant of E, then*

$$\frac{\langle \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}}, \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}} \rangle}{\left(\pi^{-2}\, \Omega_E^+\, \Omega_E^-\right)^{[K_n^+:\mathbb{Q}]}} \;=\; (\,p-\text{adic unit}) \;\times\; \frac{\left|\mathrm{Disc}(K_n^+)\right|_\infty}{\left|\mathrm{Disc}(\mathbb{Q}(\mu_{p^n})^+)\right|_\infty} \;\times\; \xi(E/K_n^+).$$

The demonstration of this result is given at the end of this section.

It is a basic exercise in the arithmetic of cyclotomic fields to show that

$$\mathrm{ord}_p\Big(\mathrm{Disc}(K_n^+)\Big) \;=\; p^{n-1}(pn-n-1)$$

and

$$\mathrm{ord}_p\Big(\mathrm{Disc}\big(\mathbb{Q}(\mu_{p^n})^+\big)\Big) \;=\; \big(p^{n-1}(pn-n-1)-1\big)/2.$$

The calculation of the period ratio therefore reduces to a computation of ψ-twisted symmetric square L-series at $s=2$. Using the computer package MAGMA (see [BCP97]) and the subroutine *LSeries*, we attempted to compute these L-values and obtain $\xi(E/K_n^+)$ as a rational number; more details on the computations are given in Appendix B.

Unfortunately, the conductors of the twists $\mathrm{Sym}^2 E \otimes \psi$ get very large as n increases, and we were forced to restrict ourselves to the layer $n=1$. We focus on the first three CM elliptic curves over $\mathbb{Q}$ of rank zero and minimal conductor; in Cremona's notation they are $27A(1)$, $32A(1)$ and $49A(1)$.

We also want to check numerically whether the p-primary Selmer group $\mathrm{Sel}_{K_{FT}}(E)_{p^\infty}$ is trivial. For this we quote a result of Hachimori and Venjakob. First, if $\mathcal{S}$ is a p-primary G_∞-module (recall that $G_\infty = \mathrm{Gal}(K_{FT}/K)$), one may define the Euler characteristic

$$\mathbf{EC}\,(G_\infty, \mathcal{S}) \;:=\; \prod_{j=0}^{\infty} \#\Big(H^j\big(G_\infty, \mathcal{S}\big)\Big)^{(-1)^j}$$

assuming that the Galois cohomology groups $H^j(G_\infty, \mathcal{S})$ are finite for all j.

Proposition 6.3.3. *Suppose the analytic rank of $E/K(\mu_p)$ is zero. The p-primary Selmer group of E over the p-adic Lie extension K_{FT} is trivial if and only if*

$$\mathbf{EC}\big(G_\infty, \mathrm{Sel}_{K_{\mathrm{FT}}}(E)_{p^\infty}\big) = 1.$$

Proof. See [HV03] Prop 4.12. □

The latter Euler characteristic will coincide with the leading term of $\mathrm{Norm}_{0,1}\big(\mathcal{L}_p(E,\rho_0)\big)$ up to a unit, provided the full Birch and Swinnerton-Dyer conjecture holds for E over $K(\mu_p)$. Therefore we want to check whether $\mathrm{Norm}_{0,1}\big(\mathcal{L}_p(E,\rho_0)\big)$ evaluated at the trivial character is a p-adic unit.

Let us define the quantity

$$\mathcal{X}_E(\rho) \;:=\; \epsilon_p(\rho)\times\frac{P_p(\rho^\vee,\alpha_p^{-1})}{P_p(\rho,p^{-1}\alpha_p)}\times\alpha_p^{-\mathfrak{f}_p(\rho)}\times\frac{L_{\{p\Delta\}}(E,\rho,1)}{(\Omega_E^+)^{\dim^+\rho}\,(\Omega_E^-)^{\dim^-\rho}}\,,$$

which is the conjectural p-adic L-value of $\mathcal{L}_{E/K_{FT}}$ evaluated at the Artin representation ρ. We want to check whether $\mathcal{X}_E\left(\mathrm{Reg}_{K(\mu_p)/\mathbb{Q}}\right)$ is a unit, but it is sufficient to compute $\mathcal{X}_E\left(\mathrm{Reg}_{\mathbb{Q}(\mu_p)/\mathbb{Q}}\right)$ because

$$\mathbf{1}\big(\mathrm{Norm}_{0,1}\big(\mathcal{L}_p(E,\rho_0)\big)\big)\;=\;\mathcal{X}_E\left(\mathrm{Reg}_{\mathbb{Q}(\sqrt{-D},\mu_p)/\mathbb{Q}}\right)=\mathcal{X}_E\left(\mathrm{Reg}_{\mathbb{Q}(\mu_p)/\mathbb{Q}}\right)^2,$$

as the quadratic twist $E\otimes\left(\frac{-D}{\cdot}\right)$ is always $\mathbb{Q}$-isogenous to the original elliptic curve. Bearing in mind our formula for $\mu_{p,n}^{\mathrm{Per}}(E)$ given in 6.1.6 when $n\gg 1$, we make the following definition.

Definition 6.3.4. *For each triple (E,p,Δ) as before, we write*

$$\mu_{p,1}^{\mathrm{naive}}(E)\;:=\;(p-1)\;-\;\nabla_{K_1^+}^{\mathrm{Sym}^2E}\;-\;\mathrm{ord}_p\big(h^-(K_1)\big)$$

which is a naive estimate of the value $\mu_{p,n}^{\mathrm{Per}}(E)$ at the bottom layer $n=1$.

The following tables show the data we computed for our chosen elliptic curves. For each case in which the analytic rank of $E/K(\mu_p)$ is zero, we have chosen a value of Δ in order to compute $\mathcal{X}_E\left(\mathrm{Reg}_{\mathbb{Q}(\mu_p)/\mathbb{Q}}\right)$. Note that we have chosen each Δ so that the removed Euler factor is a p-adic unit. Whenever $\mu_{p,1}^{\mathrm{Per}}$ and $\mu_{p,1}^{\mathrm{naive}}$ differ in value, we have highlighted the latter in boldface.

Table 6.1: The elliptic curve $E = 27A(1) : y^2 + y = x^3$.

p	Δ	$\mathcal{X}_E(\mathrm{Reg}_{\mathbb{Q}(\mu_p)/\mathbb{Q}})$	$\mathrm{Sel}_{K_{FT}}(E)_{p^\infty} = 0$?	$\mu_{p,1}^{\mathrm{Per}}$	$\mu_{p,1}^{\mathrm{naive}}$
7	2	$1.7^0 + 3.7^1 + 1.7^2 + O(7^3)$	Yes	4	**5**
13	2	$7.13^0 + 5.13^1 + 9.13^2 + O(13^3)$	Yes	10	10
19	-	0	No	17	17
31	-	0	No	29	29
37	-	0	No	33	33
43	7	$24.43^0 + 20.43^1 + 1.43^2 + O(43^3)$	Yes	41	41
61	2	$16.61^0 + 50.61^1 + 46.61^2 + O(61^3)$	Yes	53	**54**
67	17	$53.67^0 + 21.67^1 + 52.67^2 + O(67^3)$	Yes	61	61
73	2	$13.73^2 + 13.73^4 + 20.73^5 + O(73^6)$	No	64	**66**
79	2	$50.79^0 + 77.79^1 + 55.79^2 + O(79^3)$	Yes	75	**77**
97	2	$87.97^2 + 88.97^3 + 29.97^4 + O(97^5)$	No	94	94
103	2	$79.103^0 + 96.103^1 + O(103^2)$	Yes	97	97
109	-	0	No	104	**106**
127	-	0	No	125	125
139	5	$12.139^0 + 87.139^1 + O(139^2)$	Yes	136	136
151	2	$5.151^2 + 1.151^3 + O(151^4)$	No	143	**147**
157	2	$3.157^0 + 17.157^1 + O(157^2)$	Yes	152	152
163	13	$119.163^2 + 35.163^3 + O(163^4)$	No	161	161
181	-	0	No	176	**178**
193	2	$1.193^0 + 52.193^1 + O(193^2)$	Yes	180	180
199	2	$32.199^2 + 57.199^3 + O(199^4)$	No	194	**196**

Table 6.2: The elliptic curve $E = 32A(1) : y^2 = x^3 + 4x$.

p	Δ	$\mathcal{X}_E(\mathrm{Reg}_{\mathbb{Q}(\mu_p)/\mathbb{Q}})$	$\mathrm{Sel}_{K_{FT}}(E)_{p^\infty} = 0$?	$\mu_{p,1}^{\mathrm{Per}}$	$\mu_{p,1}^{\mathrm{naive}}$
5	-	0	No	3	3
13	-	0	No	11	11
17	-	0	No	14	14
29	-	0	No	27	27
37	-	0	No	34	34
41	-	0	No	38	38
53	-	0	No	51	51
61	-	0	No	56	**58**
73	3	$35.73^0 + 26.73^1 + 61.73^2 + O(73^3)$	Yes	68	68
89	3	$67.89^0 + 13.89^1 + 59.89^2 + O(89^3)$	Yes	82	**84**
97	3	$9.97^0 + 2.97^1 + 29.97^2 + O(97^3)$	Yes	94	94
101	-	0	No	97	97
109	-	0	No	105	105
113	3	$106.113^2 + 20.113^3 + O(113^4)$	No	108	108
137	-	0	No	131	**133**
149	-	0	No	145	145
157	-	0	No	149	**151**
173	-	0	No	171	171
181	-	0	No	179	179
193	3	$166.193^2 + 178.193^3 + O(193^4)$	No	187	**189**

Table 6.3: The elliptic curve $E = 49A(1) : y^2 + xy = x^3 - x^2 - 2x - 1$.

