p-adic periods, p-adic L-functions and the p-adic uniformization of Shimura curves

Massimo Bertolini[1]
Henri Darmon[2]

Contents

1 Introduction 1
2 Definite quaternion algebras and graphs 4
3 The p-adic L-function 8
4 The theory of p-adic uniformization of Shimura curves 14
5 p-adic Shintani cycles and special values of complex L-functions 17
6 p-adic Shintani cycles and derivatives of p-adic L-functions 19
7 Proof of theorem 6.1 22
References 30

1 Introduction

Let $E/\mathbb{Q}$ be a modular elliptic curve of conductor N, and let p be a prime of split multiplicative reduction for E. Write $\mathbb{C}_p$ for a fixed completion of an algebraic closure of $\mathbb{Q}_p$. Tate's theory of p-adic uniformization of elliptic curves yields a rigid-analytic, $\mathrm{Gal}(\mathbb{C}_p/\mathbb{Q}_p)$-equivariant uniformization of the $\mathbb{C}_p$-points of E

$$0 \to q^{\mathbb{Z}} \to \mathbb{C}_p^\times \xrightarrow{\Phi_{\mathrm{Tate}}} E(\mathbb{C}_p) \to 0, \tag{1}$$

where $q \in p\mathbb{Z}_p$ is the p-adic period of E.

Mazur, Tate and Teitelbaum conjectured in [MTT] that the cyclotomic p-adic L-function of $E/\mathbb{Q}$ vanishes at the central point to order one greater than that of its classical counterpart. Furthermore, they proposed a formula for the leading coefficient of such a p-adic L-function. In the special case where the analytic rank of $E(\mathbb{Q})$ is zero, they predicted that the ratio of the special value of the first derivative of the cyclotomic p-adic L-function and the algebraic part of the special value of the complex L-function of $E/\mathbb{Q}$ is equal to the quantity

$$\frac{\log_p(q)}{\mathrm{ord}_p(q)}$$

[1]Partially supported by GNSAGA (C.N.R.); M.U.R.S.T., progetto nazionale "Geometria algebrica"; Human Capital and Mobility Programme of the European Community, under contract ERBCH RXCT940557.

[2]Partially supported by grants from FCAR, NSERC and by an Alfred P. Sloan research award.

(where $\log_p$ is Iwasawa's cyclotomic logarithm), which is defined purely in terms of the p-adic uniformization of E. Greenberg and Stevens [GS] gave a proof of this special case. See also the work of Boichut [Boi] in the case of analytic rank one.

The article [BD1] formulates an analogue of the conjectures of [MTT] in which the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ is replaced by the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field K. When p is split in K and the sign of the functional equation of $L(E/K,s)$ is $+1$, this conjecture relates the first derivative of the anticyclotomic p-adic L-function of E to the anticyclotomic logarithm of the p-adic period of E. The present paper supplies a proof of this conjecture. Our proof is based on the theory of p-adic uniformization of Shimura curves.
More precisely, assume that K is an imaginary quadratic field with $(\mathrm{disc}(K), N) = 1$ such that:

(i) p is split in K;

(ii) E is semistable at the rational primes which divide N and are inert in K;

(iii) the number of these rational primes is odd.

The complex L-function $L(E/K,s)$ of E over K has a functional equation and an analytic continuation to the whole complex plane. Under our assumptions, the sign of the functional equation of $L(E/K,s)$ is $+1$ (cf. [GZ], p. 71), and hence $L(E/K,s)$ vanishes to even order at $s = 1$.

Fix a positive integer c prime to N, and let $\mathcal{O}$ be the order of K of conductor c. Let H_n be the ring class field of K of conductor cp^n, with $n \geq 0$, and let H_∞ be the union of the H_n. By class field theory, the Galois group $\mathrm{Gal}(H_\infty/H_0)$ is identified with $\mathcal{O}^\times\backslash(\mathcal{O}_K \otimes \mathbb{Z}_p)^\times/\mathbb{Z}_p^\times \simeq \mathbb{Z}_p \times \mathbb{Z}/((p-1)/u)\mathbb{Z}$, with $u := \frac{1}{2}\#\mathcal{O}^\times$. Moreover, $\mathrm{Gal}(H_0/K)$ is identified with the Picard group $\mathrm{Pic}(\mathcal{O})$. Set

$$\mathbf{G}_n := \mathrm{Gal}(H_n/K), \quad \mathbf{G}_\infty := \mathrm{Gal}(H_\infty/K).$$

Thus, $\mathbf{G}_\infty$ is isomorphic to the product of $\mathbb{Z}_p$ by a finite abelian group. Choose a prime $\mathfrak{p}$ of K above p. Identify $K_\mathfrak{p}$ with $\mathbb{Q}_p$, and let

$$\mathrm{rec}_p : \mathbb{Q}_p^\times \to \mathbf{G}_\infty$$

be the reciprocity map of local class field theory. Define the integral completed group ring of $\mathbf{G}_\infty$ to be

$$\mathbb{Z}[\![\mathbf{G}_\infty]\!] := \lim_{\substack{\leftarrow \\ n}} \mathbb{Z}[\mathbf{G}_n],$$

where the inverse limit is taken with respect to the natural projections of group rings.

In section 3, we recall the construction explained in [BD1], section 2.7 of an element

$$\mathcal{L}_p(E/K) \in \mathbb{Z}[\![\mathbf{G}_\infty]\!]$$

attached to $(E, H_\infty/K)$, which interpolates the special values $L(E/K,\chi,1)$ of $L(E/K,s)$ twisted by finite order characters of $\mathbf{G}_\infty$. The construction of this p-adic L-function is based on the ideas of Gross [Gr] and a generalization due to Daghigh [Dag]. We will show that $\mathcal{L}_p(E/K)$ belongs to the augmentation ideal I of $\mathbb{Z}[\![\mathbf{G}_\infty]\!]$. Let $\mathcal{L}'_p(E/K)$ be the natural image of $\mathcal{L}_p(E/K)$ in $I/I^2 = \mathbf{G}_\infty$. The element $\mathcal{L}'_p(E/K)$ should be viewed as the first derivative of $\mathcal{L}_p(E/K)$ at the central point.

Let $f = \sum_{n\geq 1} a_n q^n$ be the newform attached to E, and let

$$\Omega_f := 4\pi^2 \iint_{\mathcal{H}/\Gamma_0(N)} |f(\tau)|^2 d\tau \wedge i d\bar{\tau}$$

be the Petersson inner product of f with itself. We assume that E is the strong Weil curve for the Shimura curve parametrization defined in section 4. Set $d := \mathrm{disc}(\mathcal{O})$, and let n_f be the positive integer defined later in this introduction, and specified further in section 2. Our main result (stated in a special case: see theorem 6.4 for the general statement) is the following.

Theorem 1.1
Suppose that $c = 1$. The equality (up to sign)

$$\mathcal{L}'_p(E/K) = \frac{\mathrm{rec}_p(q)}{\mathrm{ord}_p(q)} \sqrt{L(E/K,1)\Omega_f^{-1} \cdot d^{\frac{1}{2}} u^2 n_f}$$

holds in $I/I^2 \otimes \mathbb{Q}$.

For the convenience of the reader, we now briefly sketch the strategy of the proof of theorem 1.1.

Write the conductor N of E as pN^+N^-, where N^+, resp. N^- is divisible only by primes which are split, resp. inert in K. Under our assumptions, N^- has an odd number of prime factors, and pN^- is squarefree. Denote by B the definite quaternion algebra over $\mathbb{Q}$ of discriminant N^-, and fix an Eichler order R of B of level N^+p. Let Γ be the subgroup of elements of $\mathbb{Q}_p^\times \backslash R[\frac{1}{p}]^\times$ whose norm has even p-adic valuation, and set $\mathcal{N} := \mathrm{Hom}(\Gamma, \mathbb{Z})$. The module $\mathcal{N}$ is a free abelian group, and is equipped with the action of a Hecke algebra $\mathbb{T}$ attached to modular forms of level N which are new at N^-p. In section 2, we will also define a canonical free quotient $\mathcal{N}_{\mathrm{sp}}$ of $\mathcal{N}$, which is stable for the action of $\mathbb{T}$ and is such that the image of $\mathbb{T}$ in $\mathrm{End}(\mathcal{N}_{\mathrm{sp}})$ corresponds to modular forms which are split multiplicative at p. Let π_f be the idempotent of $\mathbb{T} \otimes \mathbb{Q}$ associated with f, and let n_f be a positive integer such that $\eta_f := n_f \pi_f$ belongs to $\mathbb{T}$. Denote by $\mathcal{N}^f$ the submodule of $\mathcal{N}$ on which $\mathbb{T}$ acts via the character

$$\phi_f : \mathbb{T} \to \mathbb{Z}, \quad T_n \mapsto a_n$$

defined by f. By the multiplicity-one theorem, the module $\mathcal{N}^f$ is isomorphic to $\mathbb{Z}$. The operator η_f yields a map (denoted in the same way by an abuse of notation) $\eta_f : \mathcal{N} \to \mathcal{N}^f$, which factors through $\mathcal{N}_{\mathrm{sp}}$. We will define an element $\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K) \in \mathcal{N}_{\mathrm{sp}} \otimes \mathbb{Z}[\![\mathbf{G}_\infty]\!]$, such that (up to sign)

$$(\eta_f \otimes \mathrm{id})(\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K)) = c_p \cdot \mathcal{L}_p(E/K),$$

where $c_p := \mathrm{ord}_p(q)$. Recall that the derivative $\mathcal{L}'_p(E/K)$ of $\mathcal{L}_p(E/K)$ belongs to $\mathcal{N}^f \otimes \mathbf{G}_\infty = \mathbf{G}_\infty$.

On the other hand, the module $\mathcal{N}$ is related to the theory of p-adic uniformization of Shimura curves. Let $\mathcal{B}$ be the indefinite quaternion algebra of discriminant pN^-, and let $\mathcal{R}$ be an Eichler order of $\mathcal{B}$ of level N^+. Write X for the Shimura curve over $\mathbb{Q}$ associated with $\mathcal{R}$ (see section 4), and J for the jacobian of X. A theorem of Cerednik ([Cer]), combined with the theory of jacobians of Mumford curves ([GVdP]), yields a rigid-analytic uniformization

$$0 \to \Lambda \to \mathcal{N} \otimes \mathbb{C}_p^\times \xrightarrow{\Phi} J(\mathbb{C}_p) \to 0, \tag{2}$$

where Λ is the lattice of p-adic periods of J. The Tate uniformization (1) is obtained from the sequence (2) by applying the operator η_f to the Hecke modules $\mathcal{N} \otimes \mathbb{C}_p^\times$ and $J(\mathbb{C}_p)$ of (2). In particular, the p-adic period q of E can be viewed as an element of the module $\mathcal{N}^f \otimes \mathbb{C}_p^\times$, and in fact one checks it belongs to $\mathcal{N}^f \otimes \mathbb{Q}_p^\times = \mathbb{Q}_p^\times$. An explicit calculation of p-adic periods, combined with a formula for $L(E/K, 1)$ given in [Gr] and [Dag], will prove theorem 1.1.

A similar strategy was used in [BD2], when p is inert in K and the sign of the functional equation of $L(E/K, s)$ is -1, to obtain a p-adic analytic construction of a Heegner point in terms of the first derivative of an anticyclotomic p-adic L-function.

It is worth observing that an analogous strategy has not (yet) proven to work in the case of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. The difficulty is that of relating in a natural way the construction of the cyclotomic p-adic L-function, which is defined in terms of modular symbols, to the p-adic uniformization of Shimura curves. P. Schneider [Sch] has proposed the definition of a p-adic L-function based on the notion, which stems directly from the theory of p-adic uniformization, of rigid-analytic modular symbol. C. Klingenberg [Kl] has proven an exceptional zero formula similar to theorem 1.1 for this rigid-analytic p-adic L-function. However, the relation (if any) between Schneider's p-adic L-function and the cyclotomic p-adic L-function considered in [MTT] is at present mysterious.

The reader is also referred to Teitelbaum's paper [T], where the theory of p-adic uniformization of Shimura curves is used to formulate analogues of the conjectures of [MTT] for cyclotomic p-adic L-functions attached to modular forms of higher weight.

The proof by Greenberg and Stevens [GS] of the cyclotomic "exceptional zero" formula of [MTT] follows a completely different strategy from the one of this paper, and is based on Hida's theory of p-adic families of modular forms.

Finally, let us mention that Kato, Kurihara and Tsuji [KKT] have recently announced more general results on the conjectures of [MTT], which make use of an Euler System constructed by Kato from modular units in towers of modular function fields.

2 Definite quaternion algebras and graphs

Keep the notations and assumptions of the introduction. In particular, recall that K is an imaginary quadratic field, and B is a definite quaternion algebra of discriminant N^-. Given a rational prime ℓ, and orders O of K and S of B, set

$$K_\ell := K \otimes \mathbb{Z}_\ell, \quad B_\ell := B \otimes \mathbb{Z}_\ell, \quad O_\ell := O \otimes \mathbb{Z}_\ell, \quad S_\ell := S \otimes \mathbb{Z}_\ell.$$

Denote by $\hat{\mathbb{Z}} = \prod \mathbb{Z}_\ell$ the profinite completion of $\mathbb{Z}$. Set

$$\hat{K} := K \otimes \hat{\mathbb{Z}}, \quad \hat{B} := B \otimes \hat{\mathbb{Z}}, \quad \hat{O} := O \otimes \hat{\mathbb{Z}} = \prod O_\ell, \quad \hat{S} := S \otimes \hat{\mathbb{Z}} = \prod S_\ell.$$

Fix an Eichler order R of B of level N^+p. Equip R with an *orientation*, i.e., a collection of algebra homomorphisms

$$\mathfrak{o}_\ell^+ : R \to \mathbb{Z}/\ell^n\mathbb{Z}, \qquad \ell^n \| N^+p,$$

$$\mathfrak{o}_\ell^- : R \to \mathbb{F}_{\ell^2}, \qquad \ell \mid N^-.$$

The group $\hat{B}^\times$ acts transitively (on the right) on the set of Eichler orders of level N^+p by the rule

$$S * \hat{b} := (\hat{b}^{-1}\hat{S}\hat{b}) \cap B.$$

The orientation on R induces an orientation on $R * \hat{b}$, and the stabilizer of the oriented order R is equal to $\mathbb{Q}^\times \hat{R}^\times$. This sets up a bijection between the set of oriented Eichler orders of level N^+p and the coset space $\mathbb{Q}^\times \hat{R}^\times \backslash \hat{B}^\times$. Likewise, there is a bijection between the set of oriented Eicher orders of level N^+p modulo conjugation by $B^\times$ and the double coset space

$$\hat{R}^\times \backslash \hat{B}^\times / B^\times.$$

Set $\Gamma_+ := \mathbb{Q}_p^\times \backslash R[\frac{1}{p}]^\times$ and, as in the introduction, let Γ be the image in Γ_+ of the elements in $R[\frac{1}{p}]^\times$ whose reduced norm has even p-adic valuation.

