p-Adic Deformation of Shintani Cycles

Shahab Shahabi*

Abstract

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N with ordinary reduction at a prime p, and let K be a real quadratic field in which all the primes $\ell | N$ are split. Write ϕ for the normalised newform associated to E via Shimura-Taniyama. By Hida's theory, ϕ arises as the specialisation in weight 2 of a family $\{f_k\}$ of forms of varying weight k. We construct a p-adic analytic function $\mathcal{L}(\kappa)$ which interpolates certain Shintani cycles attached to f_k and the real quadratic field K. When p divides N exactly, we show that $\mathcal{L}(\kappa)$ vanishes to order ≥ 2 at $k = 2$. Our main result expresses the second derivative of $\mathcal{L}(\kappa)$ at $k = 2$ as the product of the formal group logarithms of two global points on E, each defined over a quadratic extension of K. This theorem can be viewed as an extension to elliptic curves of a limit formula of Kronecker, in which Eisenstein series are replaced by cusp forms.

1 Introduction

Let K be a real quadratic field of discriminant $\Delta > 0$ and write H_K^+ for the Hilbert narrow class field of K. We shall also let the mapping $\alpha \mapsto \alpha'$ stand for the non-trivial automorphism of K over $\mathbb{Q}$ (i.e., the generator of $\mathrm{Gal}(K/\mathbb{Q})$). By a *genus character* of K we understand an everywhere unramified[1] quadratic character of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of K. We remark that any such $\mathfrak{g}$ may as well be viewed as a (quadratic) character of the Galois group $\mathcal{C}_K^+ := \mathrm{Gal}(H_K^+/K)$. Any non-trivial genus character cuts out a biquadratic extension $K_{\mathfrak{g}} = \mathbb{Q}(\sqrt{\mathfrak{d}_1}, \sqrt{\mathfrak{d}_2})$ of $\mathbb{Q}$ fitting into the following diagram:

$$
\begin{tikzcd}
& H_K^+ \arrow[d, dash] & \\
& K_{\mathfrak{g}} = \mathbb{Q}(\sqrt{\mathfrak{d}_1}, \sqrt{\mathfrak{d}_2}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{\mathfrak{d}_1}) \arrow[dr, dash] & K = \mathbb{Q}(\sqrt{\Delta}) \arrow[d, dash] & \mathbb{Q}(\sqrt{\mathfrak{d}_2}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}
$$

*This work has been partially supported by NSERC and FQRNT grants

[1] More precisely, unramified at all finite places of K.

where $\Delta = \mathfrak{d}_1\mathfrak{d}_2$. In fact the genus characters of K are in a one-to-one correspondence with the factorisations of Δ into a product of two relatively prime fundamental discriminants $\mathfrak{d}_1$ and $\mathfrak{d}_2$, or what amounts to the same thing, in one-to-one correspondence with the unordered pairs (χ_1, χ_2) of primitive quadratic Dirichlet characters of coprime conductors satisfying $\chi_1\chi_2 = \chi_K$, where χ_K is the Dirichlet character associated to K (cf. [S], Chap.II, §1.) Under such bijection, the trivial genus character corresponds to the factorisation $\Delta = 1 \cdot \Delta$ (or equivalently, to the pair $(\chi_{\text{trivial}}, \chi_K)$). If we write σ_λ for the Frobenius element in $\mathcal{C}_K^+$ attached to a prime ideal λ of $\mathcal{O}_K$, then the pair (χ_1, χ_2) is uniquely characterised by the relations

$$\mathfrak{g}(\sigma_\lambda) = \mathfrak{g}(\sigma_{\lambda'}) = \chi_1(\ell) = \chi_2(\ell), \tag{1}$$

valid for any rational prime ℓ which splits in K as $\ell\mathcal{O}_K = \lambda \cdot \lambda'$. The analogous identity at infinity is

$$\mathfrak{g}(\mathfrak{c}) = \chi_1(-1) = \chi_2(-1), \tag{2}$$

where $\mathfrak{c} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is the complex conjugation. A genus character is called even (resp. odd) if $\mathfrak{g}(\mathfrak{c}) = 1$ (resp. $\mathfrak{g}(\mathfrak{c}) = -1$). Equivalently, $\mathfrak{g}$ is even (resp. odd) if and only if it cuts out a totally real (resp. totally imaginary) quadratic extension of K. It is therefore obvious that if $\mathfrak{g}$ is even (resp. odd), then so are both characters χ_1 and χ_2. *We fix once and for all a genus character* $\mathfrak{g}$, *giving us a unique pair of Dirichlet characters attached to it.*

Let now A be an element of the narrow ideal class group of K; a group which is canonically, by global class field theory, isomorphic to $\mathcal{C}_K^+$. Choose a representative $\mathfrak{a}$ of A and without loss of generality assume that $\mathfrak{a}$ acquires a $\mathbb{Z}$-basis of the form $\{1, \tau\}$. Also let ϵ_K be the fundamental unit of K of positive norm [i.e., ϵ_K is either the fundamental unit $u_K > 1$ of K or the square of that depending on whether $\mathrm{Norm}_{K/\mathbb{Q}}(u_K) > 0$ or $\mathrm{Norm}_{K/\mathbb{Q}}(u_K) < 0$]. On writing

$$\gamma_A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{where} \quad \epsilon_K\tau = a\tau + b, \qquad \epsilon_K = c\tau + d \tag{3}$$

one readily verifies that the matrix γ_A is a hyperbolic element of $\mathbf{SL_2}(\mathbb{Z})$ whose fixed points, as a Möbius transformation acting on the upper half-plane $\mathcal{H}$, are τ and τ'. Finally, upon setting

$$Q(z) := \frac{(z-\tau)(z-\tau')}{\mathrm{Norm}(\mathfrak{a})} \in \mathbb{Z}[z] \tag{4}$$

and assuming that $\mathfrak{g}$ is even, one has (cf. [S], Chap.II, §3) the following analogue of Kronecker's solution of Pell's equation in the context of real quadratic fields:

$$\sum_A \mathfrak{g}(A)\mathbf{C}(\eta, \gamma_A) = \frac{2h_1h_2}{\sqrt{\Delta}} \log\epsilon_1 \log\epsilon_2, \tag{5}$$

where A runs over all the elements of the narrow ideal class group of K, where ϵ_1 and h_1 (resp. ϵ_2 and h_2) are the fundamental unit and the narrow class number of the field $\mathbb{Q}(\sqrt{\mathfrak{d}_1})$ (resp. $\mathbb{Q}(\sqrt{\mathfrak{d}_2})$), and where

$$\mathbf{C}(\eta, \gamma_A) := \int_{z_0}^{\gamma_A z_0} \log(|\sqrt[4]{Q(z)}\eta(z)|^2)Q(z)^{-1}dz,$$

is the so-called *Shintani cycle* associated to the data described above. Here the base point z_0 is an arbitrary point on the geodesic joining τ' to τ in the upper half-plane $\mathcal{H}$, and

$$\eta(z) := e^{2\pi iz/24} \prod_{n=1}^{\infty} (1 - e^{2\pi inz}), \qquad z \in \mathcal{H}.$$

is the celebrated eta-function of Dedekind. It is known (cf. [K], Chap. III, §2) that η is intimately related to the Eisenstein series $E_2(z)$ of weight two. More precisely, $E_2(z)$ is, up to a constant, the *logarithmic derivative* of η, viz.

$$\text{dlog } \eta(z) := \frac{\eta'(z)}{\eta(z)} = \frac{2\pi i}{24} E_2(z).$$

The goal of the present paper is to replace the weight 2 Eisenstein series $E_2(z)$ with a cusp form g of even weight $k \geq 2$ and then investigate the p-adic variation of the Shintani cycles attached to K and various specialisations of a Hida family interpolating g.

To begin with, let $\gamma \in \mathbf{SL_2}(\mathbb{Z})$ be a hyperbolic element of the group $\mathbf{SL_2}(\mathbb{Z})$ and assume that $g(z)$ is a cuspidal modular form of even weight k on some congruent subgroup of $\mathbf{SL_2}(\mathbb{Z})$. The *Shintani cycle* attached to g and γ is the integer

$$\mathbf{C}(g, \gamma) := \frac{1}{\Omega_g} \text{Real} \left(\int_{z_0}^{\gamma z_0} g(z) Q(z, 1)^{\frac{k-2}{2}} dz \right), \tag{6}$$

where Ω_g is a suitable period depending only on g (introduced in Section 2) and $Q(x, y)$ is a binary quadratic form that is fixed by γ, i.e., the roots of $Q(z, 1)$ are the fixed points of γ. The quantities $\mathbf{C}(g, \gamma)$ are known to encode interesting arithmetic information, for they are related (see for instance §6 of [P]) to central critical values of the L-series of g over the splitting field of $Q(z, 1)$ [i.e., the real quadratic field generated over $\mathbb{Q}$ by the fixed points of γ]. This very fact has been successfully exploited by several people to study in particular the p-adic variation of the quantities $\mathbf{C}(g, \gamma)$ as g varies in a "family". More concretely, suppose that

$$\phi(z) = \sum_{n=1}^{\infty} a_n q^n, \tag{7}$$

is a normalised newform of weight 2 on $\Gamma_0(N)$ and assume that the p-th Fourier coefficient a_p of ϕ is a p-adic unit. In a canonical way, Hida's theory associates to ϕ a family $\{f_k\}$ of normalised eigenforms of weight k on $\Gamma_0(N)$, for all even integers $k > 2$ in a suitable p-adic neighbourhood U of 2 (see Section 3 for the details). In "good" circumstances one can prove that the assignment

$$k \mapsto \mathbf{C}(f_k, \gamma)$$

extends to a p-adic analytic function of $\kappa \in U$. Therefore it is natural to consider the special values of the resulting function as well as its successive derivatives and wonder if one could describe those values in terms of other arithmetic objects.

Assume henceforward that ϕ has rational Fourier coefficients, and let E be the elliptic curve defined over $\mathbb{Q}$ of conductor N attached to ϕ via Shimura-Taniyama. We further assume that the prime p divides N exactly [i.e., $p|N$ but $p^2 \nmid N$]. This amounts to saying that E has multiplicative reduction at p, and it therefore implies that $a_p = \pm 1$. We shall write $N = pM$. Before stating the main theorem, some further notations are to be introduced.

We let $q \in p\mathbb{Z}_p$ be the Tate period attached to E, and write

$$\Phi_{\mathrm{Tate}} : \mathbb{Q}_p^\times / q^{\mathbb{Z}} \longrightarrow E(\mathbb{Q}_p) \tag{8}$$

for the Tate uniformization whose existence is guaranteed by the fact that p is a prime of multiplicative reduction for E. Let

$$\log_p : \mathbb{Q}_p^\times \longrightarrow \mathbb{Q}_p \tag{9}$$

stand for the branch of p-adic logarithm which satisfies $\log_p(q) = 0$. The two maps Φ_{Tate} and $\log_p$ are used to define the formal group logarithm

$$\log_E : E(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$$

by the rule

$$\log_E(P) := \log_q(\Phi_{\mathrm{Tate}}^{-1}(P)). \tag{10}$$

Note that this is well-defined since $q^{\mathbb{Z}} \subseteq \ker(\log_p)$. One easily sees that the mapping $\log_E$ is a group homomorphism.

For each divisor $d|N$ with $\gcd(d, \frac{N}{d}) = 1$, we let w_d stand for the eigenvalue of the *Fricke involution* W_d acting on ϕ, namely,

$$(W_d|\phi)(z) := \phi|\begin{pmatrix} 0 & -1 \\ d & 0 \end{pmatrix}(z) = w_d \cdot \phi(z). \tag{11}$$

For $j = 1, 2$, we write $(E(\mathbb{Q}(\sqrt{\mathfrak{d}_j})) \otimes \mathbb{Q})^{\chi_j}$ for the subgroup of the Mordell-Weil group $E(H_K^+)$ on which the group $\mathrm{Gal}(H_K^+/K)$ acts via the character χ_j. If all the primes $\ell|N$ are split in K, then

Main Theorem *(i) There exists a p-adic analytic function $\mathcal{L}(\kappa)$ of κ, defined over a suitable p-adic neighbourhood U of 2, which interpolates the $\mathfrak{g}$-twisted Shintani cycles*

$$\sum_A \mathfrak{g}(A)\mathbf{C}(f_k, \gamma_A),$$

for all $k \in U \cap \mathbb{Z}^{\geq 2}$.