p	Δ	$\mathcal{X}_E(\mathrm{Reg}_{\mathbb{Q}(\mu_p)/\mathbb{Q}})$	$\mathrm{Sel}_{K_{FT}}(E)_{p^\infty} = 0$?	$\mu_{p,1}^{\mathrm{Per}}$	$\mu_{p,1}^{\mathrm{naive}}$
11	-	0	No	6	**8**
23	-	0	No	20	20
29	3	$18.29^0 + 2.29^1 + 10.29^2 + O(29^3)$	Yes	25	25
37	5	$32.37^0 + 10.37^1 + 22.37^3 + O(37^4)$	Yes	33	33
43	-	0	No	24	**28**
53	-	0	No	44	**46**
67	-	0	No	61	**63**
71	-	0	No	66	**68**
79	-	0	No	76	76
107	-	0	No	104	104
109	2	$39.109^2 + 34.109^3 + O(109^4)$	No	105	105
113	2	$77.113^0 + 46.113^1 + O(113^2)$	Yes	95	95
127	-	0	No	124	124
137	3	$3.137^2 + 54.137^3 + O(137^4)$	No	128	**130**
149	-	0	No	141	141
151	-	0	No	146	**148**
163	-	0	No	156	**160**

After some thought, we verified numerically that in all cases our naive guess coincides with the true value, if and only if the Katz-Yager L-values

$$\mathbb{L}_{\mathrm{Katz}}\Big(\Phi^2_{E,\mathfrak{p}} \times \omega_K^j\Big) \quad \text{for all} \quad j \in \big\{0, \ldots, p-2\big\}$$

are simultaneously p-units. If this condition does not hold, one expects non-triviality of either the μ_E^{cy}- or λ_E^{cy}-invariants, which will contribute to the final formula.

Conjecture 6.3.5. *If this p-unit condition on the constant terms of $\mathbb{L}_{\mathrm{Katz}}$ is satisfied, then*

$$\mu_{p,1}^{\mathrm{Per}}(E) \quad = \quad \mu_{p,1}^{\mathrm{naive}}(E) \quad := \quad (p-1) - \nabla_{K_1^+}^{\mathrm{Sym}^2 E} - \mathrm{ord}_p\big(h^-(K_1)\big)\ .$$

If this condition is not satisfied, we instead have $\mu_{p,1}^{\mathrm{Per}}(E) < \mu_{p,1}^{\mathrm{naive}}(E)$.

This prediction is true for all the examples we have calculated, and we are optimistic that it holds more generally. If it does hold, it means that the $O(1)$-term occurring in Theorem 6.1.6 is precisely the constant zero.

Proof of Proposition 6.3.2.
Our starting point is the formula from [HT93] §7 which relates the Petersson self-product of a Hilbert modular form to the imprimitive adjoint L-function.

$$\begin{aligned}\big\langle \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}}, \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}} \big\rangle_N \quad &= \quad \big|\mathrm{Disc}(K_n^+)\big|_\infty \ \times\ N_{K_n^+/\mathbb{Q}}(N) \times 2^{-2\{2\}+1} \\ &\times \quad \pi^{-[K_n^+:\mathbb{Q}]-\{2\}} \ \times\ L^{\mathrm{imp}}\big(\mathrm{Ad}(\theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}}), 1\big)\end{aligned}$$

where $N = \mathfrak{C} \times \mathfrak{C}^c \times D_{K_n/K_n^+}$ was the level of $\theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}}$. We do not give the definition of the adjoint L-function, as it can be identified with that of the symmetric square for the base-change of f_E/K_n^+. Following renormalisation, one deduces that $\big\langle \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}}, \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}} \big\rangle_N$ is equal to

$$\big|\mathrm{Disc}(K_n^+)\big|_\infty \ \pi^{-[K_n^+:\mathbb{Q}]-\{2\}} \ \times\ L^{\mathrm{imp}}\big(\mathrm{Sym}^2 E/K_n^+, 2\big),$$

up to a p-adic unit.

The field K_n^+ is an abelian extension of $\mathbb{Q}$, and so the L-function decomposes as a product over the characters of $G = \mathrm{Gal}(K_n^+/\mathbb{Q})$. As an immediate consequence

$$\begin{aligned}\big\langle \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}}, \theta(\lambda_{\mathcal{P}}) \otimes \eta'_{\mathcal{P}} \big\rangle_N &\approx \big|\mathrm{Disc}(K_n^+)\big|_\infty \prod_{\psi: G \to \mathbb{C}^\times} \pi^{-3} L^{\mathrm{imp}}(\mathrm{Sym}^2 E, \psi, 2) \\ &\approx \big|\mathrm{Disc}(K_n^+)\big|_\infty \, \xi(E/K_n^+) \prod_{\psi: G \to \mathbb{C}^\times} \frac{\langle f_E, f_E \rangle_{N_E}}{\tau(\psi^{-2})}\end{aligned}$$

where '$\approx$' denotes equality up to p-adic units. The proof will be finished, provided we can show:

$$\textbf{(a)} \qquad \prod_{\psi: G \to \mathbb{C}^\times} \tau(\psi^{-2}) \;=\; \Big|\mathrm{Disc}\big(\mathbb{Q}(\mu_{p^n})^+\big)\Big|_\infty,$$

$$\textbf{(b)} \qquad \langle f_E, f_E \rangle_{N_E} \;=\; \big(p\text{-adic unit}\big) \;\times\; \pi^{-2}\, \Omega_E^+\, \Omega_E^-.$$

Since we assume that both the degree of $\varphi_E : X_0(N_E) \twoheadrightarrow E$ and its Manin constant c_{Man} are integers coprime to p, then **(b)** follows from the well-known identity

$$\frac{8\pi^3}{N_E} \langle f_E, f_E \rangle_{N_E} \;=\; L^{\mathrm{imp}}(\mathrm{Sym}^2 E, 2) \;=\; \frac{\deg(\varphi_E)}{N_E . c_{\mathrm{Man}}^2} \times \pi i \int_{E(\mathbb{C})} \omega_E \wedge \overline{\omega_E} \;\; .$$

To show claim **(a)**, clearly we must have

$$\prod_{\psi: G \to \mathbb{C}^\times} \tau(\psi^{-2}) \;=\; \left(\prod_{\psi: G^2 \to \mathbb{C}^\times} \tau(\overline{\psi}) \right)^2.$$

If the automorphism $\sigma \in \mathrm{Gal}\big(K_n/\mathbb{Q}(\mu_{p^n})\big)$ sends $\sqrt{-D} \mapsto -\sqrt{-D}$, then

$$\mathrm{Gal}(K_n/\mathbb{Q}) \;\cong\; \langle \sigma \rangle \times \mathbb{F}_p^\times \times C_{p^{n-1}} \quad \text{whence} \quad G \;\cong\; \frac{\langle \sigma \rangle \times \mathbb{F}_p^\times}{\big\langle (\sigma, -1) \big\rangle} \times C_{p^{n-1}} \; .$$

Because p is odd, the field cut out by $G^2 \cong \big(\mathbb{F}_p^\times\big)^2 \times C_{p^{n-1}}$ has to be $\mathbb{Q}(\mu_{p^n}) \cap \mathbb{R}$. Via standard properties of Gauss sums and the conductor-discriminant formula, we arrive at

$$\prod_{\psi: G^2 \to \mathbb{C}^\times} \tau(\overline{\psi})^2 \quad = \quad \prod_{\psi: \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})^+/\mathbb{Q}) \to \mathbb{C}^\times} \psi(-1)\, f_\psi \quad = \quad \Big|\mathrm{Disc}\big(\mathbb{Q}(\mu_{p^n})^+\big)\Big|_\infty$$

and the result follows.

6.4 The Connection with Λ-modules

In this section and the next, we will show how our error terms may be described in terms of the Iwasawa invariants of the $\mathbb{Z}_p^2$-extension of K.

Since $p.\mathcal{O}_K = \mathfrak{p}.\mathfrak{p}^*$ is split over K, we choose our embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ so that $\Phi_{E/K}\big(\mathfrak{p}^*\big)$ becomes the unit. The Tate module $T_p(E)$ of the curve breaks up into $\mathbb{T}_{\mathfrak{p}} \oplus \mathbb{T}_{\mathfrak{p}^*}$ over the CM-field K, with summands

$$\mathbb{T}_{\mathfrak{p}} \;=\; \varprojlim_n E[\mathfrak{p}^n] \quad \text{and} \quad \mathbb{T}_{\mathfrak{p}^*} \;=\; \varprojlim_n E[\mathfrak{p}^{*n}].$$

It is well-known that

$$\mathrm{Gal}\big(K\big(E[p^\infty]\big)/K\big) \;=\; \Delta_{(2)} \,\times\, \Gamma_{(2)},$$

where $\#\Delta_{(2)} = (p-1)^2$ and $\Gamma_{(2)} \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

One can pick a decomposition $\Gamma_{(2)} = \Gamma_+ \times \Gamma_-$ so that the action of complex conjugation on Γ_+ is trivial, and its action on Γ_- is through inversion instead. The Iwasawa algebra $\mathbb{Z}_p\big[\big[\Gamma_+ \times \Gamma_-\big]\big]$ is (non-canonically) isomorphic to $\mathbb{Z}_p[\![S,T]\!]$; here one distinguishes the variables S and T by a choice of topological generators $\gamma_+ \in \Gamma_+$ and $\gamma_- \in \Gamma_-$ respectively.