Lemma 2.1
Γ has index 2 in Γ_+.

Proof. See [BD2], lemma 1.5.

Let $\mathcal{T}$ be the *Bruhat-Tits tree* associated with the local algebra B_p. The set of vertices $\mathcal{V}(\mathcal{T})$ of $\mathcal{T}$ is equal to the set of maximal orders in B_p. The set $\vec{\mathcal{E}}(\mathcal{T})$ of oriented edges of $\mathcal{T}$ is equal to the set of oriented Eichler orders of level p in B_p. Thus, $\vec{\mathcal{E}}(\mathcal{T})$ can be identified with the coset space $\mathbb{Q}_p^\times R_p^\times \backslash B_p^\times$, by mapping $b_p \in B_p^\times$ to $R_p * b_p = b_p^{-1} R_p b_p$. Similarly, if $\underline{R}_p$ is a maximal order in B_p containing R_p, we will identify $\mathcal{V}(\mathcal{T})$ with the coset space $\mathbb{Q}_p^\times \underline{R}_p^\times \backslash B_p^\times$. Define the graphs

$$\mathcal{G} := \mathcal{T}/\Gamma, \qquad \mathcal{G}_+ := \mathcal{T}/\Gamma_+.$$

By strong approximation ([Vi], p. 61), there is an identification

$$\vec{\mathcal{E}}(\mathcal{G}_+) = \hat{R}^\times \backslash \hat{B}^\times / B^\times$$

of the set of oriented edges of $\mathcal{G}_+$ with the set of conjugacy classes of oriented Eichler orders of level N^+p.

Fixing a vertex v_0 of $\mathcal{T}$ gives rise to an orientation of $\mathcal{T}$ in the following way. A vertex of $\mathcal{T}$ is called *even*, resp. *odd* if it has even, resp. odd distance from v_0. The direction of an edge is said to be positive if it goes from the even to the odd vertex. Since Γ sends even vertices to even ones, and odd vertices to odd ones, the orientation of $\mathcal{T}$ induces an orientation of $\mathcal{G}$. Define a map

$$\kappa : \mathcal{E}(\mathcal{G}) \to \vec{\mathcal{E}}(\mathcal{G}_+)$$

from the set of edges of $\mathcal{G}$ to the set of oriented edges of $\mathcal{G}_+$, by mapping an edge $\{v, v'\}$ (mod Γ) of $\mathcal{G}$, where v and v' are vertices of $\mathcal{T}$ and we assume that v is even, to the oriented edge (v, v') (mod Γ_+) of $\mathcal{G}_+$.

Lemma 2.2
The map κ is a bijection.

Proof. Suppose that (v, v') (mod Γ_+) $= (u, u')$ (mod Γ_+). Thus, there is $\gamma \in \Gamma_+$ such that $\gamma v = u$ and $\gamma v' = u'$. If v and u are both even, γ must belong to Γ, and this proves the injectivity of κ. As for surjectivity, (v, v') (mod Γ_+) is the image by κ of $\{v, v'\}$ (mod Γ) if v is even, and of $\{wv, wv'\}$ (mod Γ), where w is any element of $\Gamma_+ - \Gamma$, if v is odd.

Given two vertices v and v' of $\mathcal{T}$, write $\mathrm{path}(v, v')$ for the natural image in $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ of the unique geodesic on $\mathcal{T}$ joining v with v'. For example, if v and v' are even vertices joined by 4 consecutive edges e_1, e_2, e_3, e_4, by our convention for orienting the edges of $\mathcal{T}$, $\mathrm{path}(v, v')$ is the image in $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ of $e_1 - e_2 + e_3 - e_4$.

There is a coboundary map

$$\partial^* : \mathbb{Z}[\mathcal{V}(\mathcal{G})] \to \mathbb{Z}[\mathcal{E}(\mathcal{G})],$$

which maps the image in $\mathcal{V}(\mathcal{G})$ of an odd, resp. even vertex v of $\mathcal{T}$ to the image in $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ of the formal sum of the edges of $\mathcal{T}$ emanating from v, resp. the opposite of this sum. There is also a boundary map

$$\partial_* : \mathbb{Z}[\mathcal{E}(\mathcal{G})] \to \mathbb{Z}[\mathcal{V}(\mathcal{G})],$$

which maps an edge e to the difference $v' - v$ of its vertices, where v is the even vertex and v' is the odd vertex of e. The integral homology, resp. the integral cohomology of the graph $\mathcal{G}$ is defined by $H_1(\mathcal{G}, \mathbb{Z}) = \ker(\partial_*)$, resp. $H^1(\mathcal{G}, \mathbb{Z}) = \mathrm{coker}(\partial^*)$.

Let

$$\langle\ ,\ \rangle : \mathbb{Z}[\mathcal{E}(\mathcal{G})] \times \mathbb{Z}[\mathcal{E}(\mathcal{G})] \to \mathbb{Z}$$

be the pairing on $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ defined by the rule $\langle e_i, e_j \rangle := \omega_{e_i} \delta_{ij}$, where the e_i are the elements of the standard basis of $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ and ω_{e_i} is the order of the stabilizer in Γ of a lift of e_i to $\mathcal{T}$. Likewise, let

$$\langle\!\langle\ ,\ \rangle\!\rangle : \mathbb{Z}[\mathcal{V}(\mathcal{G})] \times \mathbb{Z}[\mathcal{V}(\mathcal{G})] \to \mathbb{Z}$$

be the pairing on $\mathbb{Z}[\mathcal{V}(\mathcal{G})]$ defined by $\langle\!\langle v_i, v_j \rangle\!\rangle := \omega_{v_i} \delta_{ij}$, where the v_i are the elements of the standard basis of $\mathbb{Z}[\mathcal{V}(\mathcal{G})]$ and ω_{v_i} is the order of the stabilizer in Γ of a lift of v_i to $\mathcal{T}$.

We use the notation $\mathcal{M}$ to indicate the module $H^1(\mathcal{G}, \mathbb{Z})$. Let $\bar{\Gamma}$ be the maximal torsion-free abelian quotient of Γ. As in the introduction, write $\mathcal{N}$ for $\mathrm{Hom}(\bar{\Gamma}, \mathbb{Z})$. Given an element $\gamma \in \Gamma$, denote by $\bar{\gamma}$ the natural image of γ in $\bar{\Gamma}$.

Lemma 2.3
(i) The map from $\bar{\Gamma}$ to $H_1(\mathcal{G}, \mathbb{Z})$ which sends $\bar{\gamma} \in \bar{\Gamma}$ to the cycle $\mathrm{path}(v_0, \gamma v_0)$, *where v_0 is any vertex of $\mathcal{G}$ and γ is any lift of $\bar{\gamma}$ to Γ, is an isomorphism.*

(ii) The map from $\mathcal{M}$ to $\mathcal{N}$ which sends $m \in \mathcal{M}$ to the homomorphism

$$\bar{\gamma} \mapsto \langle \mathrm{path}(v_0, \gamma v_0), m \rangle$$

is injective and has finite cokernel.

Proof (sketch). Part (i) is proved in [Se]. Part (ii) follows from part (i), and from the fact that the maps ∂^* and ∂_* are adjoint with respect to the pairings defined above.

Write $\mathcal{M}_{\mathrm{sp}}$ for the maximal torsion-free quotient of $\mathcal{M}/(w+1)\mathcal{M}$, with $w \in \Gamma_+ - \Gamma$. By part (i) of lemma 2.3, the action of $w \in \Gamma_+ - \Gamma$ on $H_1(\mathcal{G}, \mathbb{Z})$ induces an action of w on $\mathcal{N}$. Write $\mathcal{N}_{\mathrm{sp}}$ for the maximal torsion-free quotient of $\mathcal{N}/(w+1)\mathcal{N}$. We have an induced map from $\mathcal{M}_{\mathrm{sp}}$ to $\mathcal{N}_{\mathrm{sp}}$, which is injective and has finite cokernel.

The module $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ is equipped with the natural action of an algebra $\tilde{\mathbb{T}}$ generated over $\mathbb{Z}$ by the Hecke correspondences T_ℓ for $\ell \nmid N$ and U_ℓ for $\ell \mid N$, coming from its double coset description: see [BD1], sec. 1.5. The module $H_1(\mathcal{G}, \mathbb{Z})$ is stable under the action of $\tilde{\mathbb{T}}$. Hence, by part (i) of lemma 2.3, the algebra $\tilde{\mathbb{T}}$ also acts on the modules $\mathcal{N}$ and $\mathcal{N}_{\mathrm{sp}}$. Let $\mathbb{T}$ and $\mathbb{T}_{\mathrm{sp}}$ denote the image of $\tilde{\mathbb{T}}$ in $\mathrm{End}(\mathcal{N})$ and $\mathrm{End}(\mathcal{N}_{\mathrm{sp}})$, respectively. Thus, there are natural surjections $\tilde{\mathbb{T}} \to \mathbb{T} \to \mathbb{T}_{\mathrm{sp}}$. By an abuse of notation, we will denote by T_ℓ and U_ℓ also the natural images in $\mathbb{T}$ and $\mathbb{T}_{\mathrm{sp}}$ of T_ℓ and U_ℓ .

The next proposition clarifies the relation between the modules $\mathcal{N}$ and $\mathcal{N}_{\mathrm{sp}}$ and the theory of modular forms.

Proposition 2.4
Let ϕ be an algebra homomorphism from $\mathbb{T}$, resp. $\mathbb{T}_{\mathrm{sp}}$ to $\mathbb{C}$, and let $a_n := \phi(T_n)$. Then, the a_n are the Fourier coefficients of a normalized eigenform of level N, which is new at N^-p, resp. is new at N^-p and is split multiplicative at p. Conversely, any such modular form arises as above from a character of $\mathbb{T}$, resp. $\mathbb{T}_{\mathrm{sp}}$.

Proof. Eichler's trace formula identifies the Hecke-module $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ with a space of modular forms of level N which are new at N^-. Moreover, the algebra $\mathbb{T}$ can also be viewed as the Hecke algebra of the module $\mathcal{M}$ defined above, and proposition 1.4 of [BD2] shows that $\mathcal{M}$ is equal to the "p-new" quotient of $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$. This proves the statement of proposition 2.4 concerning characters of $\mathbb{T}$. The abelian variety associated to a p-new modular form f is split multiplicative at p if and only if $U_p f = f$. Moreover, the Atkin-Lehner involution at p acts on a p-new modular form as $-U_p$, and acts on $\mathcal{M}$ as Γ_+/Γ. This concludes the proof of proposition 2.4.

Modular parametrizations, I

We now make a specific choice of the operator η_f (where f is the newform of level N attached to E) considered in the introduction, that will be used in formulating the results in the sequel of the paper.

As stated in lemma 2.3, $\bar{\Gamma}$ can be identified with the homology group $H_1(\mathcal{G}, \mathbb{Z}) \subset \mathbb{Z}[\mathcal{E}(\mathcal{G})]$. Thus, when convenient, we will tacitly view elements of $\bar{\Gamma}$ as contained in $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$. The restriction of the pairing on $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ defined above to $\bar{\Gamma}$ yields the *monodromy pairing* (denoted in the same way by an abuse of notation)

$$\langle\ ,\ \rangle : \bar{\Gamma} \times \bar{\Gamma} \to \mathbb{Z}.$$

Let $\mathbb{Z}[\mathcal{E}(\mathcal{G})]^f$, resp. $\bar{\Gamma}^f$ be the submodule of $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$, resp. $\bar{\Gamma}$ on which $\tilde{\mathbb{T}}$, resp. $\mathbb{T}$ acts via the character associated with f. Note that the quotient of $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ by $\bar{\Gamma}$ is torsion-free, and thus there is a canonical identification $\mathbb{Z}[\mathcal{E}(\mathcal{G})]^f = \bar{\Gamma}^f$. Let e^f be a generator of $\bar{\Gamma}^f \simeq \mathbb{Z}$.

Define the "modular parametrizations"

$$\pi_* : \bar{\Gamma} \to \bar{\Gamma}^f, \qquad \pi^* : \bar{\Gamma}^f \to \bar{\Gamma}$$

by $\pi_*(e) := \langle e, e^f\rangle e^f$ and $\pi^*(e^f) := e^f$. Since

$$(\pi^* \circ \pi_*)^2 = \langle e^f, e^f\rangle(\pi^* \circ \pi_*),$$

we obtain that $\pi^* \circ \pi_*$ is equal to $\langle e^f, e^f\rangle\pi_f$, where π_f is the idempotent of $\mathbb{T} \otimes \mathbb{Q}$ associated with f. From now on, we will assume that the operator η_f is defined by

$$\eta_f := \pi^* \circ \pi_*,$$

so that the integer n_f is equal to $\langle e^f, e^f\rangle$.

As observed in the introduction, the operator η_f induces a map $\mathcal{N} \to \mathbb{Z}$, which is well-defined up to sign. Since f has split multiplicative reduction at p, this map factors through a map $\mathcal{N}_{\mathrm{sp}} \to \mathbb{Z}$. By an abuse of notation, we will indicate by η_f both the above maps.

Remark 2.5
The module $\bar{\Gamma}$ can be identified with the character group associated with the reduction modulo p of $\mathrm{Pic}^0(X)$, where X is the Shimura curve considered in the introduction. As will be explained in section 4, the map $\pi^* \circ \pi_*$ on $\bar{\Gamma}$ is induced by functoriality from a modular parametrization $\mathrm{Pic}^0(X) \to E$.

3 The p-adic L-function

Let $\mathcal{O}_n$ denote the order of K of conductor cp^n, $n \geq 0$. (We will usually write $\mathcal{O}$ instead of $\mathcal{O}_0$.) Equip the orders $\mathcal{O}_n$ with compatible orientations, i.e., with compatible algebra homomorphisms

$$\mathfrak{d}_\ell^+ : \mathcal{O}_n \to \mathbb{Z}/\ell^m\mathbb{Z}, \qquad \ell^m \| N^+p,$$

$$\mathfrak{d}_\ell^- : \mathcal{O}_n \to \mathbb{F}_{\ell^2}, \qquad \ell \mid N^-.$$

An algebra homomorphism of $\mathcal{O}_n$ into an oriented Eichler order S of level N^+p is called an *oriented optimal embedding* if it respects the orientation on $\mathcal{O}_n$ and on S, and does not extend to an embedding of a larger order into S. Consider pairs (R_ξ, ξ), where R_ξ is an oriented Eichler order of level N^+p and ξ is an element of $\mathrm{Hom}(K, B)$ which restricts to an oriented optimal embedding of $\mathcal{O}_n$ into R_ξ. A

Gross point of conductor cp^n $(n \geq 0)$ is a pair as above, taken modulo the action of $B^\times$.