(ii) Suppose further that E has at least two primes of multiplicative reduction, that $\chi_1(-N) = w_N$ and that $\chi_1(p) = a_p$. Then:

(a) $\mathcal{L}(\kappa)$ vanishes to order at least two at $k = 2$;

(b) There exist global points $P_{\chi_1} \in (E(\mathbb{Q}(\sqrt{\mathfrak{d}_1})) \otimes \mathbb{Q})^{\chi_1}$ and $P_{\chi_2} \in (E(\mathbb{Q}(\sqrt{\mathfrak{d}_2})) \otimes \mathbb{Q})^{\chi_2}$ and a non-zero rational number t such that

$$\frac{d^2}{d\kappa^2}\mathcal{L}(\kappa)\Big|_{k=2} = t \log_E(P_{\chi_1}) \log_E(P_{\chi_2}); \tag{12}$$

(c) The two points P_{χ_1} and P_{χ_2} are both of infinite order if and only

$$L''(E/K, \mathfrak{g}; 1) \neq 0.$$

Note the strong analogy between (12) and (5). In fact, the Main Theorem illuminates another instance of the close parallel between units of number fields and points on elliptic curves. The Dirichlet unit theorem is analogous to the Mordell-Weil theorem ; Stark units are number field counterparts of Stark-Heegner points on elliptic curves; to name just a few examples.

Remark 1.1. In this remark only assume that the prime p is inert in K (while we continue to assume that all the prime divisors of M are still split in K) and that K has narrow class number one. If the other hypotheses are as before, then Bertolini and Darmon [BD1] prove that there exists a global point P on E and defined over K, such that

$$\frac{d}{d\kappa}\mathbf{C}(f_k, \gamma_A)\big|_{k=2} \doteq \log_E(P),$$

where the symbol $\doteq$ denotes the equality up to an explicit non-zero fudge factor. They also show that the point P is of infinite order if and only if

$$L'(E/K, 1) \neq 0.$$

Indeed, the present work has been influenced by [BD1], a source from which many constructions and results have been borrowed.

Acknowledgement 1.2. This article presents the main part of the author's Ph.D. project under the supervision of Henri Darmon at McGill University. I hereby would like to express my indebtedness to Professor Darmon for proposing this project to me. I wish also to deeply acknowledge his constant help, generosity and encouragement, from which I have greatly benefited, during the time of preparation of this work.

2 Modular Symbols

2.1 Generalities on Modular Symbols

Definition 2.1. Let $\mathcal{D}_0$ denote the group of degree zero divisors on the rational projective line $\mathbb{P}_1(\mathbb{Q})$. For an abelian group A, any element of $\mathrm{Hom}_{\mathbb{Z}}(\mathcal{D}_0, A)$ is called an A-valued modular symbol. In other words, a modular symbol $\mathfrak{m}$ is an assignment which to any divisor of the form $D = (r) - (s) \in \mathcal{D}_0$, where $r, s \in \mathbb{P}_1(\mathbb{Q})$, attaches an element $\mathfrak{m}\{r \to s\}$ of A, and satisfies the relation

$$\mathfrak{m}\{r \to s\} + \mathfrak{m}\{s \to t\} = \mathfrak{m}\{r \to t\},$$

for all $r, s, t \in \mathbb{P}_1(\mathbb{Q})$. We denote by $\mathcal{MS}(A)$ the set of all such modular symbols.

If A is endowed with a left action of a subgroup G of $\mathbf{GL_2}(\mathbb{Q})$, then one may let G act on $\mathcal{MS}(A)$ on the right by the rule

$$(\mathfrak{m}, \gamma) \longrightarrow \mathfrak{m}|\gamma,$$

$$(\mathfrak{m}|\gamma)\{r \to s\} := \gamma^{-1}\mathfrak{m}\{\gamma r \to \gamma s\},$$

where G is acting on $\mathbb{P}_1(\mathbb{Q})$ on the left by the usual Möbius transformations. Thus, $\mathcal{MS}(A)$ has the structure of a right G-module.

It is readily seen from the definition that a modular symbol $\mathfrak{m}$ is G-invariant (i.e., $\mathrm{Stab}_G(\mathfrak{m}) = G$) if

$$\gamma^{-1}\mathfrak{m}\{\gamma r \to \gamma s\} = \mathfrak{m}\{r \to s\}, \text{ for all } \gamma \in G,$$

or equivalently,

$$\gamma\mathfrak{m}\{r \to s\} = \mathfrak{m}\{\gamma r \to \gamma s\}, \text{ for all } \gamma \in G.$$

The set of all G-invariant modular symbols will be denoted by $\mathcal{MS}_G(A)$.

2.2 Modular Symbols Attached to Modular Forms

Germane to the investigations of the present article are modular symbols attached to modular forms. Let

$$g = \sum_{n=1}^{\infty} a_n(g) q^n \in S_k(\Gamma_0(N)) \tag{13}$$

be a normalized eigenform of even weight $k \geq 2$ on $\Gamma_0(N)$, and denote by K_g the field generated over $\mathbb{Q}$ by the Fourier coefficients $a_n(g)$. It can be proved that K_g is a totally real number field (cf. [DS], Chapter 6). Whenever necessitated by the context, we will regard the field K_g as a complex field (resp. as a p-adic field) by fixing once and for all an embedding of K_g into $\mathbb{C}$ (resp. into $\mathbb{C}_p$.)

Let now F be a subfield of $\mathbb{C}$ or $\mathbb{C}_p$. For a given $k \geq 2$, let $\mathbf{P}_k(F)$ be the space of homogeneous polynomials of degree $k-2$ in two variables with coefficients in F. The rule

$$(P|\gamma)(X, Y) := P(aX + bY, cX + dY), \qquad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{14}$$

endows $\mathbf{P}_k(F)$ with a right linear (i.e., $(P_1 + P_2)|\gamma = P_1|\gamma + P_2|\gamma$.) action of $\mathbf{GL_2}(F)$.

We also denote by $\mathbf{V}_k(F)$ the F-linear dual to $\mathbf{P}_k(F)$. The rule

$$(\gamma \cdot \phi)(P) := \phi(P|\gamma), \tag{15}$$

where $\phi \in \mathbf{V}_k(F), \gamma \in \mathbf{GL}_2(F)$ and $P \in \mathbf{P}_k(F)$ also shows that $\mathbf{V}_k(F)$ inherits a left linear action by the same group.

The motivation to bring up these spaces is the following well known construction of Eichler and Shimura which to the form g associates a $\mathbf{V}_k(\mathbb{C})$-valued modular symbol $\widetilde{\mathbf{I}}_g$ by assigning to any homogeneous polynomial $P(X, Y)$ in $\mathbb{C}[X, Y]$ of degree $k-2$ the complex integral

$$\widetilde{\mathbf{I}}_g\{r \to s\}(P) := 2\pi i \int_r^s g(z)P(z,1)dz, \tag{16}$$

where the integral is along the geodesic on the upper half-plane joining r and s. One notices that since g is assumed to be a cusp form, the integral used to define $\widetilde{\mathbf{I}}_g$ is convergent. The invariance property of the holomorphic differential $2\pi i g(z)$ under the group $\Gamma_0(N)$ also implies, after a simple change of variables, that the modular symbol $\widetilde{\mathbf{I}}_g$ enjoys an invariance property under the action of the same group, i.e., for any $\gamma \in \Gamma_0(N)$,

$$\widetilde{\mathbf{I}}_g\{\gamma^{-1}r \to \gamma^{-1}s\}(P|\gamma) = \widetilde{\mathbf{I}}_g\{r \to s\}(P).$$

In other words, $\widetilde{\mathbf{I}}_g$ belongs to $\mathcal{MS}_{\Gamma_0(N)}(\mathbf{V}_k(\mathbb{C}))$. One decomposes this latter space as a direct sum of two eigen-subspaces of the linear involution

$$\mathfrak{m} \longrightarrow \mathfrak{m}|\iota$$

induced by the matrix $\iota = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. This is made possible by exploiting the fact that ι normalizes the group $\Gamma_0(N)$, i.e. $\iota^{-1}\Gamma_0(N)\iota = \Gamma_0(N)$, and that $\iota^2 = \mathbf{1}_2$. This gives rise to the decomposition of $\mathcal{MS}_{\Gamma_0(N)}(\mathbf{V}_k(\mathbb{C}))$ as a direct sum of the two eigen-subspaces corresponding to the two eigenvalues $+1$ and -1 respectively. For any $\Gamma_0(N)$-invariant modular symbol $\mathfrak{m}$, write respectively $\mathfrak{m}^+$ and $\mathfrak{m}^-$ for the plus and minus eigen-components of $\mathfrak{m}$ with respect to the involution above. This being done, we have the following important theorem of Shimura (cf. [Shim77]).

Theorem 2.2. (Shimura) There exist complex periods Ω_g^+ and Ω_g^- with the property that the modular symbols

$$\mathbf{I}_g^+ := \frac{1}{\Omega_g^+}\widetilde{\mathbf{I}}_g^+, \qquad \mathbf{I}_g^- := \frac{1}{\Omega_g^-}\widetilde{\mathbf{I}}_g^-$$

belong to $\mathcal{MS}_{\Gamma_0(N)}(\mathcal{O}_g)$, where $\mathcal{O}_g$ is the ring of integers of the number field K_g. These periods can be chosen so as to satisfy

$$\Omega_g^+\Omega_g^- = \langle g, g \rangle,$$

where $\langle , \rangle$ is the Petersson inner product on $S_k(N)$.

We recall the fixed genus character $\mathfrak{g}$ and the corresponding pair of Dirichlet characters (χ_1, χ_2) of the Introduction, and set

$$\Omega_g := \begin{cases} \Omega_g^+ & \text{if } \mathfrak{g}(\mathfrak{c}) = +1; \\ \Omega_g^- & \text{if } \mathfrak{g}(\mathfrak{c}) = -1; \end{cases} \qquad \mathbf{I}_g := \begin{cases} \mathbf{I}_g^+ & \text{if } \mathfrak{g}(\mathfrak{c}) = +1; \\ \mathbf{I}_g^- & \text{if } \mathfrak{g}(\mathfrak{c}) = -1. \end{cases}$$

2.3 Relation with the Values of Twisted Complex L-Functions

Let χ be a primitive Dirichlet character of conductor $\mathfrak{f}$. The twisted L-function $L(g, \chi; s)$ attached to the cusp form g of the previous section begins life as the Dirichlet series

$$L(g, \chi; s) := \sum_{n=1}^{\infty} \chi(n) a_n(g) n^{-s}, \tag{17}$$

originally defined over the half-plane $\mathrm{Re}(s) > \dfrac{k+1}{2}$. One knows ([Shim72], Chap. 3), however, that $L(g, \chi; s)$ has an analytic continuation to the whole complex plane. We wish now to study the central critical values $L(g, \chi; j)$ $(1 \leq j \leq k-1)$ of the function $L(g, \chi, s)$, by means of the modular symbol $\mathbf{I}_g$. So, for any integer a, let

$$\mathbf{I}_g[j, a] := \mathbf{I}_g\{\infty \to \frac{a}{\mathfrak{f}}\}(P(X, Y)),$$

where $P(X, Y)$ is the degree $k-2$ homogeneous polynomial

$$P(X, Y) = \left(X - \frac{a}{\mathfrak{f}} Y\right)^{j-1} Y^{k-j-1}.$$

and where the even integer $k \geq 2$ is as before the weight of the form g. By exploiting the invariance property of $\mathbf{I}_g$ under the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, one readily verifies that $\mathbf{I}_g[j, a]$, as a function of a, is $\mathfrak{f}$-periodic, i.e., its value depends only on the class of a modulo $\mathfrak{f}$.

Before stating the relationship between critical values of $L(g, \chi; s)$ and $\mathbf{I}_g$, we need to recall the definition of the Gauss sum $\tau(\chi)$ attached to χ. It should be noted that for the following definition χ need not be primitive; we stick to this assumption, however, because it is needed in the proposition below. The Gauss sum associated to χ is by definition the quantity

$$\tau(\chi) := \sum_{a=1}^{\mathfrak{f}} \chi(a) e^{\frac{2\pi i a}{\mathfrak{f}}},$$

and it satisfies the well known relation $|\tau(\chi)|^2 = \chi(-1)\tau(\chi)\tau(\overline{\chi}) = \mathfrak{f}$. For a proof of the following proposition, the reader is referred to [MTT], Chap. I, §8.

Proposition 2.3. The assumptions being as before, the quantity

$$L^*(g, \chi; j) := \frac{(j-1)! \tau(\chi)}{(-2\pi i)^{j-1} \Omega_g} L(g, \chi; j) \tag{18}$$

is related to modular symbols via the formula

$$L^*(g,\chi;j) = \sum_{a \bmod \mathfrak{f}} \chi(a)\mathbf{I}_g[j,a]. \tag{19}$$

If we further assume that $\chi(-1) = (-1)^{j-1}\mathfrak{g}(\mathfrak{c})$, then

$$L^*(g,\chi;j) \in K_g.$$

The chosen embedding of K_g into $\mathbb{C}_p$ will allow us, in light of the second part of the proposition, to view $L^*(g,\chi;j)$, a priori a complex number and often referred to as the *algebraic part* of $L(g,\chi;j)$, as an element of $\mathbb{C}_p$.