Finally, we will write $\mathcal{M}_\infty$ for the maximal abelian pro-p-extension of $K\big(E[p^\infty]\big)$ unramified outside the places lying over $\mathfrak{p}$, and we set

$$\mathfrak{X}_\infty \;:=\; \mathrm{Gal}\left(\mathcal{M}_\infty \big/ K(E[p^\infty])\right).$$

Proposition 6.4.1. *For all integers $n \geq 1$, we have*

$$\begin{aligned}\mu_{p,n}^{\mathrm{Per}}(E) \;&=\; p^{n-1}\left(pn - n - 1\right) \,+\, n \,-\, \mathrm{ord}_p\big(h^-(K_n)\big) \\ &\quad - \nabla_{K_n^+}^{\mathrm{Sym}^2 E} \;+\; \mathrm{ord}_p\left(\frac{\#H^0\big(\Gamma_+^{p^{n-1}},\, \mathcal{Z}_{\infty,+}\big)}{\#H^1\big(\Gamma_+^{p^{n-1}},\, \mathcal{Z}_{\infty,+}\big)}\right) \;+\; k(E,p)\end{aligned}$$

where $k = k(E,p)$ is a constant independent of n, and $\mathcal{Z}_{\infty,+}$ is the compact $\mathbb{Z}_p\big[\big[\Gamma_+\big]\big]$-module defined by

$$\mathcal{Z}_{\infty,+} \;:=\; \bigoplus_{j=0}^{p-2} H^1\Big(\Gamma_-,\, \mathfrak{X}_\infty \otimes_{\mathbb{Z}_p} \mathbb{T}_{\mathfrak{p}}^{\otimes -2}\Big)^{\Delta_{(2)} = \omega_K^j}.$$

The reader will notice the appearance of the $\big(\Gamma_+\big)^{p^{n-1}}$-Euler characteristic for the $\Phi_{E,\mathfrak{p}}^{\otimes -2}$-twisted coinvariants $\mathcal{Z}_{\infty,+}$. The long-term growth in this error function is controlled by its (μ,λ)-invariants (discussed in Section 6.5).

Henceforth, we write ϵ for the real quadratic character $\big(\big(\frac{-D}{\cdot}\big)\cdot\omega\big)^{(p-1)/2}$. We now claim that 6.4.1 is a direct consequence of the following two lemmas.

Lemma 6.4.2. *Up to an element of $\mathcal{O}_{\mathbb{C}_p}^\times$, the quantity $\xi(E/K_n^+)$ equals*

$$p^{k'+\nabla_{K_n^+}^{\mathrm{Sym}^2 E}} \times \frac{\big|\mathrm{Disc}(\mathbb{Q}(\mu_{p^n})^+)\big|_\infty}{\big|\mathrm{Disc}(K_n^+)\big|_\infty^2} \times \prod_{\substack{\psi:\mathrm{Gal}(K_n^+/\mathbb{Q})\to\mathbb{C}^\times \\ \psi\neq \mathbf{1},\,\psi\neq\epsilon}} \frac{\tau(\psi)L^{\mathrm{prim}}\big(\mathrm{Sym}^2 E\otimes\psi^{-1},1\big)}{\pi\,\langle f_E,f_E\rangle_{N_E}}$$

for some constant k' independent of n.

Lemma 6.4.3. *There exists another constant k'' independent of n, such that*

$$\prod_{\psi\neq\mathbf{1},\epsilon} \frac{\tau(\psi)L^{\mathrm{prim}}\big(\mathrm{Sym}^2 E\otimes\psi^{-1},1\big)}{\pi\times\langle f_E,f_E\rangle_{N_E}} \quad\approx\quad \frac{p^{k''}\,h^-(K_n)}{\#\mathbb{G}_m(K_n)_{\mathrm{tors}}} \times \mathbf{X}_{\Phi_E^{-2}}\Big(\Gamma_+^{p^{n-1}}\Big)^{-1}$$

where we write $\mathbf{X}_{\Phi_E^{-2}}\Big(\Gamma_+^{p^{n-1}}\Big)$ for the ratio $\frac{\#H^0\left(\Gamma_+^{p^{n-1}},\,\mathcal{Z}_{\infty,+}\right)}{\#H^1\left(\Gamma_+^{p^{n-1}},\,\mathcal{Z}_{\infty,+}\right)}$.

To see why these two lemmas imply our principal result, we observe

$$p^{\mu_{p,n}^{\mathrm{Per}}(E)} \overset{\text{by } 6.3.2}{=} \big(p\text{-adic unit}\big) \times \frac{\big|\mathrm{Disc}(\mathbb{Q}(\mu_{p^n})^+)\big|_\infty}{\big|\mathrm{Disc}(K_n^+)\big|_\infty} \times \xi(E/K_n^+)^{-1}\,.$$

Because K_n^+ has discriminant equal to $p^{p^{n-1}(pn-n-1)}\times\mathrm{Disc}(K)^{\phi(p^n)/2}$, and further $\#\mathbb{G}_m(K_n)_{\mathrm{tors}} = \text{unit}\times p^n$, Proposition 6.4.1 follows upon taking $k=-(k'+k'')$.

Proof of Lemma 6.4.2.

We begin with the trivial comment

$$\xi(E/K_n^+) \;=\; \frac{L^{\mathrm{imp}}\big(\mathrm{Sym}^2 E/K_n^+,2\big)}{L^{\mathrm{prim}}\big(\mathrm{Sym}^2 E/K_n^+,2\big)} \times \prod_{\psi} \frac{\tau(\psi^{-2})\;L^{\mathrm{prim}}(\mathrm{Sym}^2 E\otimes\psi,2)}{\pi^3\langle f_E,f_E\rangle_{N_E}}$$

where ψ ranges over all characters $\mathrm{Gal}(K_n^+/\mathbb{Q})\to\mathbb{C}^\times$; the first factor $L^{\mathrm{imp}}/L^{\mathrm{prim}}$ has p-adic order equal to $\nabla_{K_n^+}^{\mathrm{Sym}^2 E}$ by its definition. If we fix a character ψ of $\mathrm{Gal}(K_n^+/\mathbb{Q})$,

the functional equation for $L(\mathrm{Sym}^2 E \otimes \psi, s)$ implies

$$\frac{\tau(\psi^{-2})L^{\mathrm{prim}}(\mathrm{Sym}^2 E \otimes \psi, 2)}{\pi^3 \langle f_E, f_E \rangle_{N_E}} \;=\; \frac{\tau(\psi^{-2}).\tau(\psi)^2}{u_\psi \; \mathfrak{f}_\psi^3} \;\times\; \frac{\tau(\psi)L^{\mathrm{prim}}\big(\mathrm{Sym}^2 E \otimes \psi^{-1}, 1\big)}{\pi \; \langle f_E, f_E \rangle_{N_E}}$$

where the algebraic number $u_\psi = \frac{1}{2}\,\overline{\psi}\left(\mathfrak{f}_{\mathrm{Sym}^2 E}\right)\sqrt{\mathfrak{f}_{\mathrm{Sym}^2 E}}$ is a p-adic unit.

A straightforward exercise (c.f. the proof of 6.3.2) shows that

$$\prod_{\psi : \mathrm{Gal}(K_n^+/\mathbb{Q}) \to \mathbb{C}^\times} \frac{\tau(\psi^{-2}).\tau(\psi)^2}{u_\psi \; \mathfrak{f}_\psi^3} \quad \approx \quad \frac{\big|\mathrm{Disc}(\mathbb{Q}(\mu_{p^n})^+)\big|_\infty}{\big|\mathrm{Disc}(K_n^+)\big|_\infty^2}$$

so putting

$$k' = \sum_{\psi = \mathbf{1}, \epsilon} \mathrm{ord}_p \left(\frac{\tau(\psi)L^{\mathrm{prim}}(\mathrm{Sym}^2 E \otimes \psi^{-1}, 1)}{\pi \; \langle f_E, f_E \rangle_{N_E}} \right),$$

the result follows.

Proof of Lemma 6.4.3.

This statement is a lot deeper. The key point is that for $\psi \neq \mathbf{1}, \epsilon$ one has

$$\Phi_{E/K}\big(\mathfrak{p}^*\big)^{-2\mathfrak{f}_{\psi_p}} . \frac{\tau(\psi)L^{\mathrm{prim}}\big(\mathrm{Sym}^2 E \otimes \psi^{-1}, 1\big)}{\pi \; \langle f_E, f_E \rangle_{N_E}} \;=\; \int_{\mathrm{Gal}(K_\infty^+/\mathbb{Q})} \overline{\psi}(g) \; . \; \mathrm{d}\tau_{\mathrm{Sym}^2 E}(g)$$

where $\tau_{\mathrm{Sym}^2 E}$ denotes the p-adic measure attached to the symmetric square of E at $s = 1$ (see [CS87]). Moreover the formal identity

$$L^{\mathrm{prim}}\big(\mathrm{Sym}^2 E \otimes \psi^{-1}, s\big) \;=\; L\left(\psi^{-1}.\Big(\frac{-D}{}\Big), s-1\right) \; L\Big(\Phi_{E/K}^2.\big(\psi^{-1} \circ N_{K/\mathbb{Q}}\big), s\Big)$$

forces the distribution $\tau_{\mathrm{Sym}^2 E}$ to split into the convolution of a 1-dimensional and a 2-dimensional component.