By our previous remarks, a Gross point can be viewed naturally as an element of the double coset space

$$W := (\hat{R}^\times \backslash \hat{B}^\times \times \mathrm{Hom}(K, B))/B^\times.$$

(See [Gr], sec. 3 for more details.) Strong approximation gives the identification

$$W = (\vec{\mathcal{E}}(\mathcal{T}) \times \mathrm{Hom}(K, B))/\Gamma_+.$$

By lemma 2.2, there is a natural map of $\mathbb{Z}$-modules $\mathbb{Z}[W] \to \mathbb{Z}[\mathcal{E}(\mathcal{G})]$, where $\mathbb{Z}[W]$ is the module of finite formal $\mathbb{Z}$-linear combinations of elements of W. The Hecke algebra $\tilde{\mathbb{T}}$ of $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ acts naturally also on $\mathbb{Z}[W]$ (see [BD1], sec. 1.5), in such a way that the above map is $\tilde{\mathbb{T}}$-equivariant.

The group $\mathbf{G}_n = \mathrm{Pic}(\mathcal{O}_n) = \hat{\mathcal{O}}_n^\times \backslash \hat{K}^\times / K^\times$ acts simply transitively on the Gross points of conductor cp^n by the rule

$$\sigma(R_\xi, \xi) := (R_\xi * \hat{\xi}(\sigma)^{-1}, \xi),$$

where $\hat{\xi}$ denotes the extension of ξ to a map from $\hat{K}$ to $\hat{B}$.

Now, fix a Gross point $P_0 = (R_0, \xi_0) \pmod{B^\times}$ of conductor c. By the above identification, P_0 corresponds to a pair $(\vec{e}_0, \xi_0) \in \vec{\mathcal{E}}(\mathcal{T}) \times \mathrm{Hom}(K, B)$, modulo the action of Γ_+. As above, the origin v_0 of $\vec{e}_0$ determines an orientation of $\mathcal{T}$. Let $\vec{e}$ be one of the p oriented edges of $\mathcal{T}$ originating from $\vec{e}_0$. All the Gross points corresponding to pairs $(\vec{e}, \xi_0)$ as above have conductor cp, except for one, which has conductor c. Fix an end

$$(\vec{e}_0, \vec{e}_1, \ldots, \vec{e}_n, \ldots),$$

such that $(\vec{e}_1, \xi_0)$ defines a Gross point of conductor cp. Then, $(\vec{e}_n, \xi_0)$ defines a Gross point P_n of conductor cp^n, for all $n \geq 0$.

Denote by $\mathrm{Norm}_{H_{n+1}/H_n}$ the norm operator $\sum_{g \in \mathrm{Gal}(H_{n+1}/H_n)} g$.

Lemma 3.1
1) Let $u = \frac{1}{2}\#\mathcal{O}^\times$. *The equality*

$$U_p P_0 = u \mathrm{Norm}_{H_1/H_0} P_1 + \sigma_{\mathfrak{p}} P_0$$

holds in $\mathbb{Z}[W]$ *for a prime* $\mathfrak{p}$ *above* p, *where* $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(H_0/K)$ *denotes the image of* $\mathfrak{p}$ *by the Artin map.*

2) For $n \geq 1$,

$$U_p P_n = \mathrm{Norm}_{H_{n+1}/H_n} P_{n+1}.$$

Proof. It follows from the definition of the operator U_p (see [BD1], sec. 1.5) and the action of $\mathrm{Pic}(\mathcal{O}_n)$ on the Gross points.

The picture below, drawn in the case $p = 2$, illustrates geometrically the relation between the Galois action and the action of the Hecke correspondence U_p.

By lemma 2.3, the natural map from $\mathbb{Z}[W]$ to $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ induces maps from $\mathbb{Z}[W]$ to the modules $\mathcal{N}$ and $\mathcal{N}_{\mathrm{sp}}$. These maps are Hecke-equivariant.

The Gross points P_n give rise to a p-adic distribution on $\mathbf{G}_\infty$ with values in the module $\mathcal{N}_{\mathrm{sp}}$ as follows. Given $g \in \mathbf{G}_n$, denote by e_n^g the natural image of P_n^g in $\mathcal{N}_{\mathrm{sp}}$. For $n \geq 0$, define the truncated p-adic L-function

$$\mathcal{L}_{p,n}(\mathcal{N}_{\mathrm{sp}}/K) := \sum_{g \in \mathbf{G}_n} e_n^g \cdot g^{-1} \in \mathcal{N}_{\mathrm{sp}} \otimes \mathbb{Z}[\mathbf{G}_n].$$

Note that $\mathcal{L}_{p,n}(\mathcal{N}_{\mathrm{sp}}/K)$ is well-defined up to multiplication by elements of $\mathbf{G}_n$.

For $n \geq 1$, let $\nu_n : \mathbb{Z}[\mathbf{G}_n] \to \mathbb{Z}[\mathbf{G}_{n-1}]$ be the natural projection of groups rings.

Lemma 3.2
1) The equality

$$\nu_1(\mathcal{L}_{p,1}(\mathcal{N}_{\mathrm{sp}}/K)) = u^{-1}(1-\sigma_{\mathfrak{p}})\mathcal{L}_{p,0}(\mathcal{N}_{\mathrm{sp}}/K)$$

holds in $\mathcal{N}_{\mathrm{sp}} \otimes \mathbb{Z}[\mathbf{G}_0]$.
2) For $n \geq 2$*, the equality*

$$\nu_n(\mathcal{L}_{p,n}(\mathcal{N}_{\mathrm{sp}}/K)) = \mathcal{L}_{p,n-1}(\mathcal{N}_{\mathrm{sp}}/K)$$

holds in $\mathcal{N}_{\mathrm{sp}} \otimes \mathbb{Z}[\mathbf{G}_{n-1}]$.

Proof. By proposition 2.4, the operator U_p acts as $+1$ on $\mathcal{N}_{\mathrm{sp}}$. The claim follows from lemma 3.1 and the fact that $\mathcal{N}_{\mathrm{sp}}$ is torsion-free.

Define the p-adic L-function attached to $\mathcal{N}_{\mathrm{sp}}$ to be

$$\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K) := \varprojlim_n \mathcal{L}_{p,n}(\mathcal{N}_{\mathrm{sp}}/K) \in \mathcal{N}_{\mathrm{sp}} \otimes \mathbb{Z}[\![\mathbf{G}_\infty]\!].$$

We now define the p-adic L-function attached to E. Observe that the maximal quotient $\bar{\Gamma}_f$ of $\bar{\Gamma}$ on which $\mathbb{T}$ acts via the character associated with f is isomorphic to $\mathbb{Z}$. Let e_f be a generator of $\bar{\Gamma}_f$. The monodromy pairing on $\bar{\Gamma}$ induces a $\mathbb{Z}$-valued pairing on $\bar{\Gamma}^f \times \bar{\Gamma}_f$. Write $\hat{c}_p$ for the positive integer $|\langle e^f, e_f\rangle|$.

Lemma 3.3
The element $(\eta_f \otimes \mathrm{id})(\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K)) \in \mathbb{Z}[\![\mathbf{G}_\infty]\!]$ *is divisible by* $\hat{c}_p$.

Proof. Consider the maps

$$\tilde{\pi}_* : \mathbb{Z}[\mathcal{E}(\mathcal{G})] \to \mathbb{Z}[\mathcal{E}(\mathcal{G})]^f, \qquad \tilde{\pi}^* : \mathbb{Z}[\mathcal{E}(\mathcal{G})]^f \to \mathbb{Z}[\mathcal{E}(\mathcal{G})]$$

defined by $\tilde{\pi}_*(e) := \langle e, e^f\rangle e^f$ and $\tilde{\pi}^*(e^f) := e^f$. (The modular parametrizations π_* and π^* introduced in section 2 are obtained from these maps by restriction.) Hence, $\tilde{\eta}_f := \tilde{\pi}^* \circ \tilde{\pi}_*$ is an element of $\tilde{\mathbb{T}}$, equal to $\langle e^f, e^f\rangle\tilde{\pi}_f$, where $\tilde{\pi}_f$ is the idempotent in $\tilde{\mathbb{T}} \otimes \mathbb{Q}$ associated with f. We have a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}[\mathcal{E}(\mathcal{G})] & \longrightarrow & \mathcal{N} \\ {\scriptstyle \tilde{\eta}_f}\big\downarrow & & {\scriptstyle \eta_f}\big\downarrow \\ \mathbb{Z}[\mathcal{E}(\mathcal{G})]^f & \longrightarrow & \mathcal{N}^f, \end{array}$$

where the upper horizontal map is defined in lemma 2.3, and the lower horizontal map is the restriction of the upper one. Note that $\mathcal{N}^f$ is equal to $\mathrm{Hom}(\bar{\Gamma}_f, \mathbb{Z})$, and therefore is generated by the homomorphism $e_f \mapsto 1$. With our choices of generators for $\mathbb{Z}[\mathcal{E}(\mathcal{G})]^f$ and $\mathcal{N}^f$, the lower map of the above diagram is described as multiplication by the integer $\langle e^f, e_f \rangle$. The proof of lemma 3.2 also shows that mapping the Gross points of conductor cp^n to $\mathbb{Z}[\mathcal{E}(\mathcal{G})]^f$ by the map $\tilde{\eta}_f$ yields a p-adic distribution in $\mathbb{Z}[\mathcal{E}(\mathcal{G})]^f \otimes \mathbb{Z}[\![\mathbf{G}_\infty]\!]$. By the above diagram, the image of this distribution in $\mathcal{N}^f \otimes \mathbb{Z}[\![\mathbf{G}_\infty]\!]$ is equal to $(\eta_f \otimes \mathrm{id})(\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K))$. This proves the lemma.

Remark 3.4 In section 4, we will show that the integers $\hat{c}_p$ and c_p are equal.

Define the p-adic L-function attached to E to be

$$\mathcal{L}_p(E/K) = \hat{c}_p^{-1}(\eta_f \otimes \mathrm{id})(\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K)) \in \mathbb{Z}[\![\mathbf{G}_\infty]\!].$$

Observe that $\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K)$ and $\mathcal{L}_p(E/K)$ are well-defined up to multiplication by elements of $\mathbf{G}_\infty$.

Recall the quantities Ω_f and d defined in the introduction.

Theorem 3.5
Let $\chi : \mathbf{G}_\infty \to \mathbb{C}^\times$ be a finite order character of conductor cp^n, with $n \geq 1$. Then the equality

$$|\chi(\mathcal{L}_p(E/K))|^2 = \frac{L(E/K, \chi, 1)}{\Omega_f}\sqrt{d} \cdot (n_f u)^2$$

holds.

Proof. See [Gr], [Dag], and [BD1], section 2.10.

Remark 3.6
1) Theorem 3.5 suggests that $\mathcal{L}_p(E/K)$ should really be viewed as the square root of a p-adic L-function, and hence we should define the anticyclotomic p-adic L-function of E to be $\mathcal{L}_p(E/K) \otimes \mathcal{L}_p(E/K)^*$, where $*$ denotes the involution of $\mathbb{Z}[\![\mathbf{G}_\infty]\!]$ given on group-like elements by $g \mapsto g^{-1}$. See section 2.7 of [BD1] for more details.
2) More generally, the p-adic L-function $\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K)$ interpolates special values of the complex L-series attached to the modular forms on $\mathbb{T}_{\mathrm{sp}}$ (described in proposition 2.4).

Let $\sigma_{\mathfrak{p}}$ be as in lemma 3.1. Denote by H the subextension of H_0 which is fixed by $\sigma_{\mathfrak{p}}$, and set

$$G_n := \mathrm{Gal}(H_n/H), \qquad G_\infty := \mathrm{Gal}(H_\infty/H),$$

$$\Sigma := \mathrm{Gal}(H_0/H) = G_0, \qquad \Delta := \mathrm{Gal}(H/K).$$

Note the exact sequences of Galois groups

$$0 \to G_n \to \mathbf{G}_n \to \Delta \to 0,$$

$$0 \to G_\infty \to \mathbf{G}_\infty \to \Delta \to 0.$$

The group Δ is naturally identified with the Picard group $\mathrm{Pic}(\mathcal{O}[\frac{1}{p}])$, and G_∞ is equal to the image of the reciprocity map $\mathrm{rec}_p : \mathbb{Q}_p^\times \to \mathbf{G}_\infty$ (where we have identified $\mathbb{Q}_p^\times$ with $K_{\mathfrak{p}}^\times$). Let I be the kernel of the augmentation map $\mathbb{Z}[\![\mathbf{G}_\infty]\!] \to \mathbb{Z}$, and let I_Δ be the kernel of the augmentation map $\mathbb{Z}[\![\mathbf{G}_\infty]\!] \to \mathbb{Z}[\Delta]$.

Lemma 3.7
i) $\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K)$ *belongs to* $\mathcal{N}_{\mathrm{sp}} \otimes I_\Delta$.
ii) $\mathcal{L}_p(E/K)$ *belongs to* I_Δ.

Proof. There are canonical isomorphisms

$$\mathbb{Z}[\![\mathbf{G}_\infty]\!]/I_\Delta = \mathbb{Z}[\mathbf{G}_n]/I_{\Delta,n} = \mathbb{Z}[\Delta],$$

where $I_{\Delta,n}$ is the natural image of I_Δ in $\mathbb{Z}[\mathbf{G}_n]$. By lemma 3.2, the image of $\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K)$ in $\mathcal{N}_{\mathrm{sp}} \otimes (\mathbb{Z}[\![\mathbf{G}_\infty]\!]/I_\Delta)$ is equal to the image of $\mathcal{L}_{p,1}(\mathcal{N}_{\mathrm{sp}}/K)$ in $\mathcal{N}_{\mathrm{sp}} \otimes (\mathbb{Z}[\mathbf{G}_1]/I_{\Delta,1}) = \mathcal{N}_{\mathrm{sp}} \otimes \mathbb{Z}[\Delta]$. The first part of the lemma now follows from lemma 3.2, 1). The second part follows directly from the first.