3 Hida Families Attached to Ordinary Forms

We begin by recalling some standard facts concerning the ring of Iwasawa functions. It is a known fact that the group of p-adic units $\mathbb{Z}_p^\times$ decomposes canonically as the product of the group of *principal units* $1+p\mathbb{Z}_p$ and the group $\boldsymbol{\mu}_{p-1}$ of $(p-1)$st roots of unity:

$$\begin{aligned} \mathbb{Z}_p^\times &= (1+p\mathbb{Z}_p)\times\boldsymbol{\mu}_{p-1} \\ t &= \langle t\rangle\cdot\omega(t), \end{aligned} \tag{20}$$

where $\langle\cdot\rangle$ denotes the projection to principal units and where the projection to roots of unity is given by the *Teichmüller character* $\omega(\cdot)$. One can show that for all $t\in\mathbb{Z}_p^\times$, the relation $\langle t\rangle = \lim_n t^{1-p^n}$ holds. Now let

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

denote the usual *Iwasawa algebras*, i.e., the completed group rings of $\mathbb{Z}_p^\times$ and $(1+p\mathbb{Z}_p)^\times$ respectively. For each element $t\in\mathbb{Z}_p^\times$, let $[t]\in\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$ denote the corresponding element of $\mathbb{Z}_p[[\mathbb{Z}_p^\times]]$. For each continuous character

$$\kappa : \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times$$

we denote by the same symbol the unique continuous ring homomorphism $\kappa : \tilde{\boldsymbol{\Lambda}} \longrightarrow \mathbb{Z}_p$ sending $[t]$ to $\kappa(t)$ for all $t\in\mathbb{Z}_p^\times$. This induces the identification

$$\mathcal{X} := \mathrm{Hom}_{\mathrm{ct}}(\tilde{\boldsymbol{\Lambda}},\mathbb{Z}_p) = \mathrm{Hom}_{\mathrm{ct}}(\mathbb{Z}_p^\times,\mathbb{Z}_p^\times) \cong \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}\times\mathbb{Z}_p, \tag{21}$$

and makes it possible to regard elements of $\tilde{\boldsymbol{\Lambda}}$ as functions on the space $\mathcal{X}$ and write $\lambda(\kappa)$ for $\kappa(\lambda)$, where $\lambda\in\tilde{\boldsymbol{\Lambda}}$ and $\kappa\in\mathcal{X}$. One embeds $\mathbb{Z}$ into the space $\mathcal{X}$ by the rule

$$k\mapsto\mathbf{x}_k, \qquad \mathbf{x}_k(t) := t^{k-2} \quad \text{for } t\in\mathbb{Z}_p^\times.$$

Reserving the letter κ for a generic element of $\mathcal{X}$ and following an abuse of notation, we shall write k in place of its image under the above embedding. It is noted that under such embedding the element 2 corresponds to the augmentation map on $\tilde{\mathbf{\Lambda}}$ and $\mathbf{\Lambda}$. It is also noted that $\mathcal{X}$ with its natural topology contains $\mathbb{Z}^{\geq 2}$ as a dense subset. Hence, $U \cap \mathbb{Z}^{\geq 2}$ is dense in U, for any open subset U of $\mathcal{X}$.

Recall that E has multiplicative reduction at p. This follows from the fact that the p-th Fourier coefficient a_p of ϕ is ± 1, and hence a p-adic unit. Following Hida [H](see also [GS] and [BD2]), one can attach to ϕ a formal power series

$$\mathbf{h}_\infty = \sum_{n=1}^{\infty} \mathfrak{a}_n q^n = \sum_{n=1}^{\infty} \mathfrak{a}_n(\kappa) q^n \tag{22}$$

with the coefficients $\mathfrak{a}_n = \mathfrak{a}_n(\kappa)$ in the ring $\mathcal{A}(U)$ of p-adic analytic functions on an appropriate neighbourhood U of $2 \in \mathcal{X}$. We may assume for simplicity that U is contained in the residue disc of 2 modulo $p-1$. This is made possible by the fact that since $\mathcal{X}$ is identified with the direct product of $\mathbb{Z}/(p-1)\mathbb{Z}$ and $\mathbb{Z}_p$, it could be viewed as a disjoint union of $p-1$ copies of $\mathbb{Z}_p$. The formal q-expansion $\mathbf{h}_\infty$ is characterised by the following two properties:

- For any integer $k \geq 2$ in U, the q-expansion

  $$f_k := \sum_{n=1}^{\infty} \mathfrak{a}_n(k) q^n \tag{23}$$

  is a normalized classical eigenform of weight k on $\Gamma_0(N)$. For that reason, the form $f_k = \sum_{n=1}^{\infty} a_n(f_k) q^n$ is often referred to as the weight-k-specialization of $\mathbf{h}_\infty$.
- $f_2 = \phi$.

Remark 3.1. While being new at all the prime divisors of M, the form f_k (for $k > 2$) is *old* at the prime p in the sense that it arises from a normalised newform $\hat{f}_k = \sum_{n=1}^{\infty} \hat{a}_n(k) q^n$ of weight k on $\Gamma_0(M)$. More precisely, one has

$$f_k(z) = \hat{f}_k(z) - \beta_p(k) \hat{f}_k(pz),$$

where $\beta_p(k)$ is the *Frobenius non-unit root* appearing in the factorisation of the Euler p-factor of the L-series of $\hat{f}_k$ as

$$1 - \hat{a}_p(k) p^{-s} + p^{k-1-2s} = (1 - \alpha_p(k) p^{-s})(1 - \beta_p(k) p^{-s}).$$

It is possible to order the Frobenius unit and non-unit eigenvalues $\alpha_p(k)$ and $\beta_p(k)$ in such a way that

$$\alpha_p(k) = a_p(k), \quad \beta_p(k) = p^{k-1} a_p(k)^{-1}.$$

With this conventions, one can also verify that if $p \nmid n$, then $\hat{a}_n(k) = a_n(f_k)$. Therefore, the relationship between their associated χ-twisted L-functions turns out to be

$$L(f_k, \chi; s) = \left(1 - \chi(p) a_p(k)^{-1} p^{k-1-s}\right) L(\hat{f}_k, \chi; s). \tag{24}$$

It follows from the preceding discussion that the number field $K_{\hat{f}_k}$ generated by the Fourier coefficients of $\hat{f}_k$ is the same as that of f_k; it could therefore, as before, be viewed as a subfield of both $\mathbb{C}$ and $\mathbb{C}_p$. Also as in Proposition 2.2, to the form f_k are associated the Shimura periods $\Omega^{\pm}_{f_k}$ as well as the modular symbol $\mathbf{I}_{f_k}$. In order to relax the notation, we shall write

$$\Omega^{\pm}_k := \Omega^{\pm}_{f_k}, \qquad \mathbf{I}_k := \mathbf{I}_{f_k}, \qquad \hat{\mathbf{I}}_k := \mathbf{I}_{\hat{f}_k}.$$

We choose $\Omega^{\pm}_k$ so as to satisfy

$$\Omega^+_2 \Omega^-_2 = \langle \phi, \phi \rangle, \qquad\qquad \Omega^+_k \Omega^-_k = \langle \hat{f}_k, \hat{f}_k \rangle \quad (k > 2),$$

and then use them as in (18) to define likewise the algebraic part of the special values of $L(\hat{f}_k, \chi; s)$. Note that, with these conventions and for $1 \leq j \leq k-1$, one has

$$L^*(f_k, \chi; j) = (1 - \chi(p) a_p(k)^{-1} p^{k-1-j}) L^*(\hat{f}_k, \chi; j).$$

To define the algebraic part of the $\mathfrak{g}$-twisted L-function $L(f_k/K, \mathfrak{g}; s)$ of the form f_k over the real quadratic field K of the Introduction, let us first remark that, just by comparing the Euler factors at various primes, one verifies the relation

$$L(f_k/K, \mathfrak{g}; s) = L(f_k, \chi_1; s) L(f_k, \chi_2; s). \tag{25}$$

The algebraic part of $L(f_k/K, \mathfrak{g}; s)$ is now defined as the quantity

$$L^*(f_k/K, \mathfrak{g}; s) := \frac{\Delta^{\frac{k-1}{2}} (k/2-1)!^2}{(2\pi i)^{k-2} \langle f_k, f_k \rangle} L(f_k/K, \mathfrak{g}; s). \tag{26}$$

4 Measure-Valued Modular Symbols

Let

$$L_* := \mathbb{Z}_p^2 = \mathbb{Z}_p \oplus \mathbb{Z}_p \tag{27}$$

denote the *standard* $\mathbb{Z}_p$-lattice in $\mathbb{Q}_p^2$. For any $\mathbb{Z}_p$-lattice L in $\mathbb{Q}_p^2$, we write L' for the set of *primitive vectors* in L, that is, the set of those vectors $v \in L$ which are not divisible by p in L:

$$L' := L \setminus pL = \{v \in L \ : \ v \notin pL\}. \tag{28}$$

Note, for example, that

$$L'_* = (\mathbb{Z}_p \times \mathbb{Z}_p^{\times}) \sqcup (\mathbb{Z}_p^{\times} \times p\mathbb{Z}_p), \tag{29}$$

which is a simple consequence of the fact that $\mathbb{Z}_p = \mathbb{Z}_p^\times \sqcup p\mathbb{Z}_p$.[2]

We equip the space of continuous $\mathbb{C}_p$-valued functions on L'_* with the right action of $\mathbf{GL_2}(\mathbb{Z}_p)$ defined by the rule

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

and with a topology given by the sup norm. Its continuous dual, denoted $\mathbf{D}_*$, is called the space of *measures* on L'_*. The action of the group $\mathbb{Z}_p^\times$ on L'_* given by $t(x,y) := (tx, ty)$ gives rise to a natural $\tilde{\mathbf{\Lambda}}$-module structure on $\mathbf{D}_*$ by setting

$$\int_{L'_*} F(x,y) d([t]\cdot\mu)(x,y) := \int_{L'_*} F(tx,ty) d\mu(x,y),$$

for all $t \in \mathbb{Z}_p^\times$. If X is any compact-open subset of L'_*, we adopt the common notation

$$\int_X F d\mu := \int_{L'_*} \mathbf{1}_X F d\mu,$$

where $\mathbf{1}_X$ is the indicator (i.e., characteristic) function of X. Note that the group $\mathbf{GL_2}(\mathbb{Z}_p)$ also acts on $\mathbf{D}_*$ on the left by translation, so that

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

Denote by $\Gamma_0(p\mathbb{Z}_p)$ the group of matrices in $\mathbf{GL_2}(\mathbb{Z}_p)$ which are upper triangular modulo p. The space $\mathbf{D}_*$ is endowed, for all $k \in \mathbb{Z}^{\geq 2}$, with a $\Gamma_0(p\mathbb{Z}_p)$-equivariant homomorphism

$$\rho_k : \mathbf{D}_* \longrightarrow \mathbf{V}_k(\mathbb{C}_p), \quad \mu \mapsto \rho_k(\mu)$$

defined by the rule

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

One easily notes that any mapping $\rho : A \longrightarrow B$ between abelian groups induces a mapping on modular symbols $\mathcal{MS}(A) \longrightarrow \mathcal{MS}(B)$, $\mathfrak{m} \mapsto \rho(\mathfrak{m})$, by the rule

$$(r,s) \mapsto \rho(\mathfrak{m}\{r \to s\}).$$

In particular, the homomorphisms ρ_k, for all $k \geq 2$, lift to homomorphisms on modular symbols. It can also be verified that such lift will send $\Gamma_0(M)$-invariant $\mathbf{D}_*$-valued modular symbols to $\Gamma_0(N)$-invariant $\mathbf{V}_k(\mathbb{C}_p)$-valued modular symbols (cf. [GS]). That is to say, each ρ_k gives rise to a mapping

$$\rho_k : \mathcal{MS}_{\Gamma_0(M)}(\mathbf{D}_*) \longrightarrow \mathcal{MS}_{\Gamma_0(N)}(V_k),$$

which is, just for simplicity, denoted by the same letter.