Remark 6.4.4. It was shown by Coates and Schmidt in [CS87], Propositions 5.7 and 5.13 that

$$\begin{aligned} \int_{\mathrm{Gal}(K_\infty^+/\mathbb{Q})} \psi \; . \; \mathrm{d}\tau_{\mathrm{Sym}^2 E} \;&=\; I_\vartheta \;\times\; u_\vartheta\big(\,\mathrm{Res}(\psi)(\gamma_+) - 1\big) \;\times\; \Omega_{\mathfrak{p}}^{-2} \\ \times \;\; L\left(\psi.\Big(\frac{-D}{}\Big), 0\right) \;&\times\; \mathrm{char}_{\mathbb{Z}_p[[S]]}\Big(\big(\mathfrak{X}_{\infty,\vartheta} \otimes_{\mathbb{Z}_p} \mathbb{T}_{\mathfrak{p}}^{\otimes -2}\big)_{\Gamma_-}\Big)\Big|_{S = \mathrm{Res}(\psi)(\gamma_+) - 1} . \end{aligned}$$

Here $\vartheta = \Phi_{E,\mathfrak{p}}^2.\,\mathrm{Res}(\psi)\Big|_{\Delta^{(2)}}$, the power series $u_\vartheta(S)$ lies in $\mathbb{Z}_p[[S]]^\times$, and the algebraic number I_ϑ is given by

$$I_\vartheta \;=\; \frac{\left(\pi^{-1}\,\Omega\right)^2}{\langle f_E, f_E\rangle_{N_E}} \;\times\; \frac{\sqrt{\mathrm{Disc}(K)\,.\,\mathrm{Norm}_{K/\mathbb{Q}}\left(\mathfrak{f}_{\Phi^2_{E/K}}\right)}}{24\;W\left(\overline{\Phi}^2_{E/K}\right)}\;,$$

where Ω is the complex period attached to the lattice of E in $\mathbb{C}$, and $W(\overline{\Phi}^2_{E/K})$ is the root number which appears in the functional equation of $L(\overline{\Phi}^2_{E/K}, s)$.

One can check that I_ϑ is a unit whenever $p > 3$ does not divide the degree of the modular parametrisation. Also, the p-adic period $\Omega_\mathfrak{p}$ always belongs to $\mathcal{O}_{\mathbb{C}_p}^\times$ in the CM scenario.

In fact, Coates and Schmidt consider the Lie group $\mathrm{Gal}\left(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}\right)$ instead of $\mathrm{Gal}\left(K(\mu_{p^\infty})^+/\mathbb{Q}\right)$, but the details are otherwise identical. Their proof of this result relies on the two-variable main conjecture, which had not been proved at the time their article [CS87] was published; however, thanks to the fundamental work of Rubin [Rub99], this formula is now unconditional.

Consider the Iwasawa module

$$\mathfrak{X}''_\infty := H^0\left(\Delta_{(2)}\,,\left(\mathfrak{X}_\infty \oplus \left(\mathfrak{X}_\infty \otimes \omega_K^{(p-1)/2}\right)\right) \otimes_{\mathbb{Z}_p} \mathbb{T}_\mathfrak{p}^{\otimes -2}\right).$$

The proof of 6.4.3 reduces to showing the following two statements:

$$\textbf{Fact 1 :} \qquad \prod_{\psi \neq \mathbf{1},\epsilon} L\left(\psi.\left(\overline{-D}\right), 0\right) \;\approx\; \frac{h^-(K_n)}{\#\mathbb{G}_m(K_n)_{\mathrm{tors}}} \times \frac{1}{L\left(\left(\overline{-D}\right), 0\right).L\left(\epsilon.\left(\overline{-D}\right), 0\right)};$$

$$\textbf{Fact 2 :} \qquad \mathbf{X}_{\Phi_E^{-2}}\left(\Gamma_+^{p^{n-1}}\right) \times \prod_{\psi \neq \mathbf{1},\epsilon} \mathrm{char}_{\mathbb{Z}_p[\![S]\!]}\left(\left(\mathfrak{X}_{\infty,\vartheta} \otimes_{\mathbb{Z}_p} \mathbb{T}_\mathfrak{p}^{\otimes -2}\right)_{\Gamma_-}\right)\Big|_{S=\psi_K(\gamma_+)-1}$$

$$\approx \quad \#H^0\left(\Gamma_+, \left(\mathfrak{X}''_\infty\right)_{\Gamma_-}\right) \Big/ \#H^1\left(\Gamma_+, \left(\mathfrak{X}''_\infty\right)_{\Gamma_-}\right).$$

Granted we can prove these statements, Lemma 6.4.3 will hold for the constant

$$k'' \;=\; \mathrm{ord}_p\left(\frac{\#H^0\left(\Gamma_+, \left(\mathfrak{X}''_\infty\right)_{\Gamma_-}\right)}{\#H^1\left(\Gamma_+, \left(\mathfrak{X}''_\infty\right)_{\Gamma_-}\right)}\right) - \mathrm{ord}_p\left(L\left(\left(\overline{-D}\right), 0\right).L\left(\epsilon.\left(\overline{-D}\right), 0\right)\right).$$

To prove the first fact, we use the odd part of the analytic class number formula

$$\prod_{\psi:\mathrm{Gal}(K_n^+/\mathbb{Q})\to\mathbb{C}^\times} L\left(\psi.\left(\frac{-D}{\ }\right),1\right) \;=\; \frac{(2\pi)^{[K_n^+:\mathbb{Q}]}\; h^-(K_n)\;\sqrt{\left|\mathrm{Disc}(K_n^+)\right|_\infty}}{Q_{K_n/K_n^+}\;\#\mathbb{G}_m(K_n)_{\mathrm{tors}}\;\sqrt{\left|\mathrm{Disc}(K_n)\right|_\infty}}$$

then apply the $\psi.\left(\frac{-D}{\ }\right)$-twisted functional equation (e.g. see [Was96] Theorem 4.17). The index Q_{K_n/K_n^+} is either 1 or 2, hence it plays no role in the calculation.

Remark 6.4.5. To establish that Fact 2 is true, let's assume $\mathcal{W}$ denotes some compact finitely-generated $\mathbb{Z}_p\big[\!\big[\Gamma_+ \times \Delta_{(2)}\big]\!\big]$-torsion module. We shall write $\widetilde{\omega}$ to denote the mapping $\Delta_{(2)} \to \mathbb{F}_p^\times$ given by the composition

$$\Delta_{(2)} \;=\; \mathrm{Gal}\big(K\big(E[p]\big)/K\big) \;\twoheadrightarrow\; \mathrm{Gal}\big(K(\mu_p)/K\big) \;\xrightarrow{\sim}\; \mathbb{F}_p^\times.$$

Then

$$\begin{aligned}\prod_{\substack{\eta=\mathrm{Res}(\psi),\\ \psi:\mathrm{Gal}(K_n^+/\mathbb{Q})\to\mathbb{C}_p^\times}} \mathrm{char}_{\mathbb{Z}_p[\![S]\!]}\big(\mathcal{W}_{\vartheta'}\big)\Big|_{S=\eta(\gamma_+)-1} \;&=\; \prod_{j=0}^{p-2}\prod_{\eta'}\mathrm{char}_{\mathbb{Z}_p[\![S]\!]}\big(\mathcal{W}_{\widetilde{\omega}^j}\big)\Big|_{S=\eta'(\gamma_+)-1}\\ &\approx\; \prod_{j=0}^{p-2}\;\frac{\#H^1\Big(\Gamma_+^{p^{n-1}},\;\mathcal{W}_{\widetilde{\omega}^j}\Big)}{\#H^0\Big(\Gamma_+^{p^{n-1}},\;\mathcal{W}_{\widetilde{\omega}^j}\Big)}\end{aligned}$$

where η' ranges over all characters $\Gamma_+/\Gamma_+^{p^{n-1}} \to \mathbb{C}_p^\times$. This identity holds provided that each characteristic power series does not vanish at the points $\eta(\gamma_+) - 1$. In the first product, the η's are the restrictions to G_K of all even characters $\psi : G_\mathbb{Q} \twoheadrightarrow \mathrm{Gal}(K_n/\mathbb{Q}) \longrightarrow \mathbb{C}_p^\times$, and the finite character $\vartheta' = \eta\big|_{\Delta_{(2)}}$ again means 'the restriction of η' to the torsion-subgroup in $\mathrm{Gal}\big(K(E[p^\infty])/K\big)$.

If we now choose $\mathcal{W} = \big(\mathfrak{X}_\infty \otimes_{\mathbb{Z}_p} \mathbb{T}_\mathfrak{p}^{\otimes -2}\big)_{\Gamma_-}$ then it has been shown that

$$\mathrm{char}_{\mathbb{Z}_p[\![S]\!]}\big(\mathcal{W}_{\vartheta'}\big)\big(\psi_K(\gamma_+) - 1\big) \;\neq\; 0$$

for every ψ_K-twist, as the special values $L\big(\Phi^2_{E/K}.\psi_K^{-1}, 1\big)$ are all non-vanishing (see

[CS87] p.147 for an explanation). Consequently, the product becomes

$$\prod_{\psi:\mathrm{Gal}(K_n^+/\mathbb{Q})\to\mathbb{C}_p^\times} \mathrm{char}_{\mathbb{Z}_p[\![S]\!]}\Big(\big(\mathfrak{X}_{\infty,\vartheta}\otimes_{\mathbb{Z}_p}\mathbb{T}_{\mathfrak{p}}^{\otimes -2}\big)_{\Gamma_-}\Big)\Big|_{S=\mathrm{Res}(\psi)(\gamma_+)-1}$$

$$= \prod_{\eta=\mathrm{Res}(\psi)} \mathrm{char}_{\mathbb{Z}_p[\![S]\!]}\big(\mathcal{W}_{\vartheta'}\big)\Big|_{S=\eta(\gamma_+)-1} \overset{\text{by 6.4.5}}{\approx} \prod_{j=0}^{p-2} \frac{\#H^1\Big(\Gamma_+^{p^{n-1}},\ \mathcal{W}_{\widetilde{\omega}^j}\Big)}{\#H^0\Big(\Gamma_+^{p^{n-1}},\ \mathcal{W}_{\widetilde{\omega}^j}\Big)}$$

which is none other than the inverse of $\mathbf{X}_{\Phi_E^{-2}}\left(\Gamma_+^{p^{n-1}}\right)$.

Lastly, it is an easy exercise to verify that when we omit the exceptional characters $\psi = \mathbf{1}$ and $\psi = \epsilon$ from the product above, one must adjust by the same factor as in the statement of Fact 2.