Since I_Δ is contained in I, the element $\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K)$ belongs to $\mathcal{N}_{\mathrm{sp}} \otimes I$ and $\mathcal{L}_p(E/K)$ belongs to I. Denote by

$$\mathcal{L}_p'(\mathcal{N}_{\mathrm{sp}}/K), \qquad \mathcal{L}_p'(\mathcal{N}_{\mathrm{sp}}/H)$$

the natural image of $\mathcal{L}_p(\mathcal{N}_{\mathrm{sp}}/K)$ in $\mathcal{N}_{\mathrm{sp}} \otimes I/I^2 = \mathcal{N}_{\mathrm{sp}} \otimes \mathbf{G}_\infty$ and $\mathcal{N}_{\mathrm{sp}} \otimes I_\Delta/I_\Delta^2 = \mathcal{N}_{\mathrm{sp}} \otimes \mathbb{Z}[\Delta] \otimes G_\infty$, respectively. Likewise, let

$$\mathcal{L}_p'(E/K), \qquad \mathcal{L}_p'(E/H)$$

be the natural image of $\mathcal{L}_p(E/K)$ in $I/I^2 = \mathbf{G}_\infty$ and $I_\Delta/I_\Delta^2 = \mathbb{Z}[\Delta] \otimes G_\infty$, respectively. The above elements should be viewed as derivatives of p-adic L-functions at the central point.

In order to carry out the calculations of the next sections, it is useful to observe that the derivatives $\mathcal{L}_p'(\mathcal{N}_{\mathrm{sp}}/K)$ and $\mathcal{L}_p'(\mathcal{N}_{\mathrm{sp}}/H)$ can be expressed in terms of the derivatives of certain partial p-adic L-functions. Set $h := \#(\Delta)$. Fix Gross points of conductor c

$$P_0 = P_0^1, \ldots, P_0^h,$$

corresponding to pairs (R_0^i, ξ_0^i), $i = 1, \ldots, h$, which are representatives for the Σ-orbits of the Gross points of conductor c. Writing $[P_0^i]$ for the Σ-orbit of P_0^i, let δ_i be the element of Δ such that

$$[\delta_i P_0^1] = [P_0^i].$$

Suppose that P_0^i corresponds to a pair $(\vec{e}_0(i), \xi_0^i) \in \vec{\mathcal{E}}(\mathcal{T}) \times \mathrm{Hom}(K, B)$, modulo the action of Γ_+. Fix ends

$$(\vec{e}_0(i), \vec{e}_1(i), \ldots, \vec{e}_n(i), \ldots)$$

such that $(\vec{e}_1(i), \xi_0^i)$ defines a Gross point of conductor cp. Thus, $(\vec{e}_n(i), \xi_0^i)$ defines a Gross point P_n^i of conductor cp^n, for all $n \geq 0$. For $g \in G_n$, let $e_n(i)^g$ denote the natural image of $(P_n^i)^g$ in $\mathcal{N}_{\mathrm{sp}}$. Let

$$\mathcal{L}_{p,n}(\mathcal{N}_{\mathrm{sp}}/H, P_0^i) := \sum_{g \in G_n} e_n(i)^g \cdot g^{-1} \in \mathcal{N}_{\mathrm{sp}} \otimes \mathbb{Z}[G_n].$$

The proof of lemma 3.2 also shows that the elements $\mathcal{L}_{p,n}(\mathcal{N}_{\rm sp}/H, P_0^i)$ are compatible under the maps induced by the natural projections of group rings. Thus, we may define the partial p-adic L-function attached to $\mathcal{N}_{\rm sp}$ and P_0^i to be

$$\mathcal{L}_p(\mathcal{N}_{\rm sp}/H, P_0^i) := \lim_{\substack{\leftarrow \\ n}} \mathcal{L}_{p,n}(\mathcal{N}_{\rm sp}/H, P_0^i) \in \mathcal{N}_{\rm sp} \otimes \mathbb{Z}[\![G_\infty]\!].$$

Observe that $\mathcal{L}_p(\mathcal{N}_{\rm sp}/H, P_0^i)$ depends only on the Σ-orbit of P_0^i, up to multiplication by elements of G_∞.

Let I_H be the kernel of the augmentation map $\mathbb{Z}[\![G_\infty]\!] \to \mathbb{Z}$. Like in the proof of lemma 3.7, one checks that $\mathcal{L}_p(\mathcal{N}_{\rm sp}/H, P_0^i)$ belongs to I_H. Write $\mathcal{L}'_p(\mathcal{N}_{\rm sp}/H, P_0^i)$ for the natural image of $\mathcal{L}_p(\mathcal{N}_{\rm sp}/H, P_0^i)$ in $\mathcal{N}_{\rm sp} \otimes I_H/I_H^2 = \mathcal{N}_{\rm sp} \otimes G_\infty$. Thus,

$$\mathcal{L}'_p(\mathcal{N}_{\rm sp}/H, P_0^i) = \lim_{\substack{\leftarrow \\ n}} \mathcal{L}'_{p,n}(\mathcal{N}_{\rm sp}/H, P_0^i),$$

where

$$\mathcal{L}'_{p,n}(\mathcal{N}_{\rm sp}/H, P_0^i) = \sum_{g \in G_n} e_n(i)^g \otimes g^{-1}. \tag{3}$$

We obtain directly:

Lemma 3.8
i)

$$\mathcal{L}'_p(\mathcal{N}_{\rm sp}/K) = \sum_{i=1}^{h} \mathcal{L}'_p(\mathcal{N}_{\rm sp}/H, P_0^i).$$

ii)

$$\mathcal{L}'_p(\mathcal{N}_{\rm sp}/H) = \sum_{i=1}^{h} \mathcal{L}'_p(\mathcal{N}_{\rm sp}/H, P_0^i) \cdot \delta_i^{-1}.$$

4 The theory of p-adic uniformization of Shimura curves

For more details on the results stated in this section, the reader is referred to [BC], [Cer], [Dr], [GVdP] and [BD2].

Let $\mathcal{B}$ be the indefinite quaternion algebra over $\mathbb{Q}$ of discriminant N^-p, and let $\mathcal{R}$ be an Eichler order of $\mathcal{B}$ of level N^+. Denote by X the Shimura curve over $\mathbb{Q}$ associated with the order $\mathcal{R}$. We refer the reader to [BC] and [BD2], section 4 for the definition of X via moduli. Here we content ourselves with recalling Cerednik's theorem, which describes a rigid-analytic uniformization of X. Write

$$\mathcal{H}_p := \mathbb{C}_p - \mathbb{Q}_p$$

for the p-adic upper half plane. The group $\mathrm{GL}_2(\mathbb{Q}_p)$ acts (on the left) on $\mathcal{H}_p$ by linear fractional transformations. Thus, fixing an isomorphism

$$\psi : B_p \to M_2(\mathbb{Q}_p)$$

induces an action of Γ on $\mathcal{H}_p$. This action is discontinuous, and the rigid-analytic quotient $\Gamma\backslash\mathcal{H}_p$ defines the $\mathbb{C}_p$-points of a non-singular curve $\mathcal{X}$ over $\mathbb{Q}_p$. The curves X and $\mathcal{X}$ are equipped with the action of Hecke algebras $\mathbb{T}_X$ and $\mathbb{T}_{\mathcal{X}}$, respectively ([BC], [BD1]).

By lemma 2.1, the action of Γ_+/Γ induces an involution W of $\mathcal{X}$. Let $\mathbb{Q}_{p^2}$ be the unique unramified quadratic extension of $\mathbb{Q}_p$ contained in $\mathbb{C}_p$, and let τ be the generator of $\mathrm{Gal}(\mathbb{Q}_{p^2}/\mathbb{Q}_p)$. Denote by $\natural \in H^1(\langle\tau\rangle, \mathrm{Aut}(\mathcal{X}))$ the class of the cocycle mapping τ to W, and write $\mathcal{X}^\natural$ for the curve over $\mathbb{Q}_p$ obtained by twisting $\mathcal{X}$ by $\natural$.

Theorem 4.1 (Cerednik)
There is a Hecke-equivariant isomorphism $X \simeq \mathcal{X}^\natural$ of curves over $\mathbb{Q}_p$. In particular, X and $\mathcal{X}$ are isomorphic over $\mathbb{Q}_{p^2}$.

Proof. See [Cer], [Dr], [BC].

Building on theorem 4.1, the results in [GVdP] yield a rigid-analytic description of the jacobian of X. If $D = P_1 + \cdots + P_r - Q_1 - \cdots - Q_r \in \mathrm{Div}^0(\mathcal{H}_p)$ is a divisor of degree zero on $\mathcal{H}_p$, define the theta function

$$\vartheta(z; D) = \prod_{\epsilon\in\Gamma} \frac{(z-\epsilon P_1)\cdots(z-\epsilon P_r)}{(z-\epsilon Q_1)\cdots(z-\epsilon Q_r)} .$$

Write $\bar{\delta}$ for the natural image in $\bar{\Gamma}$ of an element δ of Γ. For all δ in Γ, the above theta function satisfies the functional equation

$$\vartheta(\delta z; D) = \phi_D(\bar{\delta})\vartheta(z; D),$$

where ϕ_D is an element of $\mathrm{Hom}(\bar{\Gamma}, \mathbb{C}_p^\times) = \mathcal{N} \otimes \mathbb{C}_p^\times$ which does not depend on z. For $\gamma \in \Gamma$, the number $\phi_{(\gamma z)-(z)}(\bar{\delta})$ does not depend on the choice of $z \in \mathcal{H}_p$, and depends only on the image of γ in $\bar{\Gamma}$. This gives rise to a pairing

$$[\ ,\ ] : \bar{\Gamma} \times \bar{\Gamma} \to \mathbb{Q}_p^\times .$$

The pairing $[\ ,\ ]$ is bilinear and symmetric. The next proposition explains the relation between $[\ ,\ ]$ and the monodromy pairing $\langle\ ,\ \rangle : \bar{\Gamma} \times \bar{\Gamma} \to \mathbb{Z}$ defined in section 2.

Proposition 4.2
The pairings $\langle\ ,\ \rangle$ and $\mathrm{ord}_p \circ [\ ,\ ]$ are equal.

Proof. See [M], th. 7.6.

It follows that $\mathrm{ord}_p \circ [\ ,\ ]$ is positive definite, so that themap

$$j : \bar{\Gamma} \to \mathcal{N} \otimes \mathbb{Q}_p^\times$$

induced by $[\ ,\ ]$ is injective and has discrete image. Set $\Lambda := j(\bar{\Gamma})$. Given a divisor D of degree zero on $\mathcal{X}(\mathbb{C}_p) = \Gamma\backslash\mathcal{H}_p$, let $\tilde{D}$ denote an arbitrary lift to a degree zero divisor on $\mathcal{H}_p$. The automorphy factor $\phi_{\tilde{D}}$ depends on the choice of the lift $\tilde{D}$, but its image in $(\mathcal{N}\otimes\mathbb{C}_p^\times)/\Lambda$ depends only on D. Thus, the assignment $D\mapsto\phi_{\tilde{D}}$ gives a well-defined map from $\mathrm{Div}^0(\mathcal{X}(\mathbb{C}_p))$ to $(\mathcal{N}\otimes\mathbb{C}_p^\times)/\Lambda$.

Proposition 4.3
The map $\mathrm{Div}^0(\mathcal{X}(\mathbb{C}_p))\to(\mathcal{N}\otimes\mathbb{C}_p^\times)/\Lambda$ defined above is trivial on the group of principal divisors, and induces a Hecke-equivariant isomorphism from the $\mathbb{C}_p$-points of the jacobian $\mathcal{J}$ of $\mathcal{X}$ to $(\mathcal{N}\otimes\mathbb{C}_p^\times)/\Lambda$.

Proof. See [GVdP], VI.2 and VIII.4, and also [BC], ch. III.

Let

$$\Phi:\mathcal{N}\otimes\mathbb{C}_p^\times\to\mathcal{J}(\mathbb{C}_p)$$

stand for the map induced by (the inverse of) the isomorphism defined in proposition 4.3.

Modular parametrizations, II

The map $\eta_f:\mathcal{N}\to\mathbb{Z}$ defined in section 2 induces a map

$$\eta_f\otimes\mathrm{id}:\mathcal{N}\otimes\mathbb{C}_p^\times\to\mathbb{C}_p^\times.$$

The Jacquet-Langlands correspondence [JL] implies that the quotient abelian variety $\eta_f J$ is an elliptic curve $\mathbb{Q}$-isogenous to E. From now on, we assume that $E=\eta_f J$ is the *strong Weil curve* for the parametrization by the Shimura curve X. By an abuse of notation, we denote by η_f also the surjective map

$$J(\mathbb{C}_p)\to E(\mathbb{C}_p)$$

induced by η_f.

Let Λ^f be the submodule of Λ on which $\mathbb{T}$ acts via the character ϕ_f.

Proposition 4.4
The kernel $q^{\mathbb{Z}}$ of Φ_{Tate} is canonically equal to the module Λ^f, and the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Lambda & \longrightarrow & \mathcal{N}\otimes\mathbb{C}_p^\times & \xrightarrow{\Phi} & \mathcal{J}(\mathbb{C}_p) & \longrightarrow & 0\\
 & & {\scriptstyle\eta_f}\big\downarrow & & {\scriptstyle\eta_f\otimes\mathrm{id}}\big\downarrow & & {\scriptstyle\eta_f}\big\downarrow & & \\
0 & \longrightarrow & \Lambda^f & \longrightarrow & \mathbb{C}_p^\times & \xrightarrow{\Phi_{\mathrm{Tate}}} & E(\mathbb{C}_p) & \longrightarrow & 0
\end{array}$$

is Hecke-equivariant and commutes up to sign.

Proof. The right-most square in the above diagram is a consequence of proposition 4.3, combined with theorem 4.1 and the fact that f is split-multiplicative at p. In order to obtain the left-most square, it is enough to prove that the kernel of Φ_{Tate} is equal to Λ^f. Note that the target $\mathbb{C}_p^\times=\mathcal{N}^f\otimes\mathbb{C}_p^\times$ of the map $\eta_f\otimes\mathrm{id}$ is naturally a submodule of $\mathcal{N}\otimes\mathbb{C}_p^\times$, since the quotient of $\mathcal{N}$ by $\mathcal{N}^f$ is torsion-free. By definition, $E(\mathbb{C}_p)$ may similarly be viewed as an abelian subvariety of $\mathcal{J}(\mathbb{C}_p)$. It follows that Φ_{Tate} can be described as the restriction of Φ to $\mathbb{C}_p^\times$. In particular, $\ker(\Phi_{\mathrm{Tate}})$ is equal to $\Lambda\cap\mathbb{C}_p^\times$. In turn, this last module is equal to Λ^f.