[2] The symbol $\sqcup$ stands for the *disjoint union.*

We denote by $\mathbf{\Lambda}^\dagger \supset \mathbf{\Lambda}$ the ring of power series with coefficients in $\mathbb{C}_p$ which converge in some neighbourhood of $2 \in \mathcal{X}$, and set

$$\mathbf{D}_*^\dagger := \mathbf{D}_* \otimes_{\mathbf{\Lambda}} \mathbf{\Lambda}^\dagger.$$

If

$$\mu = \lambda_1\mu_1 + \cdots + \lambda_r\mu_r, \qquad \text{with } \lambda_j \in \mathbf{\Lambda}^\dagger,\ \mu_j \in \mathbf{D}_*,$$

is any element of $\mathbf{D}_*^\dagger$, then there exists a neighbourhood U_μ of $2 \in \mathcal{X}$ on which all the coefficients λ_j converge. Call such a region U_μ a *neighbourhood of regularity* for μ.

Given $\kappa \in U_\mu$, a continuous function $F(x,y)$ on L'_* is said to be *homogeneous of degree* $\kappa - 2$ if $F(tx, ty) = t^{\kappa-2}F(x,y)$, for all $t \in \mathbb{Z}_p^\times$. For any $\kappa \in U_\mu$, and any homogeneous function $F(x,y)$ of degree $\kappa - 2$, the function F can be integrated against μ by the rule

$$\int_X F d\mu := \lambda_1(k)\int_X F d\mu_1 + \cdots + \lambda_r(k)\int_X F d\mu_r,$$

for any compact-open $X \subset L'_*$.

The space $\mathcal{MS}_{\Gamma_0(M)}(\mathbf{D}_*)$ is equipped with a natural action of the Hecke operator U_p, given by the formula

$$\int_X F d(U_p|\mu)\{r \to s\} := \sum_{a=0}^{p-1} \int_{\frac{1}{p}\gamma_a(X)} (F|p\gamma_a^{-1}) d\mu\{\gamma_a r \to \gamma_a s\},$$

where for each $0 \le a \le p-1$, $\gamma_a := \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix}$. Let $\mathcal{MS}^{\text{ord}}_{\Gamma_0(M)}(\mathbf{D}_*)$ denote the *ordinary subspace* of $\mathcal{MS}_{\Gamma_0(M)}(\mathbf{D}_*)$, and set

$$\mathcal{MS}^{\text{ord}}_{\Gamma_0(M)}(\mathbf{D}_*)^\dagger := \mathcal{MS}^{\text{ord}}_{\Gamma_0(M)}(\mathbf{D}_*) \otimes_{\mathbf{\Lambda}} \mathbf{\Lambda}^\dagger \subset \mathcal{MS}_{\Gamma_0(M)}(\mathbf{D}_*^\dagger).$$

Given $\mu \in \mathcal{MS}^{\text{ord}}_{\Gamma_0(M)}(\mathbf{D}_*)^\dagger$, the measure $\mu\{r \to s\}$, for $r, s \in \mathbb{P}_1(\mathbb{Q})$, may be viewed as an element of $\mathbf{D}_*^\dagger$, and a common neighbourhood of regularity U_μ for all the measures $\mu\{r \to s\}$ can be chosen. This makes it possible to define $\rho_k(\mu)$ for all $k \in U_\mu \cap \mathbb{Z}^{\ge 2}$. All this being said, we record the following important result of Greenberg and Stevens [GS].

Theorem 4.1. (Greenberg-Stevens) There exists a neighbourhood U of $2 \in \mathcal{X}$ and a measure-valued modular symbol $\mu_* \in \mathcal{MS}^{\text{ord}}_{\Gamma_0(M)}(\mathbf{D}_*)^\dagger$ which is regular on U, and satisfies the following two conditions:

1. For each $k \in U \cap \mathbb{Z}^{\ge 2}$, there exists a scalar $\lambda(k) \in \mathbb{C}_p$ such that

$$\rho_k(\mu_*) = \lambda(k)\mathbf{I}_k. \tag{30}$$

   In other words, for any $r, s \in \mathbb{P}_1(\mathbb{Q})$ and any homogeneous polynomial $P(X,Y) \in \mathbf{P}_k(\mathbb{C}_p)$ of degree $k-2$, we have

$$\int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} P(x,y) d\mu_*\{r \to s\} = \lambda(k)\mathbf{I}_k\{r \to s\}\left(P(z,1)\right). \tag{31}$$

2. $\lambda(2) = 1$.

Remark 4.2. According to Proposition 1.7 of [BD2] the neighbourhood U in the statement of theorem above may be chosen so as to satisfy

$$\lambda(k) \neq 0, \quad \text{for all } k \in U \cap \mathbb{Z}^{\geq 2}.$$

We assume, from now on, that this has been done.

It will be important to know what happens if we integrate a homogeneous polynomial of degree $k-2$ against the measure μ_* over the larger domain $L'_* = (\mathbb{Z}_p \times \mathbb{Z}_p^\times) \sqcup (\mathbb{Z}_p^\times \times p\mathbb{Z}_p)$. Such identity is furnished by the next proposition whose proof is explained in [BD1].

Proposition 4.3. For any $r, s \in \mathbb{P}_1(\mathbb{Q})$ and for any homogeneous polynomial $P(X,Y) \in \mathbf{P}_k(\mathbb{C}_p)$ of degree $k-2$, we have

$$\int_{L'_*} P(x,y) d\mu_*\{r \to s\} = \lambda(k)(1 - a_p(k)^{-2} p^{k-2}) \hat{\mathbf{I}}_k\{r \to s\} \left(P(z,1)\right). \tag{32}$$

Let $\mathbf{D}$ denote the $\boldsymbol{\Lambda}$-module of compactly supported measures on

$$\mathcal{W} := \mathbb{Q}_p^2 \setminus \{(0,0)\} = \{v \in \mathbb{Q}_p^2 \ : \ v \neq (0,0)\},$$

and put $\mathbf{D}^\dagger := \mathbf{D} \otimes_{\boldsymbol{\Lambda}} \boldsymbol{\Lambda}^\dagger$. The space $\mathbf{D}_*$ is contained in $\mathbf{D}$ by viewing elements of $\mathbf{D}_*$ as measures on $\mathcal{W}$ with compact support in L'_*. In Proposition 1.8 of [BD2] (see also [BDI]), a family $\{\mu_L\}$ of $\mathbf{D}^\dagger$-valued modular symbols indexed by the $\mathbb{Z}_p$-lattices L in $\mathbb{Q}_p^2$ is attached to μ_* by exploiting the action of the group

$$\sum := \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL_2}(\mathbb{Z}[1/p]) \ : \ M \mid c, \quad \det(\gamma) > 0 \right\}. \tag{33}$$

Proposition 4.4. There exists a unique collection $\{\mu_L\}$ of $\mathbf{D}^\dagger$-valued modular symbols, indexed by the $\mathbb{Z}_p$-lattices $L \subset \mathbb{Q}_p^2$, and satisfying

1. $\mu_{L_*} = \mu_*$;
2. For all $\gamma \in \sum$, and all compact-open $X \subset \mathcal{W}$,

$$\int_{\gamma X} (F|\gamma^{-1}) d\mu_{\gamma L}\{\gamma r \to \gamma s\} = \int_X F d\mu_L\{r \to s\}. \tag{34}$$

5 p-Adic L-Functions

In this section we recall the definitions and/or some basic properties of various L-functions which play a role in this article. Our account will be very brief, and we will only provide references for the convenience of the reader.

5.1 Mazur-Swinnerton-Dyer p-Adic L-Function Attached to E

The article [MTT] (see also [GS]), based on ideas of [MSD], explains how a one variable p-adic L-function $L_p(g, \chi; s)$ could be attached to any pair consisting of an ordinary[3] normalised eigenform g on $\Gamma_0(N)$ and a Dirichlet character χ of conductor prime to N, viewed as a character with values in $\mathbb{C}_p^\times$. If χ is the trivial character, we simply write $L_p(g, s)$. In particular, since the p-th Fourier coefficient a_p of the newform ϕ of the Introduction is ± 1, hence a p-adic unit, ϕ possesses a p-adic L-function $L_p(\phi, s)$ attached to it. We set

$$L(E, s) := L(\phi, s), \quad \text{and} \quad L_p(E, s) := L_p(\phi, s).$$

Both the complex and the p-adic L-functions satisfy functional equations with respect to the substitution $s \mapsto 2 - s$. More precisely, if we let

$$\Lambda(E, s) := N^{s/2}(2\pi)^{-s}L(E, s) \quad \text{and} \quad \Lambda_p(E, s) := \langle M \rangle^{s/2} L_p(E, s),$$

then

$$\Lambda(E, 2 - s) = -w_{_N}\Lambda(E, s) \quad \text{and} \quad \Lambda_p(E, 2 - s) = -w_{_M}\Lambda(E, s), \tag{35}$$

where, as before, w_d (for $d|N$ and $(d, N/d) = 1$) is the eigenvalue of the Fricke involution W_d of (11) acting on ϕ. [Needles to say that in the first functional equation s is a complex variable, whereas in the second s represents a p-adic variable.] More generally, for any quadratic Dirichlet character χ of conductor prime to N, the sign in the functional equation satisfied by $L(E, \chi; s)$ is equal to $-w_{_N}\chi(-N)$. The relationship between $w_{_N}$ and $w_{_M}$ is given by a result of Atkin and Lehner as

$$w_{_N} = -a_p w_{_M}. \tag{36}$$

This relation is indeed equivalent to the equality $w_p = -a_p$ (cf. [GS]).

5.2 Mazur-Kitagawa p-adic L-function

The p-adic L-functions $L_p(f_k, s)$, associated to the weight-k-specialisations of $\mathbf{h}_\infty$, can be packaged into a single two-variable p-adic L-function. Mazur and Kitagawa were the first to construct examples of these two-variable p-adic L-functions attached to any ordinary $\mathbf{\Lambda}$-adic cusp form (cf, §3 of [GS]). This $\mathbb{C}_p$-valued function $L_p(\mathbf{h}_\infty; \kappa, s)$ is p-adic analytic on $U \times \mathbb{Z}_p$, and for each integer $k \geq 2$ in U, interpolates the p-adic L-function $L_p(f_k, s)$ in the sense that

$$L_p(\mathbf{h}_\infty; k, s) = \lambda(k)L_p(f_k, s), \quad (s \in \mathbb{Z}_p)$$

[3] "Ordinary" simply means that the p-th Fourier coefficient $a_p(g)$ is p-integral.

where $\lambda(k)$ is as in the Equation (30). More generally, one can attach to $\mathbf{h}_\infty$ and a quadratic Dirichlet character χ a p-adic analytic function which likewise interpolates the twisted p-adic L-functions $L_p(f_k, \chi; s)$. Thus, let $\chi : \left(\frac{\mathbb{Z}}{\mathfrak{f}\mathbb{Z}}\right)^\times \longrightarrow \{\pm 1\}$ be a primitive (quadratic) Dirichlet character of conductor $\mathfrak{f}$, and as before, let $\tau(\chi)$ denote the Gauss sum attached to it.

Definition 5.1. The Mazur-Kitagawa two-variable p-adic L-function associated to $\mathbf{h}_\infty$ and χ is the function of $(k, s) \in U \times \mathbb{Z}_p$ defined by the rule

$$L_p(\mathbf{h}_\infty, \chi; \kappa, s) := \sum_{a=1}^{\mathfrak{f}} \chi(ap) \int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times} \left(x - \frac{pa}{\mathfrak{f}} y\right)^{s-1} y^{k-s-1} d\mu_* \{\infty \to \frac{pa}{\mathfrak{f}}\}.$$

As alluded to in the first paragraph of this section, the function $L_p(\mathbf{h}_\infty, \chi; \kappa, s)$ satisfies the following interpolation property with respect to special values of the classical L-functions $L(f_k, \chi; s)$. For a proof, the reader is referred to [BD2].

Theorem 5.2. Suppose that $p \nmid \mathfrak{f}$, and that $1 \leq j \leq k-1$ satisfies $\chi(-1) = (-1)^{j-1}\mathfrak{g}(\mathfrak{c})$. Then, for $k \in U \cap \mathbb{Z}^{\geq 2}$, we have

$$L_p(\mathbf{h}_\infty, \chi, k, j) = \lambda(k)(1 - \chi(p)a_p(k)^{-1}p^{j-1})L^*(f_k, \chi, j). \tag{37}$$

Remark 5.3. Theorem 5.2 can also be rewritten in terms of the form $\hat{f}_k$ as

$$L_p(\mathbf{h}_\infty, \chi, k, j) = \lambda(k)(1 - \chi(p)a_p(k)^{-1}p^{j-1})(1 - \chi(p)a_p(k)^{-1}p^{k-j-1})L^*(\hat{f}_k, \chi, j).$$

Note in particular that, after specialising to $j = k/2$, one sees

$$L_p(\mathbf{h}_\infty, \chi, k, k/2) = \lambda(k)\left(1 - \chi(p)a_p(k)^{-1}p^{\frac{k}{2}-1}\right)^2 L^*(\hat{f}_k, \chi, k/2). \tag{38}$$

That the Euler factor appearing in this formula is a square will play a significant role in later applications.