6.5 Asymptotic Growth in the CM Periods

Recall that we are trying to derive a formula for the ratio of $\Omega_{K_n^+}^{\mathrm{mot}}(E)$ with $\Omega_{K_n^+}^{\mathrm{aut}}(E)$. Using Proposition 6.4.1, we know its p-adic order $\mu_{p,n}^{\mathrm{Per}}(E)$ is equal to

$$p^{n-1}\big(p\,n-n-1\big)\ +\ n\ -\ \mathrm{ord}_p\big(h^-(K_n)\big)\ -\ \nabla_{K_n^+}^{\mathrm{Sym}^2 E}\ +\ \mathrm{ord}_p\left(\mathbf{X}_{\Phi_E^{-2}}\left(\Gamma_+^{p^{n-1}}\right)\right)$$

up to some fixed constant $k = k(E,p)$.

Therefore to complete the proof of Theorem 6.1.6, we must show

Proposition 6.5.1. *If the μ_{ω^j} $(\mathcal{Z}_{\infty,+})$-invariants simultaneously vanish at every j, one has the growth estimate*

$$\mathbf{X}_{\Phi_E^{-2}}\left(\Gamma_+^{p^{n-1}}\right)\ =\ \big(\text{a constant}\big)\ \times\ \prod_{j=0}^{p-2} p^{-n\,\cdot\,\lambda_{\omega^j}(\mathcal{Z}_{\infty,+})}\quad \textit{for integers } n \gg 1.$$

Proof. Again we set $\mathcal{W} = \big(\mathfrak{X}_\infty\otimes_{\mathbb{Z}_p}\mathbb{T}_{\mathfrak{p}}^{\otimes -2}\big)_{\Gamma_-}$, so from the precise definition of $\mathcal{Z}_{\infty,+}$

$$\mathbf{X}_{\Phi_E^{-2}}\left(\Gamma_+^{p^{n-1}}\right) = \frac{\#H^0\left(\Gamma_+^{p^{n-1}},\ \bigoplus_{j=0}^{p-2}\mathcal{W}_{\widetilde{\omega}^j}\right)}{\#H^1\left(\Gamma_+^{p^{n-1}},\ \bigoplus_{j=0}^{p-2}\mathcal{W}_{\widetilde{\omega}^j}\right)}\ =\ \prod_{j=0}^{p-2}\frac{\#H^0\left(\Gamma_+^{p^{n-1}},\mathcal{W}_{\widetilde{\omega}^j}\right)}{\#H^1\left(\Gamma_+^{p^{n-1}},\mathcal{W}_{\widetilde{\omega}^j}\right)}\,.$$

Focussing first on the H^1-term, for a given value $j \in \{0, \ldots, p-2\}$

$$\#H^1\left(\Gamma_+^{p^{n-1}}, \mathcal{W}_{\widetilde{\omega}^j}\right) \;=\; \#\Big(\mathcal{W}_{\widetilde{\omega}^j}\Big)_{\Gamma_+^{p^{n-1}}} \;=\; p^{\lambda_{\omega^j}\cdot n \,+\, p^n\cdot\mu_{\omega^j} \,+\, k_j'''} \;\text{ with } n \gg 1,$$

where the non-negative integer k_j''' is independent of n.

The proof relies on two important facts:

(i) The μ-invariants of the $\mathbb{Z}_p[\![\Gamma_+]\!]$-modules $\mathcal{W}_{\widetilde{\omega}^j}$ are assumed trivial;

(ii) All finite $\mathbb{Z}_p[\![\Gamma_+]\!]$-submodules of $\mathcal{W}_{\widetilde{\omega}^j}$ have universally bounded size.

The first statement clearly implies vanishing of the total μ_E^{cy}-invariant of $\mathcal{W}$. To see the reason why **(i)** implies **(ii)**, there is an exact sequence of finitely-generated compact $\mathbb{Z}_p[\![\Gamma_+]\!]$-modules

$$0 \longrightarrow \text{ finite } \longrightarrow \mathcal{W}_{\widetilde{\omega}^j} \xrightarrow{\mathcal{A}_j} \bigoplus_{m=1}^{t_j} \frac{\mathbb{Z}_p[[\Gamma_+]]}{F_{j,m}^{e_{j,m}}} \longrightarrow \text{ finite } \longrightarrow 0$$

where each element $F_{j,m}$ maps to an irreducible distinguished polynomial via the isomorphism $\mathbb{Z}_p[\![\Gamma_+]\!] \xrightarrow{\sim} \mathbb{Z}_p[\![S]\!]$. As a corollary, the size of any pseudo-null $\mathbb{Z}_p[\![\Gamma_+]\!]$-submodule inside $\mathcal{W}_{\widetilde{\omega}^j}$ must be bounded above *independently* by $\#\ker(\mathcal{A}_j)$, as the summands $\mathbb{Z}_p[\![\Gamma_+]\!]/(F_{j,m})^{e_{j,m}}$ are easily seen to be free of any p^∞-torsion (which establishes the second fact).

A nice consequence of **(ii)** is the boundedness of $H^0\big(\Gamma_+^{p^{n-1}}, \mathcal{W}_{\widetilde{\omega}^j}\big)$ for $n \geq 1$, since this module is contained within its $\mathrm{Gal}\big(K_n^+/K_1^+\big)$-orbit (which is then a finite $\mathbb{Z}_p[\![\Gamma_+]\!]$-submodule of $\mathcal{W}_{\widetilde{\omega}^j}$). It follows that

$$\#H^0\big(\Gamma_+^{p^{n-1}}, \mathcal{W}_{\widetilde{\omega}^j}\big) \;=\; p^{k_j''''}$$

for a fixed constant k_j'''' (when n is sufficiently large), so we have

$$\mathbf{X}_{\Phi_E^{-2}}\Big(\Gamma_+^{p^{n-1}}\Big) \;=\; \Big(p^{\sum_j k_j''' - k_j'''}\Big) \;\times\; \prod_{j=0}^{p-2} p^{-n\,\cdot\,\lambda_{\omega^j}(\mathcal{Z}_{\infty,+})}$$

as predicted by 6.5.1. The proof of the proposition is complete. □

Question: *Does the vanishing of the total μ_E^{cy}-invariant occur frequently?*

In answer to this, Greenberg provided us with the following reasoning: if we take a two-variable power series (with trivial μ-invariant) and consider all of its one-variable specialisations, then the subset of specialisations with positive μ-invariant should have density zero. Therefore, intuitively we would expect the answer to be 'Yes'.

Gillard [Gil85] Theorem 6.4.4 has shown vanishing of the cyclotomic μ-invariant inside a two-variable deformation, but without extra twisting by the Grossencharacter Φ_E^{-2}. Similarly, some recent work of Hida confirms vanishing of the μ-invariant for many *anti-cyclotomic* branches of the Katz p-adic L-function (which, unfortunately, is no use here).

Tabulated below are a few numerical calculations of the μ_E^{cy}-invariant for our three example elliptic curves: $27A(1)$, $32A(1)$ and $49A(1)$. Briefly, an upper bound on $\mu_{\omega^j}(\mathcal{Z}_{\infty,+})$ is given by the p-adic order at any special value, of the $\widetilde{\omega}^j$-branch for the $\Phi_{E,\mathfrak{p}}^2$-twisted Katz-Yager L-function (which hopefully might often be zero).

Table 6.4: Numerical bounds on μ_E^{cy} for our three elliptic curves.

$E = 27A(1)$		$E = 32A(1)$		$E = 49A(1)$	
p	μ_E^{cy}	p	μ_E^{cy}	p	μ_E^{cy}
7	≤ 2	5	0	11	≤ 2
13	0	13	0	23	0
19	0	17	0	29	0
31	0	29	0	37	0
37	0	37	0	43	≤ 4
43	0	41	0	53	≤ 2
61	≤ 2	53	0	67	≤ 2
67	0	61	≤ 2	71	≤ 2
73	≤ 2	73	0	79	0
79	≤ 2	89	≤ 2	107	0
97	0	97	0	109	0
103	0	101	0	113	≤ 2
109	≤ 2	109	0	127	0
127	0	113	0	137	≤ 2
139	0	137	≤ 2	149	0
151	≤ 4	149	0	151	≤ 2
157	0	157	≤ 2	163	≤ 4
163	0	173	0		
181	≤ 2	181	0		
193	0	193	≤ 2		
199	≤ 2				

6.6 Computational Difficulties at the Second Layer

Let us now outline the problems which arise when we look for congruences at the higher layer $n = 2$. Shifting notation slightly, let F_n denote the extension $\mathbb{Q}(\mu_{p^n})$. Kato's predicted congruence [Kat05] §3.10 over the field $\mathbb{Q}\left(\mu_{p^2}, \sqrt[p^2]{\Delta}\right)$ is precisely

$$N_{1,2}\left(\frac{a_1}{N_{0,1}(a_0)}\right)^p \times \left(\frac{a_2 \ \times \ \varphi \circ N_{0,1}(a_0)}{N_{0,2}(a_0) \ \times \ \varphi(a_1)}\right)^{p^2} \overset{??}{\equiv} \ 1 \mod p^4.\mathbb{Z}_p[\![U^{(2)}]\!]$$

where the a_j's denote the motivic p-adic L-functions $\mathcal{L}(E, \rho_j)$ for $j = 0, 1, 2$.