Corollary 4.5
The integer $\hat{c}_p = |\langle e^f, e_f\rangle|$ *(introduced in lemma 3.3) is equal to* c_p.

Proof. Working through the definition of the maps in the diagram of proposition 4.4 shows that $[e^f, e_f]$ is equal to $q^{\pm 1}$. The claim follows from proposition 4.2.

5 p-adic Shintani cycles and special values of complex L-functions

Let $P_0 = (R_0, \xi_0) \pmod{B^\times}$ be a Gross point of conductor c. The point P_0 determines a p-adic cycle $\mathfrak{c}(P_0) \in \bar{\Gamma}$ in the following way. By strong approximation, we may assume that the representative (R_0, ξ_0) for P_0 is such that the oriented orders $R_0[\frac{1}{p}]$ and $R[\frac{1}{p}]$ are equal. Thus, ξ_0 induces an embedding of $\mathcal{O}[\frac{1}{p}]$ into $R[\frac{1}{p}]$, which we still denote by ξ_0. The image by ξ_0 of a fundamental p-unit in $\mathcal{O}[\frac{1}{p}]$ having norm of even p-adic valuation determines an element $\gamma = \gamma(P_0)$ of Γ. This element is well-defined up to conjugation and up to inversion, and up to multiplication by the image of torsion elements of $\mathcal{O}^\times$.

More explicitly, write k for the order of $\sigma_{\mathfrak{p}}$ in $\mathrm{Pic}(\mathcal{O})$ (where $\sigma_{\mathfrak{p}}$ is as in lemma 3.1), and set $\mathfrak{p}^k = (v)$ with $v \in \mathcal{O}$. Let ι be 1, resp. 2 if k is even, resp. odd. Then γ is the image of $\xi_0(v)^\iota$ in Γ.

Definition. The *p-adic Shintani cycle* $\mathfrak{c} = \mathfrak{c}(P_0)$ attached to P_0 is the natural image of γ in $\bar{\Gamma}$.

This terminology is justified in the remark 5.4 below. Observe that $\mathfrak{c}$ is well-defined up to sign.

Denote by $\mathbb{Z}[\mathcal{E}(\mathcal{G})]_{\mathrm{sp}}$ the maximal torsion-free quotient of $\mathbb{Z}[\mathcal{E}(\mathcal{G})]/(w+1)\mathbb{Z}[\mathcal{E}(\mathcal{G})]$, where w is any element of $\Gamma_+ - \Gamma$. Recall the element $\tilde{\eta}_f \in \tilde{\mathbb{T}}$ defined in the proof of lemma 3.3, mapping to η_f by the natural projection $\tilde{\mathbb{T}} \to \mathbb{T}$. The next lemma relates the p-adic cycle $\mathfrak{c}$ to the image in $\mathcal{N}_{\mathrm{sp}}$ of the Gross point P_0.

Lemma 5.1
The natural images in $\mathbb{Z}[\mathcal{E}(\mathcal{G})]_{\mathrm{sp}}$ *of* $\mathfrak{c}$ *and* $\sum_{\sigma\in\Sigma} \iota P_0^\sigma$ *are equal. In particular,* $\eta_f \mathfrak{c}$ *is equal to the image of* $\sum_{\sigma\in\Sigma} \iota(\tilde{\eta}_f P_0^\sigma)$ *in* $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$.

Proof. (In order to visualize the geometric content of this proof, the reader may find it helpful to refer to the picture in section 3.) Set $P_i := \sigma_{\mathfrak{p}}^i P_0$, for $i = 0, \ldots, k-1$. By part 1 of lemma 3.1 and the definition of the action of U_p on the Bruhat-Tits tree, we can fix representatives $(\vec{e}_i, \xi_0)$ for the Gross points P_i so that the $\vec{e}_i$ are consecutive oriented edges of $\mathcal{T}$. With notations as at the beginning of this section, let $\gamma_+ \in \Gamma_+$ be the image of $\xi_0(v)$. Thus, $\gamma = \gamma_+^\iota$. Call v_0 the origin of $\vec{e}_0$. If $\iota = 1$, the even vertex of the edge $\vec{e}_{k-1}$ is equal to γv_0. If $\iota = 2$, i.e., γ_+ belongs to $\Gamma_+ - \Gamma$, then

$$\vec{e}_0, \ldots, \vec{e}_{k-1}, \gamma_+\vec{e}_0, \ldots, \gamma_+\vec{e}_{k-1}$$

is a sequence of consecutive oriented edges, and the even vertex of $\gamma_+\vec{v}_{k-1}$ is equal to γv_0. Note that $\sum_{\sigma\in\Sigma} \iota P_0^\sigma$ is equal in $\mathbb{Z}[\vec{\mathcal{E}}(\mathcal{G}_+)]$ to $\vec{e}_0 + \vec{e}_1 + \ldots + \vec{e}_{k-1}$ if $\iota = 1$, and to

$$\vec{e}_0 + \vec{e}_1 + \ldots + \vec{e}_{k-1} + \gamma_+\vec{e}_0 + \gamma_+\vec{e}_1 + \ldots + \gamma_+\vec{e}_{k-1}$$

if $\iota = 2$. Denote by e_i the unoriented edge of $\mathcal{T}$ corresponding to $\vec{e}_i$, and let w be any element of $\Gamma_+ - \Gamma$. By definition of the bijection κ of lemma 2.2, the following equalities hold in $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$:

$$\kappa^{-1}(\vec{e}_0 + \ldots + \vec{e}_{k-1}) = e_0 + we_1 + \ldots + e_{k-2} + we_{k-1} \qquad \text{if } \iota = 1,$$

$$\begin{aligned}\kappa^{-1}(\vec{e}_0 + \ldots + \vec{e}_{k-1} + \gamma_+\vec{e}_0 + \gamma_+\vec{e}_1 + \ldots + \gamma_+\vec{e}_{k-1})) = e_0 + we_1 + \ldots \\ + e_{k-1} + w(\gamma_+e_0) + (\gamma_+e_1) + \ldots + w(\gamma_+e_{k-1}) \qquad \text{if } \iota = 2.\end{aligned}$$

Projecting the right hand sides of the above equalities to $\mathbb{Z}[\mathcal{E}(\mathcal{G})]_{\mathrm{sp}}$, and keeping into account that w acts as -1 on this module, gives in both cases path$(v_0, \gamma v_0)$.

The next proposition elucidates the relation between the p-adic Shintani cycle defined above and the special values of the complex L-function of E/K. Following the notations of section 3, fix Gross points $P_0 = P_0^1, \ldots, P_0^h$ which are representatives for the Σ-orbits of the Gross points of conductor c, and list the elements of Δ so that $[\delta_i P_0^1] = [P_0^i]$, where $[P_0^i]$ denotes the Σ-orbit of P_0^i. As above, the Gross point P_0^i determines a p-adic Shintani cycle $\mathfrak{c}_i \in \bar{\Gamma}$, with $\mathfrak{c}_1 = \mathfrak{c}$. Given a complex character $\chi : \Delta \to \mathbb{C}^\times$ of Δ, set

$$\mathfrak{c}_H := \sum_{i=1}^{h} \mathfrak{c}_i \otimes \delta_i^{-1} \in \bar{\Gamma} \otimes \mathbb{Z}[\Delta],$$

$$\mathfrak{c}_{K,\chi} := \chi(\mathfrak{c}_H) = \sum_{i=1}^{h} \mathfrak{c}_i \otimes \chi(\delta_i)^{-1} \in \bar{\Gamma} \otimes \mathbb{Z}[\chi].$$

If χ is the trivial character, we will also write $\mathfrak{c}_K$ as a shorthand for $\mathfrak{c}_{K,\chi}$. Extend the pairing $\langle\ ,\ \rangle$ on $\bar{\Gamma}$ to a hermitian pairing on $\bar{\Gamma} \otimes \mathbb{Z}[\chi]$.

Proposition 5.2
Suppose that χ is primitive. The following equality holds:

$$\langle \eta_f \mathfrak{c}_{K,\chi}, \mathfrak{c}_{K,\chi} \rangle = \frac{L(E/K,\chi,1)}{\Omega_f}\sqrt{d} \cdot (\iota u)^2 \cdot n_f.$$

Proof. In view of lemma 5.1, this is simply a restatement of the results of [Gr] and [Dag].

Recall the maps $j : \bar{\Gamma} \to \mathcal{N} \otimes \mathbb{Q}_p^\times$ and $\eta_f \otimes \mathrm{id} : \mathcal{N} \otimes \mathbb{C}_p^\times \to \mathbb{C}_p^\times$ defined in section 4. By an abuse of notation, we denote in the same way the maps obtained by extending scalars to $\mathbb{Z}[\chi]$.

Corollary 5.3
The equality

$$(\eta_f \otimes \mathrm{id})(j(\mathfrak{c}_{K,\chi})) = q \otimes \rho$$

holds in $\mathbb{Q}_p^\times \otimes \mathbb{Z}[\chi]$, where $\rho \in \mathbb{Z}[\chi]$ satisfies

$$|\rho|^2 = \frac{L(E/K,\chi,1)}{\Omega_f}\sqrt{d} \cdot (\iota u)^2 \cdot n_f.$$

Proof. By proposition 4.4 combined with the definition of η_f given in section 2, ρ is equal to $\langle \mathfrak{c}_{K,\chi}, e^f \rangle \in \mathbb{Z}[\chi]$. Hence

$$\begin{aligned} |\rho|^2 &= \langle \mathfrak{c}_{K,\chi}, e^f \rangle \langle e^f, \mathfrak{c}_{K,\chi} \rangle \\ &= \langle \eta_f \mathfrak{c}_{K,\chi}, \mathfrak{c}_{K,\chi} \rangle. \end{aligned}$$

The claim follows from proposition 5.2.

Remark 5.4
Let F be a real quadratic field and let $\psi : F \to M_2(\mathbb{Q})$ be an embedding. Assume that ψ maps the ring of integers $\mathcal{O}_F$ to the Eichler order $M_0(N)$ of integral matrices with lower left entry divisible by N. Since the homology group $H_1(X_0(N), \mathbb{Z})$ can be identified with the maximal torsion-free abelian quotient of $\Gamma_0(N)$, the image by ψ of a fundamental unit in $\mathcal{O}_F$ of norm 1 determines an integral homology cycle $\mathfrak{s} \in H_1(X_0(N), \mathbb{Z})$. Shintani [Sh] proved that the cycle $\mathfrak{s}$ encodes the special values of the classical L-series over F attached to newforms on $X_0(N)$. In light of proposition 5.2, the element $\mathfrak{c}$ can be viewed as a p-adic analogue of the cycle $\mathfrak{s}$.

6 p-adic Shintani cycles and derivatives of p-adic L-functions

Let P_0 be a Gross point of conductor c. In section 5, we attached to P_0 a p-adic cycle $\mathfrak{c} \in \bar{\Gamma}$, and proved in proposition 5.2 that $\mathfrak{c}$ is related to the special values of the complex L-function of E/K. Our main result (theorem 6.1 below) shows that $\mathfrak{c}$ is also related to the first derivative of the p-adic L-function defined in section 3. By combining these results we will obtain theorem 1.1.

Write $\underline{j}$ for the composite map

$$\bar{\Gamma} \xrightarrow{j} \mathcal{N} \otimes \mathbb{Q}_p^\times \to \mathcal{N}_{\mathrm{sp}} \otimes \mathbb{Q}_p^\times \to \mathcal{N}_{\mathrm{sp}} \otimes G_\infty,$$

where the second map is induced by the natural projection of $\mathcal{N}$ onto $\mathcal{N}_{\mathrm{sp}}$, and the third map is induced by $\mathrm{rec}_p : \mathbb{Q}_p^\times \to G_\infty$. Our main result is the following.

Theorem 6.1
The following equality holds up to sign in $\mathcal{N}_{\mathrm{sp}} \otimes G_\infty$:

$$\mathcal{L}_p'(\mathcal{N}_{\mathrm{sp}}/H, P_0)^\iota = \underline{j}(\mathfrak{c}).$$

Recall the definition of the elements $\mathfrak{c}_H$ and $\mathfrak{c}_K$ given in section 5. By lemma 3.8, we obtain directly:

Corollary 6.2
(i) The following equality holds up to sign in $\mathcal{N}_{\mathrm{sp}} \otimes \mathbb{Z}[\Delta] \otimes G_\infty$:

$$\mathcal{L}'_p(\mathcal{N}_{\mathrm{sp}}/H)^\iota = \underline{j}(\mathfrak{c}_H).$$

(ii) The following equality holds up to sign in $\mathcal{N}_{\mathrm{sp}} \otimes G_\infty$:

$$\mathcal{L}'_p(\mathcal{N}_{\mathrm{sp}}/K)^\iota = \underline{j}(\mathfrak{c}_K).$$

By applying the operator η_f to both sides of the equalities of corollary 6.2, and using corollary 4.5 and the definitions of the p-adic L-functions attached to $\mathcal{N}_{\mathrm{sp}}$ and E , we find:

Corollary 6.3
(i) The following equality holds up to sign in $\mathbb{Z}[\Delta] \otimes G_\infty$:

$$c_p\mathcal{L}'_p(E/H)^\iota = \underline{j}(\eta_f \mathfrak{c}_H).$$

(ii) The following equality holds up to sign in G_∞:

$$c_p\mathcal{L}'_p(E/K)^\iota = \underline{j}(\eta_f \mathfrak{c}_K).$$

Proof of theorem 1.1
Combine corollary 6.3 with corollary 5.3.

By combining corollary 6.3 with corollary 5.3, we also obtain the following generalization of theorem 1.1. Let $\mathcal{L}'_p(E/K,\chi)$ stand for the element $\chi(\mathcal{L}'_p(E/H))$ of $G_\infty \otimes \mathbb{Z}[\chi]$.

Theorem 6.4
Suppose that χ is primitive. The following equalities hold up to sign:

$$c_p\mathcal{L}'_p(E/K,\chi) = \mathrm{rec}_p(q) \otimes \rho \qquad \text{in } G_\infty \otimes \mathbb{Z}[\frac{1}{2}][\chi]$$

and

$$\mathcal{L}'_p(E/K,\chi) = \frac{\mathrm{rec}_p(q)}{\mathrm{ord}_p(q)} \otimes \rho \qquad \text{in } G_\infty \otimes \mathbb{Q}[\chi],$$

where

$$|\rho|^2 = \frac{L(E/K,\chi,1)}{\Omega_f} \cdot d^{\frac{1}{2}} u^2 n_f.$$

Corollary 6.5
The derivative $\mathcal{L}_p'(E/K,\chi)$ is non-zero in $G_\infty \otimes \mathbb{Q}[\chi]$ if and only if the classical special value $L(E/K,\chi,1)$ is non-zero.