6 Optimal Embeddings of K

We continue to assume that K is a real quadratic extension of $\mathbb{Q}$ with discriminant Δ. Recall the elliptic curve E of the Introduction all of the prime divisors of whose conductor are assumed to be split in K (the so-called *Heegner hypotheis*). This in particular implies that $\gcd(N, \Delta) = 1$ and that the discriminant Δ is a square modulo $4N$. We fix once and for all one of the square roots of Δ modulo N, and denote it by $\sqrt{\Delta} \pmod{N}$. Another consequence implied by our running assumption is the equality

$$\operatorname{sign}(E, K) = 1, \tag{39}$$

where $\mathrm{sign}(E, K)$ denotes the sign in the functional equation satisfied by the L-function $L(E, K; s)$ of E over K. See [GS], §3 or [BD0] for an explanation of this relation.

Definition 6.1. A $\mathbb{Q}$-algebra embedding $\Psi : K \longrightarrow \mathbf{M_0}(N)$ of K is called **optimal** of level N if

$$\Psi(K) \cap \mathbf{M_0}(N) = \Psi(\mathcal{O}_K),$$

where

$$\mathbf{M_0}(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \ : \ N \mid c \right\}.$$

That such embeddings exist is a consequence of Heegner hypothesis. In fact, one has the following lemma whose proof may be found for example in [BD0], p. 185.

Lemma 6.2. *An optimal embedding of K of level N exists if and only if the Heegner hypothesis holds, namely, if and only if all the prime divisors of N are split in K.*

We remark that if Ψ is an optimal embedding, then so is the conjugate embedding

$$\Psi^\gamma := \gamma\Psi\gamma^{-1} : K \longrightarrow \mathbf{M_0}(N), \quad \alpha \mapsto \gamma\Psi(\alpha)\gamma^{-1}, \tag{40}$$

for all $\gamma \in \mathbf{M_0}(N)^\times$. Indeed, the group $\mathbf{M_0}(N)^\times$ acts transitively on the set of such Ψ's and the set of equivalence classes of this action is in bijection with the ideal class group of K. Even, more is true.

Lemma 6.3. *Let h (resp. h^+) denote the class number (resp. narrow class number) of K. Then there are exactly h (resp. h^+) distinct optimal embeddings of K of level N, up to conjugation by $\mathbf{M_0}(N)^\times$ (resp. $\Gamma_0(N)$).*

Proof. See either of [P] or [BD0] or [D] for the details. □

Definition 6.4. Let Ψ be an optimal embedding of K of level N. Attached to Ψ is the binary quadratic form

$$Q_\Psi(X, Y) := cX^2 + (d - a)XY - bY^2, \tag{41}$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} := \Psi(\sqrt{\Delta})$. Since $\Delta > 0$, the equation $Q_\Psi(z, 1) = 0$ has two real roots τ and τ'. Indeed, these are the fixed points of the action of $\Psi(K^\times)$ on $\mathbb{P}_1(\mathbb{Q})$ by Möbius transformations. We now put

$$\mathbf{e} := \begin{pmatrix} \tau \\ 1 \end{pmatrix}, \quad \mathbf{e}' := \begin{pmatrix} \tau' \\ 1 \end{pmatrix}, \quad L_\Psi := \mathbb{Z}_p\mathbf{e} \oplus \mathbb{Z}_p\mathbf{e}'. \tag{42}$$

Remark 6.5. It will be important for later use to know the variations under conjugation of the quadratic forms $Q_\Psi(X,Y)$ and the $\mathbb{Z}_p$-lattices L_Ψ associated to optimal embeddings. Such relationships are readily verified to be given by

$$Q_{\gamma\Psi\gamma^{-1}}(X,Y) = (\det\gamma)\cdot(Q_\Psi|\gamma^{-1})(X,Y), \quad L_{\gamma\Psi\gamma^{-1}} = \gamma L_\Psi. \tag{43}$$

We should also notice that the $\mathbb{Z}_p$-lattice L_Ψ associated to Ψ is preserved by the action of $\Psi(K)$. One may order the two eigenvectors $\mathbf{e}$ and $\mathbf{e}'$ of this action in such a way that for any $\alpha \in K$,

$$\Psi(\alpha)\cdot\mathbf{e} = \alpha\mathbf{e}.$$

We end this section with another lemma whose statement will be of some use afterwards. Before doing so, however, one more definition is required.

Definition 6.6. Let L be a $\mathbb{Z}_p$-lattice in $\mathbb{Q}_p^2$. The generalised index of L, denoted by $|L|$, is defined as $p^{\mathrm{ord}_p\gamma}$, where γ is any element of $\mathbf{GL}_2(\mathbb{Q}_p)$ satisfying $\gamma(\mathbb{Z}_p^2) = L$.

One easily verifies that the generalised index of any lattice L is independent of the choice of γ. What is less trivial is the fact that the generalised index of the lattice L_Ψ is related to the quadratic form Q_Ψ. This relation is descried precisely in the last lemma of this section whose proof may be found in [BD2], §3.

Lemma 6.7. The function $\mathrm{ord}_p Q_\Psi$ is constant on $\mathbb{Z}_p^\times\mathbf{e}\times\mathbb{Z}_p^\times\mathbf{e}'$. More precisely,

$$\mathrm{ord}_p Q_\Psi(x,y) = \mathrm{ord}_p|L_\Psi| \qquad \text{on} \quad \mathbb{Z}_p^\times\mathbf{e}\times\mathbb{Z}_p^\times\mathbf{e}'. \tag{44}$$

7 Yet Another p-Adic L-Function Attached to E and K

As explained in the Introduction, the main goal of this paper is to show the existence of a p-adic analytic function interpolating a certain $\mathfrak{g}$-twisted sum of Shintani cycles whose second derivative, evaluated at $k=2$, is intimately related to global points on the elliptic curve E of Introduction. This section aims at the construction of such function. We attain the notation of the previous sections. In particular, we recall that ϵ_K denotes the fundamental unit of K of positive norm. Guided by the lattice functions in §2 and §3 of [BD2], we introduce the following lattice functions.

Definition 7.1. Let the symbol $\pounds$ (resp. $[\pounds,\pounds]$) stand for the set of all $\mathbb{Z}_p$-lattices L in $\mathbb{Q}_p^2$ (resp. all pairs (L_1,L_2) of $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^2$ where L_2 is contained in L_1 with index p.) The $\mathbf{V}_k(\mathbb{C}_p)$-valued modular symbols $c_k(L_1,L_2)$ and $\hat{c}_k(L)$ are respectively defined on $[\pounds,\pounds]$ and

$\pounds$ by the formulae

$$c_k(L_1, L_2)\{r \to s\}(P) \quad := \quad \int_{L_1' \cap L_2'} P d\mu_{L_2}\{r \to s\}, \tag{45}$$

$$\hat{c}_k(L)\{r \to s\}(P) \quad := \quad \int_{L'} P d\mu_{L}\{r \to s\}. \tag{46}$$

Using the invariant property (34) of Proposition 4.4, one immediately verifies that both c_k and $\hat{c}_k$ are $\sum$-invariant in the sense that for each $\gamma \in \sum$,

$$c_k(\gamma L_1, \gamma L_2)\{\gamma r \to \gamma s\}(P|\gamma^{-1}) \quad = \quad c_k(L_1, L_2)\{r \to s\}(P), \tag{47}$$

$$\hat{c}_k(\gamma L)\{\gamma r \to \gamma s\}(P|\gamma^{-1}) \quad = \quad \hat{c}_k(L)\{r \to s\}(P). \tag{48}$$

Another simple observation is that both c_k and $\hat{c}_k$ are homogeneous functions of degree p^{k-2}, namely,

$$c_k(pL_1, pL_2) = p^{k-2} c_k(L_1, L_2), \quad \hat{c}_k(pL) = p^{k-2}\hat{c}_k(L). \tag{49}$$

Lemma 7.2. (Main Identity) For any pair (L_1, L_2) in $[\pounds, \pounds]$, we have

$$\begin{aligned}(1 - a_p(k)^{-1}p^{k-2})c_k(L_1, L_2) \quad &= \quad \hat{c}_k(L_2) - a_p(k)^{-1}\hat{c}_k(pL_1) \\ &= \quad \hat{c}_k(L_2) - a_p(k)^{-1}p^{k-2}\hat{c}_k(L_1). \end{aligned}\tag{50}$$

Proof. Recall the standard lattice $L_* = \mathbb{Z}_p \oplus \mathbb{Z}_p$ of Section 4. Let us also introduce $L_\infty := \mathbb{Z}_p \oplus p\mathbb{Z}_p$, which is a sublattice of L_* with index p. It is a simple matter of computation to see that

$$\frac{1}{p}L_\infty' \cap L_*' = \mathbb{Z}_p \times \mathbb{Z}_p^\times, \qquad L_*' \cap L_\infty' = \mathbb{Z}_p^\times \times p\mathbb{Z}_p. \tag{51}$$

The usefulness of introducing these lattices arises from the fact that in the special case where

$$L_1 = \frac{1}{p}L_\infty, \quad \text{and} \quad L_2 = L_*,$$

the statement of the lemma is just a manifestation of the identity

$$\mathbf{I}_k\{r \to s\}(P) = \hat{\mathbf{I}}_k\{r \to s\}(P) - a_p(k)^{-1}\hat{\mathbf{I}}_k\{\theta^{-1}r \to \theta^{-1}s\}(P|\theta); \tag{52}$$

an identity which is implicit in the proof of Proposition 2.3 of [BD1]. Here θ is any element in the group $\sum$ of (33) satisfying[4]

$$\theta(\frac{1}{p}L_\infty) = L_*, \quad \theta(L_*) = L_\infty. \tag{53}$$

[4]Of which there are infinitely many.

The second remark to follow is that the group $\sum$ acts transitively on $[\pounds, \pounds]$ (cf. [BD2]). These two facts combined will yield the general case. To see this, given an arbitrary pair (L_1, L_2) in $[\pounds, \pounds]$, let us choose $\gamma \in \sum$ to satisfy

$$\gamma\left(\frac{1}{p}L_\infty\right) = L_1, \quad \gamma(L_*) = L_2. \tag{54}$$

Replacing $r,\ s$ and P respectively by $\gamma^{-1}r,\ \gamma^{-1}s$ and $P|\gamma$ in (52) and multiplying the factor $\lambda(k)(1 - a_p(k)^{-2}p^{k-2})$ to both sides of the resulting equality, we arrive at

$$\begin{aligned}
&\lambda(k)(1 - a_p(k)^{-2}p^{k-2})\mathbf{I}_k\{\gamma^{-1}r \to \gamma^{-1}s\}(P|\gamma) = \\
&\quad = \lambda(k)(1 - a_p(k)^{-2}p^{k-2})\hat{\mathbf{I}}_k\{\gamma^{-1}r \to \gamma^{-1}s\}(P|\gamma) \\
&\quad - a_p(k)^{-1}\lambda(k)(1 - a_p(k)^{-2}p^{k-2})\hat{\mathbf{I}}_k\{\theta^{-1}\gamma^{-1}r \to \theta^{-1}\gamma^{-1}s\}(P|\gamma\theta).
\end{aligned}$$

By applying (31) this can be rewritten, in light of (51), as

$$\begin{aligned}
&(1 - a_p(k)^{-2}p^{k-2}) \textstyle\int_{\frac{1}{p}L'_\infty \cap L'_*}(P|\gamma)d\mu_*\{\gamma^{-1}r \to \gamma^{-1}s\} = \\
&\quad = \int_{L'_*}(P|\gamma)d\mu_*\{\gamma^{-1}r \to \gamma^{-1}s\} \\
&\quad - a_p(k)^{-1}\int_{L'_*}(P|\gamma\theta)d\mu_*\{\theta^{-1}\gamma^{-1}r \to \theta^{-1}\gamma^{-1}s\} \\
&\quad = \int_{L'_*}(P|\gamma)d\mu_*\{\gamma^{-1}r \to \gamma^{-1}s\} \\
&\quad - a_p(k)^{-1}\int_{L'_\infty}(P|\gamma)d\mu_{L_\infty}\{\gamma^{-1}r \to \gamma^{-1}s\},
\end{aligned}$$

where the last equality follows from the invariant property of (34) under θ. This last equality can be rewritten in terms of the lattice functions c_k and $\hat{c}_k$ as

$$\begin{aligned}
(1 - a_p(k)^{-2}p^{k-2})c_k(\frac{1}{p}L_\infty, L_*)\{\gamma^{-1}r \to \gamma^{-1}s\}(P|\gamma) &= \hat{c}_k(L_*)\{\gamma^{-1}r \to \gamma^{-1}s\}(P|\gamma) \\
&- a_p(k)^{-1}\hat{c}_k(L_\infty)\{\gamma^{-1}r \to \gamma^{-1}s\}(P|\gamma).
\end{aligned}$$

Applying the invariant properties of c_k and $\hat{c}_k$ of relations (47) and (48) under γ shall now finish the proof. □

Definition 7.3. Let $[\Psi]$ be a class (under cojugation relation and represented by Ψ) of optimal embeddings of K of level N and put $\gamma_{_\Psi} := \Psi(\epsilon_{_K})$. Also choose an arbitrary base point $z_0 \in \mathbb{P}_1(\mathbb{Q})$ on the extended upper half-plane. To this data we associate

$$\begin{aligned}
\mathcal{L}_p(\Psi, \kappa) &:= \int_{\mathbb{Z}_p^\times \mathbf{e} \times \mathbb{Z}_p^\times \mathbf{e}'} \langle Q_{_\Psi}(x,y)\rangle^{\frac{\kappa-2}{2}} d\mu_{_\Psi}\{z_0 \to \gamma_{_\Psi} z_0\} \\
&= |L_\Psi|^{-\frac{k-2}{2}} \int_{\mathbb{Z}_p^\times \mathbf{e} \times \mathbb{Z}_p^\times \mathbf{e}'} Q_{_\Psi}(x,y)^{\frac{\kappa-2}{2}} d\mu_{_\Psi}\{z_0 \to z_{_\Psi}\},
\end{aligned} \tag{55}$$

where, in order to ease the notation, we have written $\mu_{_\Psi}$ (resp. $z_{_\Psi}$) in place of the measure associated to L_Ψ (resp. in place of $\gamma_{_\Psi} z_0$).