Evaluating the above at the trivial character $\psi = \mathbf{1}$ then exploiting the basic identity $\mathbf{1} \circ \varphi \ = \ \mathbf{1}^p \ = \ \mathbf{1}$, his prediction simplifies to become

$$\left(\frac{\mathcal{X}_E\big(\operatorname{Res}_{F_2}(\rho_1)\big)}{\mathcal{X}_E\big(\operatorname{Res}_{F_2}(\rho_0)\big)^{1+p}} \times \left(\mathcal{X}_E(\rho_2) \times \frac{\mathcal{X}_E\big(\operatorname{Res}_{F_1}(\rho_0)\big)}{\mathcal{X}_E(\rho_1)}\right)^p\right)^p \overset{??}{\equiv} \ 1 \mod p^4 \, .$$

Motivated by numerical work in [DD07], we pick a non-CM elliptic curve

$$E = X_0(11) \ : \ y^2 + y \ = \ x^3 - x^2 - 10x - 20,$$

making a choice of good ordinary prime $p = 3$ and auxiliary integer $\Delta = 2$. Using MAGMA, we were able to calculate the values

$$\begin{aligned}
\mathcal{X}_E(\operatorname{Res}_{F_2}(\rho_1)) &= 1.3^0 + 2.3^1 + 2.3^2 + 1.3^3 + 2.3^4 + O(3^5) \\
\mathcal{X}_E(\operatorname{Res}_{F_2}(\rho_0)) &= 1.3^0 + 2.3^1 + 1.3^2 \qquad\qquad + O(3^5) \\
\mathcal{X}_E(\operatorname{Res}_{F_1}(\rho_0)) &= 1.3^0 \qquad + 2.3^2 + 2.3^3 + 1.3^4 + O(3^5) \\
\mathcal{X}_E(\rho_1) &= 1.3^0 \qquad + 1.3^2 + 1.3^3 + 1.3^4 + O(3^5);
\end{aligned}$$

however the computer failed to work out $\mathcal{X}_E\big(\rho_2\big)$ due to lack of available memory. This is surprising given that $X_0(11)$ has least conductor amongst elliptic curves, and likewise $(p, \Delta) = (3, 2)$ is the smallest choice available. Nevertheless, granted the K_1-congruence holds over $\mathbb{Q}\big(\mu_9, \sqrt[9]{2}\big)$, then one can make an educated guess at the value of $\mathcal{X}_E\big(\rho_2\big)^9$ modulo 81 from the tabulated L-values.

Conjecture 6.6.1. *For the elliptic curve $E = X_0(11)$, the prime $p = 3$ and $\Delta = 2$,*

$$\mathcal{X}_E\big(\rho_2\big)^{3^2} \overset{??}{\equiv} \ 28 \mod 3^4 \, .$$

This is equivalent to Kato's second layer K_1-congruence (at the trivial character), and it's easily confirmed that 28 is a 9th power modulo 3^4, e.g. $4^9 \equiv 28 \mod 3^4$. We hope to pursue the second layer K_1-congruences in future research.

Appendix A

Computing Symmetric Square Euler Factors

In this appendix we describe an algorithm to compute the error $\nabla_{K_n^+}^{\mathrm{Sym}^2 E}$ in the CM case, which by definition is the p-adic order of the factor

$$\prod_{q|N_E} P_q\big(\mathrm{Sym}^2 E/K_n^+, q^{-2}\big).$$

Lemma A.0.2. *Let V be an l-adic representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and let $M/\mathbb{Q}$ be a finite Galois extension. Write $R_{M/\mathbb{Q}}$ for the regular representation of $\mathrm{Gal}(M/\mathbb{Q})$, and $V/M = V \otimes R_{M/\mathbb{Q}}$ for the base-change of V to M. Let q be a prime different from l, and Frob_q a lift of the Frobenius element at q. We write the local polynomial of q on V as*

$$\begin{aligned} P_q(V,T) &:= \det\Big(1 - T.\mathrm{Frob}_q \Big| V^{I_q}\Big) \\ &= \prod_i (1 - \lambda_i T) \end{aligned}$$

Then, if q is unramified in $M/\mathbb{Q}$, we have

$$P_q(V \otimes R_{M/\mathbb{Q}}, T) \;=\; \prod_i \big(1 - (\lambda_i T)^f\big)^r$$

where f is the residue class degree of q in $M/\mathbb{Q}$, and r is the number of primes of M over q.

Proof. Since q is unramified in $M/\mathbb{Q}$, it is certainly true that

$$(V \otimes R_{M/\mathbb{Q}})^{I_q} \;=\; V^{I_q} \otimes R_{M/\mathbb{Q}}^{I_q},$$

so the characteristic polynomial of Frob_q on $(V/M)^{I_q}$ is given by

$$P_q(V \otimes R_{M/\mathbb{Q}}, T) \;=\; \prod_{i,j}(1 - \lambda_i \mu_j T)$$

where $P_q(R_{M/\mathbb{Q}}, T) = \prod_j (1 - \mu_j T)$. Then we observe that

$$\begin{aligned} P_q(R_{M/\mathbb{Q}}, T) &= \prod_{\text{places } v|q \text{ of } M} \left(1 - T^{f(v/q)}\right) \\ &= \left(1 - T^f\right)^r \end{aligned}$$

since $M/\mathbb{Q}$ is a Galois extension. The result follows. □

We cannot apply Lemma A.0.2 directly to the case $V = \mathrm{Sym}^2 H_l^1(E)$ and $M = K_n^+$, since the primes dividing N_E ramify in $K_n^+/\mathbb{Q}$. However, the ramification occurs only in the imaginary quadratic extension $K/\mathbb{Q}$, so we can apply Lemma A.0.2 to the representations $\mathrm{Sym}^2 H_l^1(E)$ and $\mathrm{Sym}^2 H_l^1(E) \otimes \epsilon$ separately, where ϵ is the non-trivial character of $K/\mathbb{Q}$.

Since E is assumed to have complex multiplication here, if q is a prime dividing N_E then E has additive reduction at q. Consulting [CS87] §1, we find that in this case there are 3 possiblities for the Euler factor of $L(\mathrm{Sym}^2 E, s)$ at q:

$$P_q(\mathrm{Sym}^2 E, T) \;=\; 1 - \lambda\, q\, T$$

for $\lambda = 0, 1$ or -1 (this λ may be calculated exactly following Watkins [Wat02]).

Proposition A.0.3. *Fix a prime q with $q \big| N_E$, and as above write*

$$P_q(\mathrm{Sym}^2 E, T) \;=\; 1 - \lambda\, q\, T$$

for $\lambda \in \{0, 1, -1\}$ *. Let* m *be the multiplicative order of* q *modulo* p^n*, and write* $d = \phi(p^n)$*. Then*

$$P_q(\mathrm{Sym}^2 E/K_n^+, T) \;=\; \begin{cases} \left(1-(\lambda q T)^m\right)^{d/m}\left(1-(qT)^m\right)^{d/2m} & \text{if } m \text{ is odd} \\ \left(1-(\lambda q T)^m\right)^{d/m}\left(1+(qT)^{m/2}\right)^{d/m} & \text{if } m \text{ is even.} \end{cases}$$

Proof. Let us write $G = \mathrm{Gal}(K_n^+/\mathbb{Q})$ and $H = \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$. We consider the character group of G:

$$\begin{aligned} \widehat{G} &= \{\psi \in \widehat{\mathrm{Gal}}(K_n/\mathbb{Q}) \,:\, \psi \text{ even }\} \\ &= \{\chi \,:\, \chi \in \widehat{H},\ \chi \text{ even }\} \,\cup\, \{\chi'\epsilon \,:\, \chi' \in \widehat{H},\ \chi' \text{ odd }\} \end{aligned}$$

where ϵ is the non-trivial character of $\mathrm{Gal}(K/\mathbb{Q})$, considered as a character of $\mathrm{Gal}(K_n/\mathbb{Q})$. Therefore

$$\begin{aligned} P_q(\mathrm{Sym}^2 E/K_n^+, T) &= \prod_{\psi \in \widehat{G}} P_q(\mathrm{Sym}^2 E, \psi, T) \\ &= \prod_{\chi \in \widehat{H},\ \chi \text{ even}} P_q(\mathrm{Sym}^2 E, \chi, T) \\ &\times \prod_{\chi' \in \widehat{H},\ \chi' \text{ odd}} P_q(\mathrm{Sym}^2 E, \chi'\epsilon, T)\,. \end{aligned}$$

We observe that

$$\prod_{\chi \in \widehat{H},\ \chi \text{ even}} P_q(\mathrm{Sym}^2 E, \chi, T) \;=\; P_q(\mathrm{Sym}^2 E/\mathbb{Q}(\mu_{p^n})^+, T)$$

and also

$$\begin{aligned} \prod_{\chi' \in \widehat{H},\ \chi' \text{ odd}} P_q(\mathrm{Sym}^2 E, \chi'\epsilon, T) &= \prod_{\eta \in \widehat{H}} P_q(\mathrm{Sym}^2 E, \eta\epsilon, T) \\ &\times \prod_{\chi \in \widehat{H},\ \chi \text{ even}} P_q(\mathrm{Sym}^2 E, \chi\epsilon, T)^{-1} \\ &= \frac{P_q(\mathrm{Sym}^2 E \otimes \epsilon/\mathbb{Q}(\mu_{p^n}), T)}{P_q(\mathrm{Sym}^2 E \otimes \epsilon/\mathbb{Q}(\mu_{p^n})^+, T)}. \end{aligned}$$

The characteristic polynomials in these formulae are all of the form considered in Theorem A.0.3. So, we can calculate them exactly using the following information:

firstly

$$P_q(\mathrm{Sym}^2 E, T) \;=\; 1 - \lambda\, q\, T,$$

and one can check that

$$P_q(\mathrm{Sym}^2 E \otimes \epsilon, T) \;=\; (1 - \lambda q T)(1 - qT).$$

by using the formula for $L(\mathrm{Sym}^2 E, \chi, s)$ in terms of the Grossencharacter of E.