Proof. By theorem 6.4, one is reduced to showing that $\mathrm{rec}_p(q)$ is a non-torsion element of G_∞, i.e., q^{p-1} does not belong to the kernel of the reciprocity map. But elements in this kernel are algebraic over $\mathbb{Q}$, and q is known to be transcendental by a result of Barré-Sirieix, Diaz, Gramain and Philibert [BSDGP].

Remark 6.6
Theorem 1.1 was conjectured in [BD1], section 5.1 in a slightly different form. We conclude this section by studying the compatibility of theorem 1.1 (and its generalization theorem 6.4) with the conjectures of [BD1]. For simplicity, assume throughout this remark that the elliptic curve E is semistable, so that N is squarefree, and that E is isolated in its isogeny class, so that the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the ℓ-torsion points of E is irreducible for all primes ℓ.

Let $p_1 \cdots p_n q_1 \cdots q_n$ be a prime factorization of the squarefree integer pN^-, with $p_1 = p$. Denote by X_1 the Shimura curve X, and by X_{n+1} the classical modular curve $X_0(N)$. For $i = 2, \ldots, n$, denote by X_i the Shimura curve associated with an Eichler order of level $N^+ p_1 \cdots p_{i-1} q_1 \cdots q_{i-1}$ in the indefinite quaternion algebra of discriminant $p_i \cdots p_n q_i \cdots q_n$. Since E is modular, the Jacquet-Langlands correspondence [JL] implies that E is parametrized by the jacobian J_i of the curve X_i, $i = 1, \ldots, n+1$. Let

$$\phi_i : J_i \to E$$

be the *strong* Weil parametrization of E by J_i. Thus, the morphism ϕ_i has connected kernel, and its dual $\phi_i^\vee : E \to J_i$ is injective. The endomorphism $\phi_i \circ \phi_i^\vee$ of E is multiplication by an integer d_{X_i}, called the *degree* of the modular parametrization of E by the Shimura curve X_i.

If $\ell \mid N$, denote by c_ℓ the order of the group of connected components of E at ℓ.

Theorem 6.7 (Ribet-Takahashi)
Under our assumptions:

i)

$$\frac{d_{X_0(N)}}{d_X} = c_{p_1} \cdots c_{p_n} c_{q_1} \cdots c_{q_n};$$

ii)

$$\langle e^f, e^f \rangle = d_X c_p \ .$$

Proof. Part i) follows from theorem 1 of [RT]. Part ii) follows from section 2 of [RT]. The results of [RT] exclude the case where N^+ is prime, but a forthcoming paper of S. Takahashi will deal with this case as well.

By combining theorem 6.7 with the relation $\Omega_f = d_{X_0(N)} \cdot \Omega_E$, where Ω_E is the complex period of E, we find that the formula of theorem 1.1 (and likewise for theorem 6.4) becomes

$$\mathcal{L}_p'(E/K) = \frac{\mathrm{rec}_p(q)}{\mathrm{ord}_p(q)} \sqrt{L(E/K,1)\Omega_E^{-1} \cdot d^{\frac{1}{2}} u^2 \prod_{\ell | N^-} c_\ell^{-1}},$$

which is the same as conjecture 5.3 of [BD1].

7 Proof of theorem 6.1

First, we give an explicit description of certain group actions on the p-adic upper half plane and on the Bruhat-Tits tree depending on our choice of a Gross point P_0 of conductor c. Then, we compute the value $\underline{j}(\mathfrak{c})$, for $\mathfrak{c}$ as in sections 5 and 6.

I Group actions on $\mathcal{H}_p$ and $\mathcal{T}$

Let $K_p := K \otimes \mathbb{Q}_p$. Our choice of a prime $\mathfrak{p}$ above p determines an identification of $K_p = K_{\mathfrak{p}} \times K_{\bar{\mathfrak{p}}}$ with $\mathbb{Q}_p \times \mathbb{Q}_p$.

As in section 5, choose a representative (R_0, ξ_0) for the Gross point P_0 such that $R_0[\frac{1}{p}]$ and $R[\frac{1}{p}]$ are equal. Let $(\vec{e}_0, \xi_0)$ be a pair corresponding to P_0, and denote by v_0 the origin of $\vec{e}_0$. Set $R_{0,p} := R_0 \otimes \mathbb{Z}_p$, and let $\underline{R}_{0,p}$ be the maximal order of B_p corresponding to v_0. Recall the isomorphism

$$\psi : B_p \to M_2(\mathbb{Q}_p)$$

fixed in section 4. We may, and will from now on, choose ψ so that:

i) ψ maps $\underline{R}_{0,p}$ onto $M_2(\mathbb{Z}_p)$;

ii) $\psi \circ \xi_0$ maps $(x, y) \in K_p = \mathbb{Q}_p \times \mathbb{Q}_p$ to the diagonal matrix $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$.

Condition i) allows us to identify $\mathcal{T} = \mathbb{Q}_p^\times \underline{R}_{0,p}^\times \backslash B_p^\times$ with $\mathrm{PGL}_2(\mathbb{Z}_p)\backslash\mathrm{PGL}_2(\mathbb{Q}_p)$. Viewing $K_p^\times$ as a subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$ thanks to the embedding $\psi \circ \xi_0$ yields actions of $K_p^\times$ on $\mathcal{H}_p$ and on $\mathcal{T} = \mathrm{PGL}_2(\mathbb{Z}_p)\backslash\mathrm{PGL}_2(\mathbb{Q}_p)$, factoring through $K_p^\times/\mathbb{Q}_p^\times$. Identify this last group with $\mathbb{Q}_p^\times$ by mapping a pair (x, y) modulo $\mathbb{Q}_p^\times$ to xy^{-1}. Under this identification, an element x of $\mathbb{Q}_p^\times$ acts on $\mathcal{H}_p$ as multiplication by x, and on $\mathcal{T}$ as conjugation by the matrix $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$.

Recall the element $v \in \mathcal{O} \subset K_p^\times$ defined in section 5 by $\mathfrak{p}^k = (v)$. Identify as above v with an element $\underline{w}$ of $\mathbb{Q}_p^\times$. Note that $\underline{w}$ is equal to p^k times a p-adic unit. Set $\tilde{G}_\infty := \mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times$. Define the quotients of $\tilde{G}_\infty$

$$\tilde{\Sigma} := \mathbb{Q}_p^\times/\mathbb{Z}_p^\times = p^{\mathbb{Z}}, \qquad \tilde{G}_n := p^{\mathbb{Z}} \times (\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times,\ n \geq 1.$$

To simplify slightly the computation, assume from now on that $\mathcal{O}^\times = \{\pm 1\}$. (If $\mathcal{O}^\times \neq \{\pm 1\}$, then K has discriminant -3 or -4, and the exact sequences below have to be modified to account for the non-trivial units of $\mathcal{O}$. The computations in this case follow closely those presented in the paper.) Class field theory yields the exact sequence

$$0 \to \langle \underline{w} \rangle \to \tilde{G}_\infty \xrightarrow{\mathrm{rec}_p} G_\infty \to 0,$$

and the induced sequences

$$0 \to \langle \underline{w} \rangle \to \tilde{\Sigma} \to \Sigma \to 0, \qquad 0 \to \langle \underline{w} \rangle \to \tilde{G}_n \to G_n \to 0.$$

For $n \geq 0$, denote by $\mathbb{Z}_p^{(n)} \subset \tilde{G}_\infty$ the subgroup of elements of $\mathbb{Z}_p^\times$ which are congruent to 1 modulo p^n.

Definition. We say that a vertex v of $\mathcal{T}$ has *level* n, and write $\ell(v) = n$, if the stabilizer of v for the action of $\tilde{G}_\infty$ is equal to $\mathbb{Z}_p^{(n)}$. Likewise, we say that an edge e of $\mathcal{T}$ has *level* n, and write $\ell(e) = n$, if the stabilizer of e for the action of $\tilde{G}_\infty$ is $\mathbb{Z}_p^{(n)}$.

Note that the group $\tilde{G}_n$ ($\tilde{\Sigma}$ if $n = 0$) acts simply transitively on the vertices and edges of level n. By definition of the action of $\tilde{G}_\infty$ on $\mathcal{T}$, v_0 is a vertex of level 0. Thus, the set of vertices of level 0 is equal to the $\tilde{\Sigma}$-orbit of v_0. More generally, the set of vertices of level n can be described as the $\tilde{G}_n$-orbit of a vertex v_n, whose distance from v_0 is n and whose distance from all the other vertices in the orbit $\tilde{\Delta}v_0$ is $> n$.

By using the standard coordinate, identify $\mathbb{P}^1(\mathbb{C}_p)$ with $\mathbb{C}_p \cup \{\infty\}$ and $\mathcal{H}_p$ with $\mathbb{P}^1(\mathbb{C}_p) - \mathbb{P}^1(\mathbb{Q}_p)$. In particular, view 0 and ∞ as elements of $\mathbb{P}^1(\mathbb{Q}_p)$. Recall the element $\gamma = \gamma(P_0)$ of Γ defined in section 5. Since the reduced norm of γ has positive valuation, our choice of the isomorphism ψ yields

$$(4) \qquad \lim_{n\to+\infty} \gamma^n z = 0, \qquad \lim_{n\to-\infty} \gamma^n z = \infty$$

for all $z \in \mathcal{H}_p$. Note also that 0 and ∞ are the fixed points for the action of $\tilde{G}_\infty$ on $\mathbb{P}^1(\mathbb{C}_p)$.

Let $\mathcal{H}_p(\mathbb{Q}_{p^2}) = \mathbb{Q}_{p^2} - \mathbb{Q}_p$ be the $\mathbb{Q}_{p^2}$-points of the p-adic upper half plane. Define the *reduction map*

$$r : \mathcal{H}_p(\mathbb{Q}_{p^2}) \to \mathcal{V}(\mathcal{T})$$

as follows. Given $z \in \mathcal{H}_p(\mathbb{Q}_{p^2})$, let $\mathcal{Q}_z$ denote the stabilizer of z in $\mathrm{GL}_2(\mathbb{Q}_p)$, together with the zero matrix. Then $\mathcal{Q}_z$ is a field isomorphic to $\mathbb{Q}_{p^2}$, and this gives rise to an embedding of $\mathbb{Q}_{p^2}$ in $M_2(\mathbb{Q}_p)$ (well-defined up to an isomorphism of $\mathbb{Q}_{p^2}$). Write $\mathbb{Z}_{p^2}$ for the ring of integers of $\mathbb{Q}_{p^2}$, and let S be the unique maximal order of $M_2(\mathbb{Q}_p)$ containing the image of $\mathbb{Z}_{p^2}$ by the above embedding. We have $r(z) = S$. (See also [BD2], section 1.)

Lemma 7.1
1) The reduction map r is $\mathrm{GL}_2(\mathbb{Q}_p)$-equivariant. In particular, r is equivariant for the group actions defined above.

2) Write $\mathbb{Z}_{p^2} = \mathbb{Z}_p\alpha + \mathbb{Z}_p$. We have $r^{-1}(v_0) = \mathbb{Z}_p^\times\alpha + \mathbb{Z}_p$.

3) If z_1 and z_2 are mapped by r to adjacent vertices of respective levels n and $n+1$, then $z_1 z_2^{-1} \equiv 1 \pmod{p^n}$.

Proof.
1) Let z be an element of $\mathcal{H}_p(\mathbb{Q}_{p^2})$, and let B be a matrix in $\mathrm{GL}_2(\mathbb{Q}_p)$. If $f : \mathbb{Q}_{p^2} \to M_2(\mathbb{Q}_p)$ is an embedding fixing z, then BfB^{-1} is an embedding fixing Bz. Suppose that S is the maximal ideal containing $f(\mathbb{Z}_{p^2})$. Then $BSB^{-1} = S * B^{-1}$ is the maximal ideal containing the image of $\mathbb{Z}_{p^2}$ by BfB^{-1}. Thus, $r(Bz) = S * B^{-1}$, as was to be shown.
2) Suppose to fix ideas that $p > 2$. Then, we may assume that $\alpha = \sqrt{\nu}$, where the integer ν is not a squaremodulo p. (The case $p = 2$ can be dealt with in a similar way, for instance by taking $\alpha = (1 + \sqrt{-3})/2$.) A direct computation shows that

$$\mathcal{Q}_{\sqrt{\nu}} = \left\{ \begin{pmatrix} b & a\nu \\ a & b \end{pmatrix} : a, b \in \mathbb{Q}_p \right\}.$$

Mapping the above matrix to $a\sqrt{\nu}+b$ yields an isomorphism of $\mathcal{Q}_{\sqrt{\nu}}$ onto $\mathbb{Q}_{p^2}$. Thus, $r(\sqrt{\nu})$ is equal to $v_0 = M_2(\mathbb{Z}_p)$. Given $z = a\sqrt{\nu}+b \in \mathcal{H}_p(\mathbb{Q}_{p^2})$, we have $z = B\sqrt{\nu}$, where B is the matrix $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. By part 1,

$$r(z) = BM_2(\mathbb{Z}_p)B^{-1}.$$

But $BM_2(\mathbb{Z}_p)B^{-1} = M_2(\mathbb{Z}_p)$ if and only if B belongs to $\mathrm{GL}_2(\mathbb{Z}_p)$, i.e., a belongs to $\mathbb{Z}_p^\times$.

3) Set $r(z_1) = v_1$ and $r(z_2) = v_2$. The edge joining v_1 to v_2 has level $n+1$. Since $\tilde{G}_\infty = \mathbb{Q}_p^\times$ acts transitively on the edges of level $n+1$, there is $g \in \mathbb{Q}_p^\times$ such that gv_1 and gv_2 have distance from v_0 equal to n and $n+1$, respectively. With notations as in the proof of part 2 of this proposition, write $gz_i = a_i\sqrt{\nu}+b_i$, $i = 1, 2$, where $a_i, b_i \in \mathbb{Z}_p$, $gcd(a_i, b_i) = 1$, and $p^n \parallel a_1$, $p^{n+1} \parallel a_2$. Thus, the vertex gv_i is represented by the matrix

$$A_i = \begin{pmatrix} a_i & b_i \\ 0 & 1 \end{pmatrix}.$$

Our assumption on gv_1 and gv_2 implies that the column $\begin{pmatrix} b_2 \\ 1 \end{pmatrix}$ of A_2 is a $\mathbb{Z}_p$-linear combination of the columns of A_1. It follows that $b_1 \equiv b_2 \pmod{p^n}$, and hence

$$z_1 z_2^{-1} = gz_1(gz_2)^{-1} \equiv 1 \pmod{p^n}.$$

II The calculation

Given $\delta \in \Gamma$, write as usual $\bar{\delta}$ for the natural image of δ in $\bar{\Gamma}$. We now compute explicitly the value of $j(\mathfrak{c})(\bar{\delta}) = [\mathfrak{c}, \bar{\delta}]$, for $\delta \in \Gamma$. We begin with the following lemma.