Remark 7.4. For one thing, note that the second equality in Definition 7.3 follows from the relation (44) of Lemma 6.7. For another thing, one sees easily that the very same lemma together with the relations (43) imply that the integral appearing in the definition of $\mathcal{L}_p(\Psi,\kappa)$ is unchanged if Ψ is replaced by $\gamma\Psi\gamma^{-1}$. Finally, that the definition of $\mathcal{L}_p(\Psi,\kappa)$ is also independent of the choice of the base point z_0 follows from the following general lemma.

Lemma 7.5. Let L be a $\mathbb{Z}_p$-lattice in $\mathbb{Q}_p^2$, let F be a homogeneous function of degree $k-2$, and let X be a compact-open set in $\mathcal{W}$. Now let $\gamma \in \sum$ preserves L, F and X, i.e.,

$$\gamma L = L, \quad \gamma X = X, \quad F|\gamma = F.$$

Then for any $r,\ s \in \mathbb{P}_1(\mathbb{Q})$, we have

$$\int_X F d\mu_L\{r \to \sigma r\} = \int_X F d\mu_L\{s \to \sigma s\}. \tag{56}$$

Proof. According to the modular symbol property, we have

$$\begin{aligned}
\int_X F d\mu_L\{r \to s\} \quad + &\quad \int_X F d\mu_L\{s \to \gamma s\} = \\
= &\quad \int_X F d\mu_L\{r \to \gamma s\} \\
= &\quad \int_X F d\mu_L\{r \to \gamma r\} + \int_X F d\mu_L\{\gamma r \to \gamma s\} \\
= &\quad \int_X F d\mu_L\{r \to \gamma r\} + \int_{\gamma^{-1}X} (F|\gamma) d\mu_{\gamma^{-1}L}\{r \to s\} \\
= &\quad \int_X F d\mu_L\{r \to \gamma r\} + \int_X F d\mu_L\{r \to s\},
\end{aligned}$$

where the penultimate equality follows form (34), whereas the last equality follows from the trivial action of γ on L, X and F. A simple cancelation now completes the proof. $\square$

Our next objective is to prove a formula expressing $\mathcal{L}_p(\Psi,k)$ in terms of the lattice function $\hat{c}_k$. Before doing so, however, let us first introduce some useful natation which will lighten the exposition. We fix once and for all a prime ideal $\mathfrak{p}$ of K lying above p and will write $\sigma_\mathfrak{p}$ for the Frobenius element associated to $\mathfrak{p}$. As explained on page 416 of [BD2] in details, one has the following relations

$$\sigma_\mathfrak{p}^j L_\Psi = \sigma_\mathfrak{p}^j(\mathbb{Z}_p\mathbf{e} \oplus \mathbb{Z}_p\mathbf{e}') = p^j\mathbb{Z}_p\mathbf{e} \oplus \mathbb{Z}_p\mathbf{e}', \quad \text{for all } j \in \mathbb{Z}.$$

Therefore, for each j, $\sigma_\mathfrak{p}^j L_{_\Psi}$ contains (resp. is contained in) $\sigma_\mathfrak{p}^{j+1} L_{_\Psi}$ (resp. $\sigma_\mathfrak{p}^{j-1} L_{_\Psi}$) with index p. For any $j \in \mathbb{Z}$ and any $k \in U \cap \mathbb{Z}^{\geq 2}$, we set

$$\Gamma_k^{(j)}[\Psi] := |\sigma_\mathfrak{p}^j L_{_\Psi}|^{-\frac{k-2}{2}} \hat{c}_k(\sigma_\mathfrak{p}^j L_{_\Psi})\{z_0 \to z_{_\Psi}\}(Q_{_\Psi}^{\frac{k-2}{2}}).$$

Whenever convenient, we remove Ψ from $\Gamma_k^{(j)}[\Psi]$ and simply write $\Gamma_k^{(j)}$, if this results in no ambegiuty.

Remark 7.6. If the lattice L_Ψ happens to be L_*, then one computes

$$\begin{aligned}
\Gamma_k^{(j)} &= |\sigma_{\mathfrak{p}}^j L_*|^{-\frac{k-2}{2}} \hat{c}_k(\sigma_{\mathfrak{p}}^j L_*)\{z_0 \to \Psi(\epsilon_K)z_0\}\left(Q_\Psi^{\frac{k-2}{2}}\right) \\
&= (\det \sigma_{\mathfrak{p}}^{-j})^{\frac{k-2}{2}} \int_{\sigma_{\mathfrak{p}}^j L_*} Q_\Psi^{\frac{k-2}{2}} d\mu_{\sigma_{\mathfrak{p}}^j L_*}\{z_0 \to \Psi(\epsilon_K)z_0\} \\
&= \int_{L_*} \left(Q_\Psi|\sigma_{\mathfrak{p}}^j\right)^{\frac{k-2}{2}} d\mu_*\{z_0 \to \Psi^{\sigma_{\mathfrak{p}}^j}(\epsilon_K)z_0\} \\
&= \lambda(k)(1-a_p(k)^{-2}p^{k-2})\hat{\mathbf{I}}_k\{z_0 \to \Psi^{\sigma_{\mathfrak{p}}^j}(\epsilon_K)z_0\}\left(Q_{\Psi^{\sigma_{\mathfrak{p}}^j}}(z,1)^{\frac{k-2}{2}}\right). \qquad (57)
\end{aligned}$$

Before stating the next lemma we remark that if t denotes the order of $\sigma_{\mathfrak{p}}$ in the group $\mathcal{C}_K^+$, since $\sigma_{\mathfrak{p}}^t$ is trivial, $\Gamma^{(j)}$, as a function of $j \in \mathbb{Z}$, is t-periodic, i.e., for all $k \in U \cap \mathbb{Z}^{\geq 2}$, we have

$$\Gamma_k^{(j+t)} = \Gamma_k^{(j)}. \qquad (58)$$

We now assert that

Lemma 7.7. For any integer $k \geq 2$ in U, we have

$$\mathcal{L}_p(\Psi,k) = \frac{1}{1-a_p(k)^{-2}p^{k-2}}\Big[(1+a_p(k)^{-2}p^{k-2})\Gamma_k^{(0)} - a_p(k)^{-1}p^{\frac{k-2}{2}}(\Gamma_k^{(-1)}+\Gamma_k^{(1)})\Big]. \qquad (59)$$

Proof. We should first remark that since the p-th Fourier coefficient $a_p(k)$ of the eigenform f_k is a p-adic unit (cf. Remark 3.1), the denominator of the fraction above never vanishes. We now proceed the proof. It is fairly easy to see that the domain of integration in the Definition 7.3 can be expressed as

$$\mathbb{Z}_p^\times \mathbf{e} \times \mathbb{Z}_p^\times \mathbf{e}' = \left(\sigma_{\mathfrak{p}}^{-1} L'_\Psi \cap L'_\Psi\right) - \left(L'_\Psi \cap \sigma_{\mathfrak{p}} L'_\Psi\right).$$

Hence,

$$\begin{aligned}
\mathcal{L}_p(\Psi,k) &= |L_\Psi|^{-\frac{k-2}{2}} \int_{\mathbb{Z}_p^\times e_1 \times \mathbb{Z}_p^\times e_2} Q_\Psi^{\frac{k-2}{2}} d\mu_{L_\Psi}\{z_0 \to z_\Psi\} \\
&= |L_\Psi|^{-\frac{k-2}{2}} \left(\int_{\sigma_{\mathfrak{p}}^{-1} L'_\Psi \cap L'_\Psi} Q_\Psi^{\frac{k-2}{2}} d\mu_{L_\Psi}\{z_0 \to z_\Psi\}\right. \\
&\left. - \int_{L'_\Psi \cap \sigma_{\mathfrak{p}} L'_\Psi} Q_\Psi^{\frac{k-2}{2}} d\mu_{L_\Psi}\{z_0 \to z_\Psi\}\right).
\end{aligned}$$

Now we use the lattice functions c_k and $\hat{c}_k$ to rewrite the above equality as

$$\begin{aligned}
\mathcal{L}_p(\Psi,k) &= |L_{\Psi}|^{-\frac{k-2}{2}}\Big[c_k(\sigma_{\mathfrak{p}}^{-1}L_\Psi, L_\Psi)\{z_0 \to z_{\Psi}\}(Q_\Psi^{\frac{k-2}{2}}) \\
&- a_p(k)^{-1}c_k(L_\Psi, \sigma_{\mathfrak{p}}L_\Psi)\{z_0 \to z_{\Psi}\}(Q_\Psi^{\frac{k-2}{2}})\Big] \\
&= \frac{|L_\Psi|^{-\frac{k-2}{2}}}{1-a_p(k)^{-2}p^{k-2}}\Bigg[\Big(\hat{c}_k(L_\Psi) - a_p(k)^{-1}p^{k-2}\hat{c}_k(\sigma_{\mathfrak{p}}^{-1}L_\Psi)\Big)\{z_0 \to z_{\Psi}\}(Q_\Psi^{\frac{k-2}{2}}) \\
&- a_p(k)^{-1}\Big(\hat{c}_k(\sigma_{\mathfrak{p}}L_\Psi) - a_p(k)^{-1}p^{k-2}\hat{c}_k(L_\Psi)\Big)\{z_0 \to z_{\Psi}\}(Q_\Psi^{\frac{k-2}{2}})\Bigg] \\
&= \frac{|L_\Psi|^{-\frac{k-2}{2}}}{1-a_p(k)^{-2}p^{k-2}}\Bigg[(1+a_p(k)^{-2}p^{k-2})\hat{c}_k(L_\Psi) \\
&- a_p(k)^{-1}p^{\frac{k-2}{2}}\Big(p^{\frac{k-2}{2}}\hat{c}_k(\sigma_{\mathfrak{p}}^{-1}L_\Psi) + p^{-\frac{k-2}{2}}\hat{c}_k(\sigma_{\mathfrak{p}}L_\Psi)\Big)\Bigg]\{z_0 \to z_{\Psi}\}(Q_\Psi^{\frac{k-2}{2}}).
\end{aligned}$$

Finally once we observe that

$$|\sigma_{\mathfrak{p}}^{j}L_\Psi| = p^j|L_\Psi|, \qquad \text{for all } j \in \mathbb{Z},$$

we may rewrite $\mathcal{L}_p(\Psi,k)$ in terms of $\Gamma_k^{(j)}$'s as

$$\mathcal{L}_p(\Psi,k) = \frac{1}{1-a_p(k)^{-2}p^{k-2}}\Big[(1+a_p(k)^{-2}p^{k-2})\Gamma_k^{(0)} - a_p(k)^{-1}p^{\frac{k-2}{2}}(\Gamma_k^{(-1)} + \Gamma_k^{(1)})\Big].$$

The proof is complete. ☐

The next proposition will pave the way for a proof of the interpolation formula of Proposition 7.11 yielding part *(i)* of the Main Theorem.