Further, the residue class degree of q in the extension $\mathbb{Q}(\mu_{p^n})/\mathbb{Q}$ is the order of q in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, which we labelled m here. It is also easy to check that

$$\text{residue class degree of } q \text{ in } \mathbb{Q}(\mu_{p^n})^+/\mathbb{Q} \;=\; \begin{cases} m & \text{if } m \text{ is odd} \\ m/2 & \text{if } m \text{ is even.} \end{cases}$$

Putting all this information into Lemma A.0.2 and applying it to the above formulae, we obtain an explicit expression for $P_q(\mathrm{Sym}^2 E/K_n^+, T)$, and after simplifying it slightly we arrive at the desired result. □

Corollary A.0.4. *With λ and m as in Proposition A.0.3, we have*

$$P_q\big(\mathrm{Sym}^2 E/K_n^+, q^{-s}\big)\Big|_{s=2} = \begin{cases} \big(1 - \lambda\, q^{-m}\big)^{d/m}\, \big(1 - q^{-m}\big)^{d/2m} & \textit{if } m \textit{ is odd} \\ \big(1 - |\lambda|\, q^{-m}\big)^{d/m} \big(1 + q^{-m/2}\big)^{d/m} & \textit{if } m \textit{ is even.} \end{cases}$$

Proof. This follows immediately from Proposition A.0.3 upon observing that $\lambda^m = \lambda$ when m is odd, and $\lambda^m = |\lambda|$ when m is even (for any $\lambda \in \{0, 1, -1\}$). □

Using Corollary A.0.4 we can easily compute the p-adic order of

$$\prod_{q | N_E} P_q\left(\mathrm{Sym}^2 H_l^1(E)/K_n^+, q^{-s}\right)\Big|_{s=2}$$

which by definition is the quantity $\nabla_{K_n^+}^{\mathrm{Sym}^2 E}$.

Appendix B

Computing L-values with MAGMA

Recall from Chapter 6 that we want to compute the p-adic order of the number

$$\xi(E/F) \;:=\; \prod_{\chi\in\widehat{\mathrm{Gal}}(F/\mathbb{Q})} \frac{\tau(\chi^{-2})\; L(\mathrm{Sym}^2 E,\chi,2)}{\pi\;\Omega_E^+\,\Omega_E^-}.$$

for a totally real field F. To compute the twisted symmetric square L-values $L(\mathrm{Sym}^2 E,\chi,2)$, we used the computer algebra package MAGMA [BCP97]. This package has inbuilt functions for dealing with motivic L-series, based on Tim Dokchitser's PARI program *ComputeL*, which uses the algorithm from his article [Dok04].

B.1 The *ComputeL* Package

Tim Dokchitser's program can compute the values of an L-series

$$L(s) \;=\; \sum_{n=1}^{\infty} a_n\, n^{-s},$$

under two standard assumptions. Firstly, we assume $L(s)$ may be continued to a meromorphic function on the whole complex plane. Secondly, we assume there

exists a weight $\kappa \geq 0$, a sign $w \in \mathbb{C}$ with absolute value 1, a conductor $N \in \mathbb{Z}$, and a Gamma factor

$$\gamma(s) \;=\; \Gamma\left(\frac{s+\lambda_1}{2}\right) \ldots \Gamma\left(\frac{s+\lambda_d}{2}\right)$$

such that the completed L-series

$$L^*(s) \;=\; \left(\frac{N}{\pi^d}\right)^{s/2} \gamma(s)\, L(s)$$

satisfies the functional equation

$$L^*(s) \;=\; w\, \hat{L}^*(\kappa - s).$$

Here we write $\hat{L}(s)$ for the dual L-series which has complex conjugate coefficients:

$$L(s) \;=\; \sum_{n=1}^{\infty} \overline{a}_n\, n^{-s}.$$

To use the *ComputeL* routine, we must input $\kappa, w, N, \gamma(s)$, and sufficiently many Dirichlet series coefficients a_n. The number of coefficients required depends on the conductor of the L-series and the precision of the output. If the conductor becomes large, it may be computationally difficult to generate enough coefficients to get a useful precision; this is the problem we encountered at the second layer of the false Tate curve tower, as mentioned in Section 6.6.

B.2 Symmetric Square L-series

The primitive symmetric square L-series $L(\mathrm{Sym}^2 E, s)$ is the motivic L-function attached to the l-adic representations $\left\{\mathrm{Sym}^2 H_l^1(E)\right\}$. It may be defined by the Euler product

$$L(\mathrm{Sym}^2 E, s) \;:=\; \prod_{\text{all primes } q} P_q(\mathrm{Sym}^2 E, q^{-s})^{-1}.$$

If the prime q does not divide N_E, the Euler factor at q is given by

$$P_q(\mathrm{Sym}^2 E, T) \;:=\; (1 - \alpha_q^2\, T)\; (1 - \alpha_q\, \alpha_q'\, T)\; (1 - \alpha_q'^2\, T)$$

where as usual we have written

$$1 - a_q(E)\,T + q\,T^2 \;=\; (1 - \alpha_q\,T)(1 - \alpha'_q\,T).$$

The following lemma from [CS87] tells us the possible Euler factors at the bad primes.

Lemma B.2.1. *If E has multiplicative reduction at the prime q, then the Euler factor of* $\mathrm{Sym}^2 E$ *at q is*

$$P_q(\mathrm{Sym}^2 E, T) \;=\; (1 - \alpha_q^2\,T)(1 - \alpha_q\,\alpha'_q\,T)(1 - \alpha_q'^2\,T).$$

This is also the case when there exists a quadratic twist of E having good reduction at q. If E has additive reduction at q (and there is no such quadratic twist) then

$$P_q(\mathrm{Sym}^2 E, T) \;=\; 1 \quad \textit{or} \quad 1 \pm qT.$$

For a given elliptic curve E, the results of Watkins [Wat02] can be used to calculate exactly the Euler factor of $\mathrm{Sym}^2 E$ at the primes of additive reduction (these are the primes q such that q^2 divides N_E).

We will now state the functional equation of the twisted L-function $L(\mathrm{Sym}^2 E, \chi, s)$, allowing us to compute its values using MAGMA. We write f_χ for the conductor of the Dirichlet character χ, and $N_{\mathrm{Sym}^2 E}$ for the conductor of the representation $\mathrm{Sym}^2 H^1_l(E)$. We also write

$$\tau(\chi) \;=\; \sum_{a=1}^{f_\chi} \psi(a)\exp(2\pi i a/f_\chi),$$

for the standard Gauss sum of χ, and put $i_\chi = 0$ or 1 so that $\chi(-1) = (-1)^{i_\chi}$. We quote the following result from [CS87], although we have rewritten it in the notation of Section B.1. Coates and Schmidt proved it under the assumption that E is modular; thanks to the work of Wiles et al, we now know it applies to any elliptic curve over $\mathbb{Q}$.

Theorem B.2.2. *Suppose that χ is a Dirichlet character such that $(N_E, f_\chi) = 1$. Define the conductor*

$$N \;=\; N_{\mathrm{Sym}^2 E}\, f_\chi^3,$$

the Gamma factor

$$\gamma(s) \;=\; \Gamma\left(\frac{s}{2}\right)\;\Gamma\left(\frac{s+1}{2}\right)\;\Gamma\left(\frac{s-i_\chi}{2}\right),$$

and the sign

$$w \;=\; \chi(N_{\mathrm{Sym}^2 E})\;\sqrt{\chi(-1)f_\chi}\;\frac{\tau(\chi)}{\tau(\overline{\chi})^2}.$$

Then, for the completed L-function

$$L^*(\mathrm{Sym}^2 E,\chi,s) \;:=\; \left(\frac{N}{\pi^3}\right)^{s/2}\gamma(s)\;L(\mathrm{Sym}^2 E,\chi,s),$$

we have the functional equation

$$L^*(\mathrm{Sym}^2 E,\chi,s) \;=\; w\;L^*(\mathrm{Sym}^2 E,\overline{\chi},3-s).$$

Let F be a finite abelian extension of $\mathbb{Q}$, such that $\mathrm{Disc}(F)$ is coprime to N_E. With the data from Theorem B.2.2, we can use MAGMA to compute the complex numbers

$$\xi(E,\chi) \;=\; \frac{\tau(\chi^{-2})\;L(\mathrm{Sym}^2 E,\chi,2)}{\pi\;\Omega_E^+\,\Omega_E^-}$$

for each character χ of $\mathrm{Gal}(F/\mathbb{Q})$. Each $\xi(E,\chi)$ lies in the field $\mathbb{Q}(\chi)$, but it may be difficult to identify them numerically as algebraic numbers. However, it is proved in [CS87] that

$$\xi(E,\chi)^\sigma = \xi(E,\chi^\sigma)$$

for all $\sigma \in \mathrm{Aut}(\mathbb{C})$, therefore the product

$$\xi(E/\mathbb{Q}(\mu_{p^n})^+) \;:=\; \prod_{\chi\in\widehat{\mathrm{Gal}}(F/\mathbb{Q})}\xi(E,\chi).$$

actually lies in $\mathbb{Q}$. It is much easier to identify this rational number, as long the values can be computed to sufficiently high precision.

B.3 The CM Case

Let E now be an elliptic curve over $\mathbb{Q}$ with complex multiplication by an order in $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{-d})$.

In Chapter 6, we wanted to compute the quantity $\xi(E/K_n^+)$, where K_n^+ is the maximal real subfield of $\mathbb{Q}(\sqrt{-d}, \mu_{p^n})$. In this case, we have characters $\chi : \mathrm{Gal}(K_n^+/\mathbb{Q}) \to \mathbb{C}^\times$ such that $(f_\chi, N_E) \neq 1$, so we cannot apply Theorem B.2.2 directly to $L(\mathrm{Sym}^2 E, \chi, s)$. To overcome this problem, we can exploit the fact that the L-function $L(\mathrm{Sym}^2 E, s)$ splits into a product of Hecke L-functions.

We quote the following result from [CS87]; we have already used it heavily in Chapter 6.