Lemma 7.2

Given $\delta \in \Gamma$, we have

$$j(\mathfrak{c})(\bar{\delta}) = \prod_{\epsilon \in \mathcal{S}} \frac{\epsilon\delta z_0}{\epsilon z_0},$$

where z_0 is any element in $\mathcal{H}_p$, and $\mathcal{S}$ is any set of representatives for $\langle\gamma\rangle\backslash\Gamma$.

Proof. (Cf. [M], theorem 2.8.)

Let $\mathcal{S}'$ be any set of representatives for $\Gamma/\langle\gamma\rangle$. In view of the formulae (4), for any z_0 and a in $\mathcal{H}_p$ we have the chain of equalities

$$\begin{aligned}
j(\mathfrak{c})(\bar{\delta}) &= \prod_{\epsilon \in \Gamma} \frac{z_0 - \epsilon a}{z_0 - \epsilon\gamma a} \cdot \frac{\delta z_0 - \epsilon\gamma a}{\delta z_0 - \epsilon a} \\
&= \prod_{\epsilon \in \mathcal{S}'} \prod_{n=-\infty}^{+\infty} \frac{z_0 - \epsilon\gamma^n a}{z_0 - \epsilon\gamma^{n+1} a} \cdot \frac{\delta z_0 - \epsilon\gamma^{n+1} a}{\delta z_0 - \epsilon\gamma^n a} \\
&= \prod_{\epsilon \in \mathcal{S}'} \lim_{N \to +\infty} \frac{z_0 - \epsilon\gamma^{-N} a}{z_0 - \epsilon\gamma^{N+1} a} \cdot \frac{\delta z_0 - \epsilon\gamma^{N+1} a}{\delta z_0 - \epsilon\gamma^{-N} a} \\
&= \prod_{\epsilon \in \mathcal{S}'} \frac{z_0 - \epsilon\infty}{z_0 - \epsilon 0} \cdot \frac{\delta z_0 - \epsilon 0}{\delta z_0 - \epsilon\infty} \\
&= \prod_{\epsilon \in \mathcal{S}'} \frac{\epsilon^{-1}\delta z_0}{\epsilon^{-1} z_0}.
\end{aligned}$$

Note that $(\mathcal{S}')^{-1}$ is a set of representatives for $\langle\gamma\rangle\backslash\Gamma$, and any set of representatives for $\langle\gamma\rangle\backslash\Gamma$ can be obtained in this way. The claim follows.

Lemma 7.3
Let d be an edge of $\mathcal{T}$, let n be a positive integer, and let $\mathcal{S}$ be a set of representatives for $\langle\gamma\rangle\backslash\Gamma$. Then the set $\{\epsilon \in \mathcal{S} : \ell(\epsilon d) \leq n\}$ is finite.

Proof. If $\{\epsilon_i\}$ is a sequence of distinct elements of $\mathcal{S}$ such that $\ell(\epsilon_i d) \leq n$, we can find integers k_i such that $\gamma^{k_i}\epsilon_i d$ describes only finitely many edges. This contradicts the discreteness of Γ.

We say that two elements of $\bar{\Gamma}$ are *linearly independent* if they generate a rank two free abelian subgroup of $\bar{\Gamma}$.

Proposition 7.4
1) Suppose that $\mathfrak{c}$ and $\bar{\delta}$ are linearly independent in $\bar{\Gamma}$. There exists a set $\mathcal{S}$ of representatives for $\langle\gamma\rangle\backslash\Gamma$ such that if ϵ belongs to $\mathcal{S}$, then all the elements of the coset $\epsilon\langle\delta\rangle$ belong to $\mathcal{S}$.

2) There exists a set $\mathcal{S} = \mathcal{S}_0 \coprod \mathcal{S}_1$ of representatives for $\langle\gamma\rangle\backslash\Gamma$ such that:

(i) the set $\mathcal{S}_0$ contains a finite number of elements which are mapped by the isomorphism ψ to diagonal matrices of $\mathrm{PGL}_2(\mathbb{Q}_p)$;

(ii) if ϵ belongs to $\mathcal{S}_1$, then all the elements of the coset $\epsilon\langle\gamma\rangle$ belong to $\mathcal{S}_1$.

Proof. (Cf. [M], lemma 2.7)
1) Consider a decomposition of Γ as disjoint union of double cosets

$$\Gamma = \coprod_{\bar{\epsilon}\in\bar{\mathcal{S}}} \langle\gamma\rangle\bar{\epsilon}\langle\delta\rangle.$$

We claim that we may take $\mathcal{S}$ to be $\{\bar{\epsilon}\delta^m : \bar{\epsilon} \in \bar{\mathcal{S}},\ m \in \mathbb{Z}\}$. For, if $\bar{\epsilon}\delta^m = \gamma^r\bar{\epsilon}\delta^n$, we find $\delta^{m-n} = \bar{\epsilon}^{-1}\gamma^r\bar{\epsilon}$. Projecting this relation to $\bar{\Gamma}$ gives $m = n$.

2) Consider a decomposition of Γ as disjoint union of double cosets

$$\Gamma = \coprod_{\bar{\epsilon}\in\bar{\mathcal{S}}} \langle\gamma\rangle\bar{\epsilon}\langle\gamma\rangle.$$

Define $\mathcal{S}_1$ to be the set of elements of Γ of the form $\bar{\epsilon}\gamma^m$, $m \in \mathbb{Z}$, where $\bar{\epsilon} \in \bar{\mathcal{S}}$ is such that $\langle\gamma\rangle\bar{\epsilon}\gamma^n \neq \langle\gamma\rangle\bar{\epsilon}\gamma^m$ whenever $m \neq n$. As for $\mathcal{S}_0$, we claim that it can be taken to be the set of elements $\bar{\epsilon} \in \bar{\mathcal{S}}$ which do not satisfy the above condition. In such a case, there is a relation $\gamma^r\bar{\epsilon}\gamma^n = \bar{\epsilon}\gamma^m$ for integers r and $m \neq n$. Then, $\gamma^r = \bar{\epsilon}\gamma^{m-n}\bar{\epsilon}^{-1}$. By projecting this equality to $\bar{\Gamma}$, we see that $m-n = r$, and hence $\bar{\epsilon}$ and γ^r commute. Since γ^r is mapped by ψ to the diagonal matrix $\begin{pmatrix} \underline{w}^{\iota r} & 0 \\ 0 & 1 \end{pmatrix}$, where $\mathrm{ord}_p(\underline{w}) = k > 0$, a direct computation shows that $\bar{\epsilon}$ is also diagonal (and thus commutes with γ). Now consider the group of all the diagonal matrices in $\psi(\Gamma)$. Since Γ is discrete, this group is the product of a finite group by a cyclic group containing the group generated by γ. In conclusion, the set $\mathcal{S}_0$ is finite, and

$$\coprod_{\bar{\epsilon}\in\mathcal{S}_0} \langle\gamma\rangle\bar{\epsilon}\langle\gamma\rangle = \coprod_{\bar{\epsilon}\in\mathcal{S}_0} \langle\gamma\rangle\bar{\epsilon}.$$

The claim follows.

In the computation of $\underline{j}(\mathfrak{c})(\bar{\delta})$, we can assume that either

(I) $\mathfrak{c}$ and $\bar{\delta}$ are linearly independent, or

(II) $\bar{\delta} = \mathfrak{c}$.

(In fact, if the rank of $\bar{\Gamma}$ is > 1, it is enough to consider elements as in the first case, since the linear map $j(\mathfrak{c})$ is completely determined by the values $j(\mathfrak{c})(\bar{\delta})$, for $\mathfrak{c}$ and $\bar{\delta}$ linearly independent.) In the case (I), we use the notation $\mathcal{S}_1 := \mathcal{S}$, and the symbol $\mathcal{S}_1$ will always refer to a choice of representatives for $\langle\gamma\rangle\backslash\Gamma$ as in part 1 of proposition 7.4. In the case (II), the symbol $\mathcal{S} = \mathcal{S}_0 \coprod \mathcal{S}_1$ will stand for a choice of representatives as in part 2 of proposition 7.4.

Lemma 7.5
Let $\delta \in \Gamma$ be as in case (I) or (II) above. Then, the images in G_∞ by the reciprocity map of $j(\mathfrak{c})(\bar{\delta})$ and $\prod_{\epsilon\in\mathcal{S}_1} \epsilon\delta z_0/\epsilon z_0$ are equal.

Proof. In the case (I) there is nothing to prove. In the case (II), proposition 7.4 combined with a direct computation shows that

$$\prod_{\epsilon\in\mathcal{S}_0} \frac{\epsilon\gamma z_0}{\epsilon z_0} = \underline{w}^{\iota\#(\mathcal{S}_0)}.$$

Since $\underline{w}$ is in the kernel of the reciprocity map, the claim follows.

By lemma 7.5, we are now reduced to compute the product $\prod_{\epsilon\in\mathcal{S}_1} \epsilon\delta z_0/\epsilon z_0$, with δ as in case (I) or (II).

We begin with some preliminary remarks. Fix an edge e of level equal to an odd integer n, having v as its vertex of level n. Moreover, assume that the distance of v from v_0 is also equal to n. Note that the image in $\mathcal{M}$ of e is equal to the image in $\mathcal{M}$ of a Gross point of conductor cp^n.

Given $\tilde{\sigma} \in \tilde{G}_n$, define $\mu_{\tilde{\sigma}}$ to be equal to 1, resp. -1 if $\tilde{\sigma}v$ has odd, resp. even distance from v_0. If $\iota = 1$, observe that $\mu_{\tilde{\sigma}}$ depends only on the image $\bar{\sigma}$ of $\tilde{\sigma}$ in Σ under the projection induced by the reciprocity map; in this case, we write $\mu_{\bar{\sigma}}$ instead of $\mu_{\tilde{\sigma}}$. If $\iota = 2$, $\mu_{\tilde{\sigma}}$ is constant on the elements $\tilde{\sigma}$ which have the same image in Σ and p-adic valuation of the same parity; moreover, the values of $\mu_{\tilde{\sigma}}$ corresponding to different parities are opposite. In this case, if $\tilde{\sigma}$ projects in Σ to $\bar{\sigma}$ and $\mathrm{ord}_p(\tilde{\sigma})$ is even, we let $\mu_{\bar{\sigma}}$ stand for $\mu_{\tilde{\sigma}}$.

Given an edge d of $\mathcal{T}$, and $\tilde{\sigma} \in \tilde{G}_n$, write $\tilde{\sigma}e \equiv d$ if the edge $\tilde{\sigma}e$ is $\mathcal{S}_1$-equivalent to d, and $\sigma e \approx d$ if the element σe of $\mathcal{M}$ is Γ-equivalent to d. If $\iota = 1$, the relation $\tilde{\sigma}e \equiv d$ implies that $\sigma e \approx d$. If $\iota = 2$, $\tilde{\sigma}e \equiv d$ yields $\sigma e \approx d$ when $\mathrm{ord}_p(\tilde{\sigma})$ is even, and $\sigma e \approx wd$, with $w \in \Gamma_+ - \Gamma$, when $\mathrm{ord}_p(\tilde{\sigma})$ is odd.

Recall that ω_d denotes the order of the stabilizer in Γ of d.

Lemma 7.6
1) Suppose that $\iota = 1$. If the odd integer n is sufficiently large, the projection $\tilde{G}_n \to G_n$ induces a ω_d-to-1 map

$$\{\tilde{\sigma} \in \tilde{G}_n : \tilde{\sigma}e \equiv d\} \to \{\sigma \in G_n : \sigma e \approx d\}.$$

2) Suppose that $\iota = 2$. If the odd integer n is sufficiently large, the projection $\tilde{G}_n \to G_n$ induces ω_d-to-1 maps

$$\{\tilde{\sigma} \in \tilde{G}_n : \tilde{\sigma} e \equiv d,\ \mathrm{ord}_p(\tilde{\sigma}) \text{ even}\} \to \{\sigma \in G_n : \sigma e \approx d\}$$

and

$$\{\tilde{\sigma} \in \tilde{G}_n : \tilde{\sigma} e \equiv d,\ \mathrm{ord}_p(\tilde{\sigma}) \text{ odd}\} \to \{\sigma \in G_n : \sigma e \approx wd\}.$$

Proof.
1) Suppose that $\tilde{\sigma}_1 e \equiv d$ and $\tilde{\sigma}_2 e \equiv d$, i.e., $\tilde{\sigma}_1 e = \epsilon_1 d$ and $\tilde{\sigma}_2 e = \epsilon_2 d$, for ϵ_1 and ϵ_2 in $\mathcal{S}_1$. If $\tilde{\sigma}_1$ and $\tilde{\sigma}_2$ have the same image in G_n, then $\tilde{\sigma}_1 = \underline{w}^r \tilde{\sigma}_2$ for $r \in \mathbb{Z}$, and hence $\gamma^r \epsilon_2 d = \epsilon_1 d$. If $r \neq 0$, i.e., $\tilde{\sigma}_1 \neq \tilde{\sigma}_2$ and $\epsilon_1 \neq \epsilon_2$, then $\gamma^r \epsilon_2 \epsilon_1^{-1}$ is a non-trivial element of the stabilizer in Γ of $\epsilon_1 d$, which is a group of cardinality ω_d. Conversely, if $\tilde{\sigma}_1 e = \epsilon_1 d$ for $\epsilon_1 \in \mathcal{S}_1$ and if β is a non-trivial element of the stabilizer of $\epsilon_1 d$, we have $\tilde{\sigma}_1 e = \beta \epsilon_1 d$. Write $\beta \epsilon_1 = \gamma^r \epsilon_2$, $r \in \mathbb{Z}$, $\epsilon_2 \in \mathcal{S}$. Then $\epsilon_1 \neq \epsilon_2$. Note that if n is large, then ϵ_2 belongs to $\mathcal{S}_1$. We obtain $\underline{w}^{-r} \tilde{\sigma}_1 e = \epsilon_2 d$. This concludes the proof of part 1.

2) The proof is exactly the same as that of part 1.