Proposition 7.8. For any $j \in \mathbb{Z}$, write Ψ_j for the action of the j-th power of the Frobenius element $\sigma_{\mathfrak{p}}$ on Ψ. Then, for all $k \in \mathbb{Z}^{\geq 2} \cap U$, we have[5]

$$\begin{aligned}
\sum_{j=0}^{t-1}\mathfrak{g}(\sigma_{\mathfrak{p}}^{j})\mathcal{L}_p(\Psi_j,k) &= \frac{\Big(1-\chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\Big)^2}{1-a_p(k)^{-2}p^{k-2}}\sum_{j=0}^{t-1}\chi_1(p)^j\Gamma_k^{(j)} \\
&= \frac{1-\chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}}{1+\chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}}\sum_{j=0}^{t-1}\chi_1(p)^j\Gamma_k^{(j)}, \qquad (60)
\end{aligned}$$

where as before t is the order of $\sigma_{\mathfrak{p}}$ in the group $\mathrm{Gal}(H_K^+/K)$.

[5]In this proposition, Γ_k^j is still a shorthand for $\Gamma_k^j[\Psi]$.

Remark 7.9. The second equality above is a simple consequence of the fact that since χ_1 is a quadratic character, $\chi_1(p)^2 = 1$, and hence

$$1 - a_p(k)^{-2}p^{k-2} = \left(1 - \chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\right)\left(1 + \chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\right).$$

Proof of the Proposition 7.8 Since p splits completely in K as $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, as one of the instances of (1), we have

$$\mathfrak{g}(\sigma_{\mathfrak{p}}) = \chi_1(p).$$

Also as noted earlier, $\Gamma_k^{(j)} = \Gamma_k^{(j+t)}$. These two facts combined with Lemma 7.7 then allow us to write the left hand-side as

$$\begin{aligned}
\sum_{j=0}^{t-1} \mathfrak{g}(\sigma_{\mathfrak{p}}^j)\mathcal{L}_p(\Psi_j, k) &= \frac{1}{1 - a_p(k)^{-2}p^{k-2}}\Bigg[(1 + a_p(k)^{-2}p^{k-2})\sum_{j=0}^{t-1}\chi_1(p)^j\Gamma_k^{(j)} \\
&- a_p(k)^{-1}p^{\frac{k-2}{2}}\sum_{j=0}^{t-1}\chi_1(p)^j\left(\Gamma_k^{(j-1)} + \Gamma_k^{(j+1)}\right)\Bigg] \\
&= \frac{1}{1 - a_p(k)^{-2}p^{k-2}}\Bigg[(1 + a_p(k)^{-2}p^{k-2})\sum_{j=0}^{t-1}\chi_1(p)^j\Gamma_k^{(j)} \\
&- \chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\left(\sum_{j=0}^{t-1}\chi_1(p)^{j-1}\Gamma_k^{(j-1)} + \sum_{j=0}^{t-1}\chi_1(p)^{j-1}\Gamma_k^{(j+1)}\right)\Bigg].
\end{aligned}$$

Now we note that $\chi_1(p)^2 = 1$, and that $\chi_1(p)^t = \mathfrak{g}(\sigma_{\mathfrak{p}})^t = \mathfrak{g}(\sigma_{\mathfrak{p}}^t) = 1$. Therefore we may write

$$\sum_{j=0}^{t-1}\chi_1(p)^{j-1}\Gamma_k^{(j-1)} = \sum_{j=0}^{t-1}\chi_1(p)^j\Gamma_k^{(j)},$$

and

$$\sum_{j=0}^{t-1}\chi_1(p)^{j-1}\Gamma_k^{(j+1)} = \sum_{j=0}^{t-1}\chi_1(p)^{j+1}\Gamma_k^{(j+1)} = \sum_{j=0}^{t-1}\chi_1(p)^j\Gamma_k^{(j)}.$$

Putting all this together yields

$$\begin{aligned}
\sum_{j=0}^{t-1} \mathfrak{g}(\sigma_{\mathfrak{p}}^j)\mathcal{L}_p(\Psi_j, k) &= \frac{1}{1 - a_p(k)^{-2}p^{k-2}}\Bigg[(1 + a_p(k)^{-2}p^{k-2})\sum_{j=0}^{t-1}\chi_1(p)^j\Gamma_k^{(j)} \\
&- \chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\left(\sum_{j=0}^{t-1}\chi_1(p)^j\Gamma_k^{(j)} + \sum_{j=0}^{t-1}\chi_1(p)^j\Gamma_k^{(j)}\right)\Bigg] \\
&= \frac{\left(1 + a_p(k)^{-2}p^{k-2} - 2\chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\right)}{1 - a_p(k)^{-2}p^{k-2}}\sum_{j=0}^{t-1}\chi_1(p)^j\Gamma_k^{(j)} \\
&= \frac{\left(1 - \chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\right)^2}{1 - a_p(k)^{-2}p^{k-2}}\sum_{j=0}^{t-1}\chi_1(p)^j\Gamma_k^{(j)}.
\end{aligned}$$

This completes the proof. $\square$

We are now ready to define the p-adic analytic function $\mathcal{L}_p(E, K, \mathfrak{g}; \kappa)$ alluded to in Introduction.

Definition 7.10. Fix once and for all an optimal embedding Ψ, and without loss of generality, assume that its associated lattice is the standard lattice L_* of (27). To the data consisting of the elliptic curve E, the real quadratic K and the genus character $\mathfrak{g}$ we attach the p-adic analytic function $\mathcal{L}_p(E, K, \mathfrak{g}; \kappa)$ of the variable $\kappa \in U$ defined by

$$\mathcal{L}_p(E, K, \mathfrak{g}; \kappa) := \sum_{\sigma \in \mathcal{C}_K^+} \mathfrak{g}(\sigma) \mathcal{L}_p(\Psi^\sigma, \kappa), \tag{61}$$

where as before $\mathcal{C}_K^+$ is the narrow ideal class group of K. Let us also set

$$L_p(E, K, \mathfrak{g}; \kappa) := \mathcal{L}_p(E, K, \mathfrak{g}; \kappa)^2. \tag{62}$$

As reflected in the terminology, $\mathcal{L}_p(E, K, \mathfrak{g}; \kappa)$ enjoys the following interpolation property.

Proposition 7.11. (Interpolation Formula) For every $k \in \mathbb{Z}^{\geq 2} \cap U$, we have

$$\begin{aligned} \mathcal{L}_p(E, K, \mathfrak{g}; k) &= \lambda(k) \left(1 - \chi_{\scriptscriptstyle 1}(p) a_p(k)^{-1} p^{\frac{k-2}{2}}\right)^2 \\ &\times \left(\sum_{\sigma \in \mathcal{C}_K^+} \mathfrak{g}(\sigma) \mathbf{C}(\hat{f}_k, \Psi^\sigma(\epsilon_{\scriptscriptstyle K})) \right) \\ &= \lambda(k) \left(1 - \chi_{\scriptscriptstyle 1}(p) a_p(k)^{-1} p^{\frac{k-2}{2}}\right)^2 \\ &\times \left(\sum_{\sigma \in \mathcal{C}_K^+} \mathfrak{g}(\sigma) \frac{1}{\Omega_k} \int_{z_0}^{\Psi^\sigma(\epsilon_{\scriptscriptstyle K}) z_0} \hat{f}_k(z) Q_{\Psi^\sigma}(z, 1)^{\frac{k-2}{2}} dz \right). \end{aligned}$$

Proof. Let $\mathcal{R}$ denote a set of representatives for the quotient group $\mathcal{C}_K^+ / \langle \sigma_{\mathfrak{p}} \rangle$. Therefore, any element of $\mathcal{C}_K^+$ has a unique representation of the form $\delta \sigma_{\mathfrak{p}}^j$, as δ runs through $\mathcal{R}$ and $0 \leq j \leq t-1$. Equivalently, for any $\delta \in \mathcal{R}$, if we write Ψ_j^δ for the optimal embedding obtained from acting the j-th power of $\sigma_{\mathfrak{p}}$ on Ψ^δ, then every equivalence class of optimal embeddings of K can be uniquely written as $[\Psi_j^\delta]$, where $0 \leq j \leq t-1$, and $\delta \in \mathcal{R}$. Therefore, we have

$$
\begin{aligned}
\mathcal{L}_p(E,K,\mathfrak{g};\kappa) &= \sum_{\sigma\in\mathcal{C}_K^+}\mathfrak{g}(\sigma)\mathcal{L}_p(\Psi^\sigma,\kappa)\\
&= \sum_{\delta\in\mathcal{R}}\mathfrak{g}(\delta)\sum_{j=0}^{t-1}\mathcal{L}_p(\Psi_j^\delta,k)\\
&= \frac{1-\chi_{_1}(p)a_p(k)^{-1}p^{\frac{k-2}{2}}}{1+\chi_{_1}(p)a_p(k)^{-1}p^{\frac{k-2}{2}}}\sum_{\delta\in\mathcal{R}}\mathfrak{g}(\delta)\sum_{j=0}^{t-1}\chi_{_1}(p)^j\Gamma_k^{(j)}[\Psi^\delta].
\end{aligned}
$$

The last remark to follow is that, without loss of generality, we may assume that the $\mathbb{Z}_p$-lattice associated to the optimal embedding Ψ^δ is the standard lattice L_*. With this convention, and by invoking Remark 7.6, we deduce that

$$
\begin{aligned}
\mathcal{L}_p(E,K,\mathfrak{g};\kappa) &= \frac{1-\chi_{_1}(p)a_p(k)^{-1}p^{\frac{k-2}{2}}}{1+\chi_{_1}(p)a_p(k)^{-1}p^{\frac{k-2}{2}}}\sum_{\delta\in\mathcal{R}}\mathfrak{g}(\delta)\sum_{j=0}^{t-1}\chi_{_1}(p)^j\Gamma_k^{(j)}[\Psi^\delta]\\
&= \frac{1-\chi_{_1}(p)a_p(k)^{-1}p^{\frac{k-2}{2}}}{1+\chi_{_1}(p)a_p(k)^{-1}p^{\frac{k-2}{2}}}\lambda(k)(1-a_p(k)^{-2}p^{k-2})\times\\
&\times\sum_{\delta\in\mathcal{R}}\mathfrak{g}(\delta)\left(\sum_{j=0}^{t-1}\chi_{_1}(p)^j\hat{\mathbf{I}}_k\{z_0\to\Psi^{\delta\sigma_{\mathfrak{p}}^j}(\epsilon_{_K})z_0\}\left(Q_{\Psi^{\delta\sigma_{\mathfrak{p}}^j}}(z,1)^{\frac{k-2}{2}}\right)\right).\\
&= \lambda(k)(1-\chi_{_1}(p)a_p(k)^{-1}p^{\frac{k-2}{2}})^2\times\\
&\times\sum_{\sigma\in\mathcal{C}_K^+}\mathfrak{g}(\sigma)\hat{\mathbf{I}}_k\{z_0\to\Psi^\sigma(\epsilon_{_K})z_0\}\left(Q_{\Psi^\sigma}(z,1)^{\frac{k-2}{2}}\right).
\end{aligned}
$$

But this last equality is equivalent to the statement of the proposition, and we are done. $\square$

The next proposition justifies the designation of the term "p-adic L-function", since it will give an interpolation formula for the central critical values of the complex L-functions $L(\hat{f}_k/K,\mathfrak{g};s)$. However, it is not $\mathcal{L}_p(E,K,\mathfrak{g};\kappa)$, but rather its square, which make an appearance in the interpolation formula. The same phenomenon will be observed in the Factorisation Formula of Proposition 7.14. We cannot say much about the factorisation of $\mathcal{L}_p(E,K,\mathfrak{g};\kappa)$, yet we will be able to decompose its square into the product of two restricted Mazur-Kitagawa L-function.