Theorem B.3.1. *Suppose E has complex multiplication by the ring of integers of an imaginary quadratic field K. Let $\Phi_{E/K}$ be the Grossencharakter associated to E/K, and $\Phi_{E/K}^2$ the primitive character attached to its square. Then*

$$L(\mathrm{Sym}^2 E, s) \;=\; L(\Phi_{E/K}^2, s)\, L(\epsilon, s-1),$$

where ϵ is the non-trivial character of the quadratic extension $K/\mathbb{Q}$. More generally, if χ is a Dirichlet character,

$$L(\mathrm{Sym}^2 E, \chi, s) \;=\; L(\Phi_{E/K}^2 \chi_K, s)\, L(\epsilon\chi, s-1)$$

where $\chi_K = \chi \circ N_{K/\mathbb{Q}}$.

Theorem B.3.1 is only stated in [CS87] in the case when $(N_E, f_\chi) \neq 1$, but in fact it holds for arbitrary χ as long as the L-functions in the equation are the primitive ones. For example, we can put $\chi = \epsilon$ into the theorem to get

$$L(\mathrm{Sym}^2 E, \epsilon, s) \;=\; L(\Phi_{E/K}^2 \epsilon_K, s)\, L(\epsilon^2, s-1).$$

One checks that ϵ^2 is not primitive, and the associated primitive character is trivial. Similarly, ϵ_K is a non-primitive Hecke character over K with trivial underlying character, and the above equation becomes

$$L(\mathrm{Sym}^2 E, \epsilon, s) \;=\; L(\Phi_{E/K}^2, s)\, \zeta(s-1).$$

As in Appendix A, let us write $G = \mathrm{Gal}(K_n^+/\mathbb{Q})$ and $H = \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$. Considering the characters of G, we have:

$$\begin{aligned}\widehat{G} &= \{\psi \in \widehat{\mathrm{Gal}}(K_n/\mathbb{Q}) \,:\, \psi \text{ even }\} \\ &= \{\chi \,:\, \chi \in \widehat{H},\ \chi \text{ even }\} \,\cup\, \{\eta\epsilon \,:\, \eta \in \widehat{H},\ \eta \text{ odd }\}.\end{aligned}$$

Suppose η is an odd character of H, so that $\eta\epsilon \in \widehat{G}$. By the comment above, we have

$$\begin{aligned}L(\mathrm{Sym}^2 E, \eta\epsilon, s) &= L(\Phi^2_{E/K}\ \eta_K\ \epsilon_K, s)\ \ L(\epsilon^2\ \eta, s-1) \\ &= L(\Phi^2_{E/K}\ \eta_K, s)\ \ L(\eta, s-1),\end{aligned}$$

assuming all the L-series are primitive. Therefore, we may write

$$\begin{aligned}\xi(E/K_n^+) &= \prod_{\chi \in \widehat{H}, \text{even}} \frac{\tau(\chi^{-2})\ L(\Phi^2_{E/K}\ \chi_K, 2)\ L(\chi\,\epsilon, 1)}{\pi\ \Omega_E^+\,\Omega_E^-} \\ &\times \prod_{\eta \in \widehat{H}, \text{odd}} \frac{\tau(\eta^{-2})\ L(\Phi^2_{E/K}\ \eta_K, 2)\ L(\eta, 1)}{\pi\ \Omega_E^+\,\Omega_E^-}.\end{aligned}$$

The Hecke L-values $L(\Phi^2_{E/K}\ \chi_K, 2)$ for characters χ of $H = \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$ may be easily computed; the functional equation of a Hecke L-function is well known (see [Tat79] for example), and we will not reproduce it here. The Dirichlet L-values $L(\chi, 1)$ are also simple to compute, and thus we have all the data needed to calculate $\xi(E/K_n^+)$ with MAGMA.

Bibliography

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the Modularity of Elliptic Curves over $\mathbb{Q}$. *J. A. M. S.*, 14:843–939, 2001.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The MAGMA algebra system I: the user language. *J. Symb. Comput.*, 24(3-4):235–265, 1997.

[BD07] A. Bouganis and V. Dokchitser. Algebraicity of L-values for Elliptic Curves in a False Tate Curve Tower. *Math. Proc. Camb. Phil. Soc.*, 142:193–204, 2007.

[Bou05] A. Bouganis. *L-functions of Elliptic Curves and False Tate Curve Extensions*. PhD thesis, University of Cambridge, 2005.

[Bur07] D. Burns. On Main Conjectures in Non-Commutative Iwasawa Theory and Related Conjectures. 2007.

[CF67] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic Number Theory*. Academic Press, 1967.

[CFK+05] J. Coates, T. Fukaya, K. Kato, R. Sujatha, and O. Venjakob. The GL_2 Main Conjecture for Elliptic Curves without Complex Multiplication. *Publ. Math. IHES.*, 101:163–208, 2005.

[CPR89] J. Coates and B. Perrin-Riou. On p-adic L-functions Attached to Motives Over $\mathbb{Q}$. *Adv. Stud. Pure Math.*, 17:23–54, 1989.

[CS87] J. Coates and C.-G. Schmidt. Iwasawa Theory for the Symmetric Square of an Elliptic Curve. *J. Reine Angew. Math.*, 375/376:104–156, 1987.

[DD07] T. Dokchitser and V. Dokchitser. Computations in Non-Commutative Iwasawa Theory. *Proc. London Math. Soc.*, (3) 94:211–272, 2007.

[DHI98] K. Doi, H. Hida, and H. Ishii. Discriminant of Hecke Fields and Twisted Adjoint L-values for GL_2. *Invent. Math.*, 134:547–577, 1998.

[Dok04] T. Dokchitser. Computing Special Values of Motivic L-functions. *Experiment. Math.*, 13(2):137–150, 2004.

[Dok05] V. Dokchitser. Root Numbers of Non-Abelian Twists of Elliptic Curves. *Proc. London Math. Soc.*, 91(2):300–324, 2005.

[DW08] D. Delbourgo and T. Ward. Non-Abelian Congruences Between L-values of Elliptic Curves. *Ann. Inst. Fourier*, 58(3):1023–1055, 2008.

[Gil85] R. Gillard. Fonctions L p-adiques des Corps Quadratiques Imaginaires et de Leurs Extensions Abéliennes. *Journal Reine Angew. Math.*, 358:76–91, 1985.

[Har87] Shai Haran. p-adic L-functions for modular forms. *Compos. Math.*, 62:31–46, 1987.

[Hid91] H. Hida. On p-adic L-functions of $\mathrm{GL}(2) \times \mathrm{GL}(2)$ Over Totally Real Fields. *Ann. Inst. Fourier*, 41:311–391, 1991.

[HT89] H. Hida and J. Tilouine. Katz p-adic L-functions, Congruence Modules and Deformation of Galois Representations. *Proceedings of Durham Symposium on Arithmetic of L-functions*, 1989.

[HT93] H. Hida and J. Tilouine. Anti-cyclotomic Katz p-adic L-functions and Congruence Modules. *Ann. Sci. École Norm. Sup.*, 26(4):189–259, 1993.

[HV03] Y. Hachimori and O. Venjakob. Completely Faithful Selmer Groups Over Kummer Extensions. *Documenta Mathematica: Extra volume in honour of Kazuya Kato's fiftieth birthday*, pages 443–478, 2003.

[Kat78] N. M. Katz. p-adic L-functions for CM Fields. *Invent. Math.*, 49:199–297, 1978.

[Kat05] K. Kato. K_1 of Some Non-Commutative Completed Group Rings. *K-theory*, 34(2):99–140, 2005.

[Lan80] R. P. Langlands. *Base Change for* GL_2. Annals of Math. Studies 96, Princeton University Press, 1980.

[MT90] B. Mazur and J. Tilouine. Représentations Galoisiennes, Différentielles de Kähler et Conjectures Principales. *Publ. Math. IHES.*, 71:65–100, 1990.

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

[Pan91] A. A. Panchishkin. *Non-Archimedean L-functions of Siegel and Hilbert Modular Forms*. Springer-Verlag, Lecture Notes in Mathematics 1471, 1991.

[Rub99] K. Rubin. Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer. *Arithmetic Theory of Elliptic Curves, Lecture Notes in Mathematics 1716*, pages 167–234, 1999.

[Ser98] J.-P. Serre. *Abelian l-adic Representations and Elliptic Curves*. Research Notes in Mathematics 7, A. K. Peters Ltd., 1998.

[Shi78] G. Shimura. Special Values of the Zeta Functions Associated with Hilbert Modular Forms. *Duke Mathematical Journal*, 45(3), 1978.

[Ste89] G. Stevens. Stickelberger Elements and the Modular Parametrizations of Elliptic Curves. *Inventiones Math.*, 98(1):75–106, 1989.

[Stu80] J. Sturm. Special Values of Zeta Functions and Eisenstein Series of Half-Integral Weight. *American J. Math.*, 102:219–240, 1980.

[Stu89] J. Sturm. Evaluation of the Symmetric Square at the Near Center Point. *American J. Math.*, 111:585–598, 1989.

[Tat79] J. Tate. Number Theoretic Background. *Proceedings of Symposia in Pure Mathematics*, 33(2):3–26, 1979.

[Til89] J. Tilouine. Sur la Conjecture Principale Anticyclotomique. *Duke Mathematical Journal*, 59:629–673, 1989.

[Ven] O. Venjakob. From Classical to Non-Commutative Iwasawa Theory: An Introduction to the GL_2 Main Conjecture.

[Was96] L. Washington. *Introduction to Cyclotomic Fields*. Springer, 1996.

[Wat02] M. Watkins. Computing the Modular Degree of an Elliptic Curve. *Experiment. Math.*, 11(4):487–502, 2002.

[Wil95] A. Wiles. Modular Elliptic Curves and Fermat's Last Theorem. *Annals of Math.*, 141:443–551, 1995.