Let
$$\mathrm{path}(v_0, \delta v_0) = d_1 - d_2 + \cdots + d_{s-1} - d_s \in \mathbb{Z}[\mathcal{E}(\mathcal{T})].$$
(Note that s is even, since δ belongs to Γ.) Write $d_j = \{v_j^e, v_j^o\}$, where v_j^e is the even vertex of d_j, and v_j^o is the odd vertex of d_j. Note that we have

$$\begin{aligned}
v_j^o &= v_{j+1}^o \quad \text{for} \quad j = 1, 3, \ldots, s-1, \\
v_j^e &= v_{j+1}^e \quad \text{for} \quad j = 2, 4, \ldots, s-2, \\
v_s^e &= \delta v_1^e.
\end{aligned}$$

Fix $z_0 \in \mathcal{H}_p(\mathbb{Q}_{p^2})$ such that $r(z_0) = v_0$. We may choose elements z_j^o and z_j^e in $\mathcal{H}_p(\mathbb{Q}_{p^2})$ such that $r(z_j^o) = v_j^o$, $r(z_j^e) = v_j^e$, and

$$\begin{aligned}
z_j^o &= z_{j+1}^o \quad \text{for} \quad j = 1, 3, \ \ldots, s-1, \\
z_j^e &= z_{j+1}^e \quad \text{for} \quad j = 2, 4, \ \ldots, s-2, \\
z_1^e &= z_0, \quad z_s^e = \delta z_0.
\end{aligned}$$

Hence

$$(\epsilon z_1^o)(\epsilon z_2^o)^{-1} \cdots (\epsilon z_{s-1}^o)(\epsilon z_s^o)^{-1} = 1, \quad (\epsilon z_2^e)(\epsilon z_3^e)^{-1} \cdots (\epsilon z_{s-2}^e)(\epsilon z_{s-1}^e)^{-1} = 1,$$

so that
$$\prod_{\epsilon \in \mathcal{S}_1} \frac{\epsilon \delta z_0}{\epsilon z_0} = \prod_{\epsilon \in \mathcal{S}_1} \left(\frac{\epsilon z_1^o}{\epsilon z_1^e}\right) \left(\frac{\epsilon z_2^o}{\epsilon z_2^e}\right)^{-1} \cdots \left(\frac{\epsilon z_s^o}{\epsilon z_s^e}\right)^{-1}.$$

Fix a large *odd* integer n. For each $1 \leq j \leq s$, let $\mathcal{S}(j)$ be the set of elements ϵ in $\mathcal{S}_1$ such that ϵd_j has level $\leq n$. Lemma 7.3 shows that the sets $\mathcal{S}(j)$ are finite. By lemma 7.1, we have the congruence

$$\prod_{\epsilon \in \mathcal{S}_1} \frac{\epsilon \delta z_0}{\epsilon z_0} \equiv \prod_{\epsilon \in \mathcal{S}(1)} \left(\frac{\epsilon z_1^o}{\epsilon z_1^e}\right) \prod_{\epsilon \in \mathcal{S}(2)} \left(\frac{\epsilon z_2^o}{\epsilon z_2^e}\right)^{-1} \cdots \prod_{\epsilon \in \mathcal{S}(s)} \left(\frac{\epsilon z_s^o}{\epsilon z_s^e}\right)^{-1} \pmod{p^n}. \tag{5}$$

Each of the factors in the right hand side of equation (5) can be broken up into three contributions:

$$\prod_{\mathcal{S}(j)} \frac{\epsilon z_j^o}{\epsilon z_j^e} = \prod_{\ell(\epsilon v_j^o)<n} \epsilon z_j^o \cdot \prod_{\ell(\epsilon v_j^e)<n} (\epsilon z_j^e)^{-1} \cdot \prod_{\ell(\epsilon d_j)=n} (\epsilon z_j^{\pi_j})^{\mu_j},$$

where $\pi_j = o$, resp. $\pi_j = e$ if the distance of the furthest vertex of ϵd_j from v_0 is odd, resp. even, and where we set $\mu_j = 1$ in the first case and $\mu_j = -1$ in the second case. By our choice of the set $\mathcal{S}_1$ as in proposition 7.4, the first two factors in this last expression cancel out in the formula (5). Hence we obtain

$$\prod_{\epsilon\in\mathcal{S}_1} \frac{\epsilon\delta z_0}{\epsilon z_0} \equiv \prod_{\ell(\epsilon d_1)=n} (\epsilon z_1^{\pi_1})^{\mu_1} \cdot \prod_{\ell(\epsilon d_2)=n} (\epsilon z_2^{\pi_2})^{-\mu_2} \cdots \prod_{\ell(\epsilon d_s)=n} (\epsilon z_s^{\pi_s})^{-\mu_s} \pmod{p^n}.$$

As in the remarks before lemma 7.6, let e be an edge of level n, such that its vertex v of level n has distance from v_0 also equal to n. Choose any $z \in \mathcal{H}_p(\mathbb{Q}_{p^2})$ with $r(z) = v$. Since $\tilde{G}_n$ acts simply transitively on the set of edges of level n, lemma 7.1 gives

$$\prod_{\epsilon\in\mathcal{S}_1} \frac{\epsilon\delta z_0}{\epsilon z_0} \equiv \prod_{\tilde{\sigma}e\equiv d_1} (\tilde{\sigma}z)^{\mu_{\tilde{\sigma}}} \cdot \prod_{\tilde{\sigma}e\equiv d_2} (\tilde{\sigma}z)^{-\mu_{\tilde{\sigma}}} \cdots \prod_{\tilde{\sigma}e\equiv d_s} (\tilde{\sigma}z)^{-\mu_{\tilde{\sigma}}} \pmod{p^n}.$$

By lemma 7.6, we obtain

$$\prod_{\epsilon\in\mathcal{S}_1} \frac{\epsilon\delta z_0}{\epsilon z_0} \equiv \prod_{\tilde{\sigma}e\equiv d_1} \tilde{\sigma}^{\mu_{\tilde{\sigma}}} \cdot \prod_{\tilde{\sigma}e\equiv d_2} \tilde{\sigma}^{-\mu_{\tilde{\sigma}}} \cdots \prod_{\tilde{\sigma}e\equiv d_s} \tilde{\sigma}^{-\mu_{\tilde{\sigma}}} \cdot (z^M) \pmod{p^n},$$

where

$$M = \begin{cases} \langle \text{path}(v_0, \delta v_0), \sum_{\sigma\in G_n} \mu_{\tilde{\sigma}}\sigma e\rangle & \text{if } \iota = 1 \\ \langle \text{path}(v_0, \delta v_0), \sum_{\sigma\in G_n} (\mu_{\tilde{\sigma}} - \mu_{\tilde{\sigma}} w)\sigma e\rangle & \text{if } \iota = 2. \end{cases}$$

By lemma 2.3, the duality $\langle\ ,\ \rangle$ induces a pairing on $H_1(\mathcal{G}, \mathbb{Z}) \times \mathcal{M}$. In the case $\iota = 1$, one sees directly that $\sum_{\sigma\in G_n} \mu_{\tilde{\sigma}}\sigma e$ has trivial image in $\mathcal{M}$, so that M is zero. Consider now the case $\iota = 2$. Since we are interested in computing $\underline{j}(\mathfrak{c})(\bar{\delta})$, we need only consider the image of the homomorphism $j(\mathfrak{c})$ in $\mathcal{N}_{\text{sp}} \otimes \mathbb{Q}_p^\times$. Thus, we may view the above pairing as being defined on $H_1(\mathcal{G}, \mathbb{Z})^- \times \mathcal{M}_{\text{sp}}$, where $H_1(\mathcal{G}, \mathbb{Z})^-$ indicates the "minus" eigenspace for the action of w on $H_1(\mathcal{G}, \mathbb{Z})$, and we may assume from now on that path$(v_0, \delta v_0)$ belongs to $H_1(\mathcal{G}, \mathbb{Z})^-$. One checks that the image $\iota \sum_{\sigma\in G_n} \mu_{\tilde{\sigma}}\sigma e$ in $\mathcal{M}_{\text{sp}}$ of the element $\sum_{\sigma\in G_n} (\mu_{\tilde{\sigma}} - w\mu_{\tilde{\sigma}})\sigma e$ is trivial, so that also in this case M is zero. Hence, in all cases

$$\prod_{\epsilon\in\mathcal{S}_1} \frac{\epsilon\delta z_0}{\epsilon z_0} \equiv \prod_{\tilde{\sigma}e\equiv d_1} \tilde{\sigma}^{\mu_{\tilde{\sigma}}} \cdot \prod_{\tilde{\sigma}e\equiv d_2} \tilde{\sigma}^{-\mu_{\tilde{\sigma}}} \cdots \prod_{\tilde{\sigma}e\equiv d_s} \tilde{\sigma}^{-\mu_{\tilde{\sigma}}} \pmod{p^n}.$$

Let $\text{rec}_{p,n} : \tilde{G}_\infty \to G_n$ be the composite of the reciprocity map with the natural projection of G_∞ onto G_n. Suppose that $\iota = 1$. By lemma 7.6, the above relation yields the equality in G_n:

$$\text{rec}_{p,n}\Big(\prod_{\epsilon\in\mathcal{S}_1} \frac{\epsilon\delta z_0}{\epsilon z_0}\Big) = \prod_{\sigma e\approx d_1} \sigma^{\omega_{d_1}\mu_{\bar{\sigma}}} \cdot \prod_{\sigma e\approx d_2} \sigma^{-\omega_{d_2}\mu_{\bar{\sigma}}} \cdots \prod_{\sigma e\approx d_s} \sigma^{-\omega_{d_s}\mu_{\bar{\sigma}}}.$$

Recall the derivative $\mathcal{L}'_{p,n}(\mathcal{N}_{\rm sp}/H, P_0) \in \mathcal{N}_{\rm sp} \otimes G_n$ defined in the formula (3) at the end of section 3. By the definition of the bijection κ of lemma 2.2, the right hand side of the above equality can be written as

$$\mathcal{L}'_{p,n}(\mathcal{N}_{\rm sp}/H, P_0)(\bar{\delta}) = \langle \mathrm{path}(v_0, \delta v_0), \sum_{g \in G_n} e_n(i)^g \otimes g^{-1} \rangle,$$

where, by an abuse of notation, $\sum_{g \in G_n} e_n(i)^g \otimes g^{-1}$ is viewed as an element of $\mathcal{M}_{\rm sp} \otimes G_n$. When $\iota = 2$, a similar computation shows that

$$\iota \mathcal{L}'_{p,n}(\mathcal{N}_{\rm sp}/H, P_0)(\bar{\delta}) = \mathrm{rec}_{p,n}(\prod_{\epsilon \in \mathcal{S}_1} \frac{\epsilon \delta z_0}{\epsilon z_0}).$$

By passing to the limit, one obtains in all cases

$$\iota \mathcal{L}'_{p}(\mathcal{N}_{\rm sp}/H, P_0)(\bar{\delta}) = \mathrm{rec}_{p}(\prod_{\epsilon \in \mathcal{S}_1} \frac{\epsilon \delta z_0}{\epsilon z_0}).$$

In other words, by definition of the map $\underline{j}$,

$$\mathcal{L}'_p(\mathcal{N}_{\rm sp}/H, P_0)^\iota = \underline{j}(\mathfrak{c}),$$

as was to be shown.

References

[**BC**] J-F. Boutot, H. Carayol, *Uniformization p-adique des courbes de Shimura: les théorèmes de Ceredník et de Drinfeld*, Astérisque **196-197** (1991) 45-158.

[**BD1**] M. Bertolini, H. Darmon, *Heegner points on Mumford-Tate curves,* Inv. Math. **126**, Fasc. 3 (1996) 413-453.

[**BD2**] M. Bertolini, H. Darmon, *Heegner points, p-adic L-functions and the Ceredník-Drinfeld uniformization*, Inv. Math., to appear.

[**Boi**] X. Boichut, *On the Mazur-Tate-Teitelbaum p-adic conjecture for elliptic curves with bad reduction at p,* in preparation.

[**BSDGP**] K. Barré-Sirieix, G. Diaz, F. Gramain, G. Philibert, *Une preuve de la conjecture de Mahler-Manin,* Inv. Math. **124** (1996) 1-9.

[**Cer**] I.V. Ceredník, *Uniformization of algebraic curves by discrete arithmetic subgroups of* $\mathrm{PGL}_2(k_w)$ *with compact quotient,* (in Russian) Math. Sbornik **100** (1976) 59-88. Transl. in Math. USSR. Sb. **29** (1976) 55-78.

[**Dag**] H. Daghigh, McGill University PhD thesis, in progress.

[**Dr**] V.G. Drinfeld, *Coverings of p-adic symmetric regions,* Funct. Anal. Appl. **10** (1976) 29-40.

[**Gr**] B.H. Gross, *Heights and special values of L-series,* CMS Conference Proceedings, H. Kisilevsky, J. Labute, Eds., **7** (1987).

[**GS**] R. Greenberg, G. Stevens, *p-adic L-functions and p-adic periods of modular forms,* Inv. Math. **111** (1993) 407-447.

[**GVdP**] L. Gerritzen, M. Van der Put, *Schottky groups and Mumford curves*, LNM 817, Springer, 1980.

[**GZ**] B.H. Gross, D. Zagier, *Heegner points and derivatives of L-series,* Inv. Math. **84** (1986) 225-320.

[**Kl**] C. Klingenberg, *On p-adic L-functions on Mumford curves,* In: p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture, B. Mazur and G. Stevens, eds., Contemporary Math. 165 (1991) 277-315.

[**KKT**] K. Kato, M. Kurihara, Tsuji, Forthcoming work.

[**JL**] H. Jacquet, R.P. Langlands, *Automorphic forms on* GL_2, LNM 114, Springer.

[**M**] Y.I. Manin, *p-adic automorphic functions,* J. Sov. Math. **5** (1976) 279-333.

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

[**RT**] K. Ribet, S. Takahashi, *Parametrization of elliptic curves by Shimura curves and by classical modular curves,* Proc. Nat. Acad. Sc. **94** (1997) 11110-11114.

[**Sch**] P. Schneider, *Rigid-analytic L-transforms,* In: Number Theory, Noordwijkerhout, LNM 1068, Springer, 1984.

[**Sh**] T. Shintani, *On the construction of holomorphic cusp forms of half integral weight,* Nagoya Math. J. **58** (1975) 83-126.

[**Se**] J-P. Serre, *Arbres, amalgames,* SL_2, Astérisque **46**, Soc. Math. de France, 1977.

[**T**] J. Teitelbaum, *Values of p-adic L-functions and a p-adic Poisson kernel,* Inv. Math. **101** (1990) 395-410.

[**Vi**] M-F. Vigneras, *Arithmétique des algèbres des quaternions,* LNM 800, Springer.