Proposition 7.12. For any $k\in U\cap\mathbb{Z}^{\geq 2}$, we have

$$
L_p(E,K,\mathfrak{g};k)=\lambda(k)^2\left(1-\chi_{_1}(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\right)^4\frac{\Delta^{\frac{k-1}{2}}(\frac{k}{2}!-1)^2}{(2\pi i)^{k-2}\Omega_k^2}L(\hat{f}_k/K,\mathfrak{g};k/2). \tag{63}
$$

Proof. The result is a direct consequence of the last proposition together with the following crucial identity

$$\left(\sum_{\sigma\in\mathcal{C}_K^+}\mathfrak{g}(\sigma)\int_{z_0}^{\Psi^\sigma(\epsilon_K)z_0}\hat{f}_k(z)Q_{\Psi^\sigma}(z,1)^{\frac{k-2}{2}}dz\right)^2=\frac{\Delta^{\frac{k-1}{2}}(\frac{k}{2}-1)!^2}{(2\pi i)^k}L(\hat{f}_k/K,\mathfrak{g};k/2).$$

For a proof of this formula the reader is referred to the page 862 of [P]. □

Remark 7.13. By setting

$$L^*(\hat{f}_k/K,\mathfrak{g};k/2):=\frac{\sqrt{\Delta}(\frac{k}{2}-1)!^2}{(2\pi i)^{k-2}\Omega_k^2}L(\hat{f}_k/K,\mathfrak{g};k/2),$$

the statement of the proposition above can be rewritten as

$$\begin{aligned} L_p(E,K,\mathfrak{g};k) &= \lambda(k)^2\left(1-\chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\right)^4\Delta^{\frac{k-2}{2}}L^*(\hat{f}_k/K,\mathfrak{g};k/2)\\ &= \lambda(k)^2\left(1-\chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\right)^2\Delta^{\frac{k-2}{2}}L^*(f_k/K,\mathfrak{g};k/2) \qquad (64)\end{aligned}$$

valid for all $k\in\mathbb{Z}^{\geq 2}\cap U$. Notice that the second equality follows from (24), (25) and (26).

Finally, a crucial ingredient used in the proof of the Main Theorem is the following formula which furnishes a factorization for $L_p(E,K,\mathfrak{g};\kappa)$ in terms of restrictions to the central critical line $\kappa=2s$ of two Mazur-Kitagawa p-adic L-functions.

Proposition 7.14. For all $\kappa\in U$,

$$L_p(E,K,\mathfrak{g};\kappa)=\Delta^{\frac{\kappa-2}{2}}L_p(\mathbf{h}_\infty,\chi_1;\kappa,\kappa/2)L_p(\mathbf{h}_\infty,\chi_2;\kappa,\kappa/2).$$

Proof. Since the two sides are continuous functions of $\kappa\in U$, and since $U\cap\mathbb{Z}^{\geq 2}$ is dense in U, it will suffice to prove the statement for $k\in U\cap\mathbb{Z}^{\geq 2}$. Having made such observation, just by comparing relations (18) and (26) with $\hat{f}_k$ in place, in light of (25), we deduce that

$$L^*(\hat{f}_k/K,\mathfrak{g};k/2)=L^*(\hat{f}_k,\chi_1;k/2)L^*(\hat{f}_k,\chi_2;k/2). \qquad (65)$$

On the other hand, the formula (38) with $\chi=\chi_1$ and $\chi=\chi_2$ respectively reads

$$L_p(\mathbf{h}_\infty,\chi_1;k,k/2)=\lambda(k)\left(1-\chi_1(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\right)^2L^*(\hat{f}_k,\chi_1;k/2), \qquad (66)$$

and

$$L_p(\mathbf{h}_\infty,\chi_2;k,k/2)=\lambda(k)\left(1-\chi_2(p)a_p(k)^{-1}p^{\frac{k-2}{2}}\right)^2L^*(\hat{f}_k,\chi_2;k/2). \qquad (67)$$

Since p is assumed to be split in K, we have $\chi_K(p)=1$. This in turn implies that $\chi_1(p)=\chi_2(p)$. The desired result is now an immediate consequence of (64), (65), (66) and (67). □

8 Proof of the Main Theorem

We have gathered all the necessary materials needed to prove the main result of this article. Before we proceed with the proof and just for convenience, however, let us first recall its statement.

Theorem 8.1. *(i) The mapping which to any $k \in U \cap \mathbb{Z}^{\geq 2}$ assigns $\sum_{\sigma \in \mathcal{C}_K^+} \mathfrak{g}(\sigma)\mathbf{C}(\hat{f}_k, \Psi^\sigma(\epsilon_K))$ extends, in a suitable way, to a p-adic analytic function $\mathcal{L}_p(E, K, \mathfrak{g}; \kappa)$ on U.*

(ii) Suppose further that E has at least two primes of multiplicative reduction, that $\chi_1(-N) = w_N$ and that $\chi_1(p) = a_p$. Then:

(a) $\mathcal{L}_p(E, K, \mathfrak{g}; \kappa)$ vanishes to order at least two at $k = 2$;

(b) There exist global points $P_{\chi_1} \in (E(\mathbb{Q}(\sqrt{\mathfrak{d}_1})) \otimes \mathbb{Q})^{\chi_1}$ and $P_{\chi_2} \in (E(\mathbb{Q}(\sqrt{\mathfrak{d}_2})) \otimes \mathbb{Q})^{\chi_2}$ and a rational number $t \in \mathbb{Q}^\times$ such that

$$\frac{d^2}{d\kappa^2}\mathcal{L}_p(E, K, \mathfrak{g}; \kappa)\Big|_{k=2} = t \log_E(P_{\chi_1}) \log_E(P_{\chi_2});$$

(c) The two points P_{χ_1} and P_{χ_2} are both of infinite order if and only if

$$L''(E/K, \mathfrak{g}; 1) \neq 0.$$

Remark 8.2. For a semistable elliptic curve E, the technical condition of an extra prime of multiplicative reduction is automatically satisfied if the sign in the functional equation satisfied by the L-function $L(E, s)$ is minus one. For, such curve must have an even number of primes of multiplicative reduction.

Proof. *(i)* This part is merely the content of Proposition 7.11.

(ii) (a) We first remark that since all the prime divisors of N are split in K and since K is a real quadratic field,

$$\chi_K(-N) = \chi_K(p) = 1.$$

We also recall that $\chi_1 \cdot \chi_2 = \chi_K$. It follows from this and from the running assumptions $\chi_1(-N) = w_N$ and $\chi_1(p) = a_p$ that

$$\chi_1(-N) = \chi_2(-N) = w_N, \quad \chi_1(p) = \chi_2(p) = a_p.$$

So, the characters χ_1 and χ_2 both satisfy the two conditions of Theorem 5.4 of [BD2]. Hence, the L-functions

$$L_p(E, \chi_1; s) \quad \text{and} \quad L_p(E, \chi_2; s)$$

have each an exceptional zero at $s = 1$, and therefore the two restricted to the line $s = \kappa/2$ Mazur-Kitagawa p-adic L-functions

$$L_p(\mathbf{h}_\infty, \chi_1; \kappa, \kappa/2) \quad \text{and} \quad L_p(\mathbf{h}_\infty, \chi_2; \kappa, \kappa/2)$$

vanish to order at least two at $k = 2$. It follows from the factorisation formula of Proposition 7.14 that the function $L_p(E, K, \mathfrak{g}; \kappa)$ vanishes to order at least four at $k = 2$. On account of (62), part *(a)* follows.

(ii) (b) Part 2 of Theorem 5.4 of [BD2] also guarantees the existence of two global points

$$P_{\chi_1} \in (E(\mathbb{Q}(\sqrt{\mathfrak{d}_1})) \otimes \mathbb{Q})^{\chi_1}$$

and

$$P_{\chi_2} \in (E(\mathbb{Q}(\sqrt{\mathfrak{d}_2})) \otimes \mathbb{Q})^{\chi_2}$$

and two rational numbers $l_1, l_2 \in \mathbb{Q}^\times$ satisfying

$$\frac{d^2}{d\kappa^2} L_p(\mathbf{h}_\infty, \chi_1; \kappa, \kappa/2)\Big|_{k=2} = l_1 \log_E^2(P_{\chi_1}),$$

and

$$\frac{d^2}{d\kappa^2} L_p(\mathbf{h}_\infty, \chi_2; \kappa, \kappa/2)\Big|_{k=2} = l_2 \log_E^2(P_{\chi_2}).$$

On the other hand, as we just saw, $L_p(E, K, \mathfrak{g}; \kappa)$ vanishes to order at least four at $k = 2$, or what amounts to the same thing, $\mathcal{L}_p(E, K, \mathfrak{g}; \kappa)$ vanishes to order at least two at $k = 2$. It follows from this and the vanishing properties of the two Mazura-Kitagawa p-adic L-functions at $k = 2$ mentioned to above that

$$\begin{aligned}
\left(\frac{d^2}{d\kappa^2} \mathcal{L}_p(E, K, \mathfrak{g}; \kappa)\Big|_{k=2}\right)^2 &= \frac{1}{6} \frac{d^4}{d\kappa^4} L_p(E, K, \mathfrak{g}; \kappa)\Big|_{k=2} \\
&= \left(\frac{d^2}{d\kappa^2} L_p(\mathbf{h}_\infty, \chi_1; \kappa, \kappa/2)\Big|_{k=2}\right) \left(\frac{d^2}{d\kappa^2} L_p(\mathbf{h}_\infty, \chi_2; \kappa, \kappa/2)\Big|_{k=2}\right) \\
&= l_1 l_2 \log_E^2(P_{\chi_1}) \log_E^2(P_{\chi_2}). \qquad (68)
\end{aligned}$$

Next we remark that according to part 4 of Theorem 5.4 of [BD2],

$$l_1 \equiv^\times l_2 \equiv^\times L^*(\phi, \psi;\ 1) \pmod{(\mathbb{Q}^\times)^2}, \qquad (69)$$

where ψ can be any quadratic Dirichlet character satisfying

- $\psi(l) = 1$ for all l dividing N/p;
- $\psi(p) = -1$;
- $L(f, \psi; 1) \neq 0$.

It is readily seen from (69) that $l_1 l_2 \in (\mathbb{Q}^\times)^2$. Combining this fact with (68) establishes the proof of *(b)*.

(ii) (c) The conditions satisfied by the character χ_j $(j = 1, 2)$ imply that the sign in the functional equation satisfied by $L(E, \chi_j, s)$ is minus one (see the last paragraph in the Subsection 5.1), and therefore we have

$$L(E, \chi_1; 1) = 0 \qquad \text{and} \qquad L(E, \chi_2; 1) = 0.$$

On the other hand, by invoking Theorem 5.4 of [BD2] one more time we see that the point P_{χ_j} $(j = 1, 2)$ is of infinite order if and only if

$$L'(E, \chi_j; 1) \neq 0.$$

However, these last two non-vanishing conditions, in light of the relation

$$L(E/K, \mathfrak{g}; s) = L(E, \chi_1; s) L(E, \chi_2; s),$$

(compare also to (25)) are equivalent to

$$L''(E/K, \mathfrak{g}; 1) \neq 0.$$

This completes the proof. $\square$

References

[BD0] M. Bertolini, and H. Darmon, *A Birch and Swinnerton-Dyer conjecture for the Mazur-Tate circle pairing.* Duke Math Journal (2004) **122** no. 1, 181-204.

[BD1] M. Bertolini, and H. Darmon, *The rationality of Stark-Heegner points over the genus fields of real quadratic fields*, Annals of Mathematics, to appear.

[BD2] M. Bertolini, and H. Darmon, *Hida families and rational points on elliptic curves*, Submitted.

[BDI] M. Bertolini, H. Darmon and A. Iovita, *Families of automorphic forms on definite quaternion algebras and Teitelbaum's conjecture.* Submitted.

[D] H. Darmon, *Heegner points, Heegner cycles, and congruences*, In "Elliptic curves and related topics", CRM proceedings and lecture notes vol. 4, H. Kisilevsky and M. Ram Murty eds. (1992) pp. 45-60.

[DS] F. Diamond, and J. Shurman, *A First Course in Modular Forms*, Graduate Text in Mahtematics **228**, Speringer-Verlag, first edition (2005).

[GS] R. Greenberg, and G. Stevens, *On the conjecture of Mazur, Tate and Teitelbaum*, Contemp. Math. **165** (1994), 183-211.

[H] H. Hida, *Galois representations into* $\mathbf{GL_2}(\mathbb{Z}[[X]])$ *attached to ordinary cusp forms,* Invent. Math. **85** (1986), 545-613.

[K] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Text in Mathematics **97**, Speringer-Verlage, second edition, (1993).

[MSD] B. Mazur, and P. Swinnerton-Dyer, *Arithmetic of Weil Curves*, Inven. Math. **25** (1974), 1-61.

[P] A. Popa, *Central values of Rankin L-series over real quadratic fields*, Compos. Math. **142** (2006), no. 4, 811-866.

[MTT] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1-48.

[Shim72] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princton University Press (1972).

[Shim77] G. Shimura, *On the periods of modular forms*, Math. Ann. **229** (1977), 211-221.

[S] C. L. Siegel, *Advanced analytic number theory.* Second edition. Tata Institute of Fundamental Research Studies in Mathematics **9**. Tata Institute of Fundamental Research, Bombay, 1980.

Shahab Shahabi

Department of Mathematics and Statistics,

McGill University,

805 Sherbrooke St. West, Montreal,

Quebec, H3A 2K6, Canada.

E-mail: shahabi@math.mcgill.ca