Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization

Massimo Bertolini[1]
Henri Darmon[2]

Contents

Acknowledgements. Work on this paper began while the second author was visiting the Università di Pavia, supported by a fellowship from the Consiglio Nazionale delle Ricerche (CNR). It was completed during a visit by the first author at the Institute for Advanced Study, funded partly by NSF grant DMS 9304580. Both authors gratefully acknowledge the financial support of the CNR, FCAR and NSERC, as well as the hospitality of the Institute for Advanced Study, Princeton University, and the Mathematical Sciences Research Institute in Berkeley.

Introduction

Let $E/\mathbb{Q}$ be a modular elliptic curve of conductor N, and let K be an imaginary quadratic field. Rankin's method gives the analytic continuation and functional equation for the Hasse-Weil L-function $L(E/K,s)$. When the sign of this functional equation is -1, a Heegner point α_K is defined on $E(K)$ using a modular curve or a Shimura curve parametrization of E.

In the case where all the primes dividing N are split in K, the Heegner point comes from a modular curve parametrization, and the formula of Gross-Zagier [GZ] relates its Néron-Tate canonical height to the first derivative of $L(E/K,s)$ at $s=1$. Perrin-Riou [PR] later established a p-adic analogue of the Gross-Zagier formula, expressing the p-adic height of α_K in terms of a derivative of the 2-variable p-adic L-function attached to E/K. At around the same time, Mazur, Tate and Teitelbaum

[1]Università di Pavia, Dipartimento di Matematica. E-mail: massimo@dragon.ian.pv.cnr.it
[2]McGill University, Mathematics Department. E-mail: darmon@math.mcgill.ca

[MTT] formulated a p-adic Birch and Swinnerton-Dyer conjecture for the p-adic L-function of E associated to the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and discovered that this L-function acquires an extra zero when p is a prime of split multiplicative reduction for E. The article [BD1] proposed analogues of the Mazur-Tate-Teitelbaum conjectures for the p-adic L-function of E associated to the anticyclotomic $\mathbb{Z}_p$-extension of K. In a significant special case, the conjectures of [BD1] predict a p-adic analytic construction of the Heegner point α_K from the first derivative of the anticyclotomic p-adic L-function. (Cf. conjecture 5.8 of [BD1].) The present work supplies a proof of this conjecture.

We state a simple case of our main result; a more general version is given in section 7. Assume from now on that N is relatively prime to disc(K), that E is semistable at all the primes which divide N and are inert in $K/\mathbb{Q}$, and that there is such a prime, say p. Let $\mathcal{O}_K$ be the ring of integers of K, and let $u_K := \frac{1}{2}\#\mathcal{O}_K^\times$. (Thus, $u_K = 1$ unless $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$.)

Note that the curve E/K_p has split multiplicative reduction, and thus is equipped with the Tate p-adic analytic uniformization

$$\Phi_{\mathrm{Tate}} : K_p^\times \longrightarrow E(K_p),$$

whose kernel is the cyclic subgroup of $K_p^\times$ generated by the Tate period $q \in p\mathbb{Z}_p$.

Let H be the Hilbert class field of K, and let H_∞ be the compositum of all the ring class fields of K of conductor a power of p. Write

$$G_\infty := \mathrm{Gal}(H_\infty/H), \quad \tilde{G}_\infty := \mathrm{Gal}(H_\infty/K), \quad \Delta := \mathrm{Gal}(H/K).$$

By class field theory, the group G_∞ is canonically isomorphic to $K_p^\times/\mathbb{Q}_p^\times\mathcal{O}_K^\times$, which can also be identified with a subgroup of the group $K_{p,1}^\times$ of elements of $K_p^\times$ of norm 1, by sending z to $(\frac{z}{\bar{z}})^{u_K}$, where $\bar{z}$ denotes the complex conjugate of z in $K_p^\times$.

A construction of [BD1], sec. 2.7 and 5.3, based on ideas of Gross [Gr], and recalled in section 2, gives an element $\mathcal{L}_p(E/K)$ in the completed *integral* group ring $\mathbb{Z}[\![\tilde{G}_\infty]\!]$ which interpolates the special values of the classical L-function of E/K twisted by complex characters of $\tilde{G}_\infty$. We will show (section 2) that $\mathcal{L}_p(E/K)$ belongs to the augmentation ideal $\tilde{I}$ of $\mathbb{Z}[\![\tilde{G}_\infty]\!]$. Let $\mathcal{L}'_p(E/K)$ denote the image of $\mathcal{L}_p(E/K)$ in $\tilde{I}/\tilde{I}^2 = \tilde{G}_\infty$. The reader should view $\mathcal{L}'_p(E/K) \in \tilde{G}_\infty$ as the first derivative of $\mathcal{L}_p(E/K)$ evaluated at the central point. One shows that the element $\mathcal{L}'_p(E/K)$ actually belongs to $G_\infty \subset \tilde{G}_\infty$, so that it can (and will) be viewed as an element of $K_p^\times$ of norm 1.

Using the theory of Jacquet-Langlands, and the assumption that E is modular, we will define a surjective map $\eta_f : J \longrightarrow \tilde{E}$, where $\tilde{E}$ is an elliptic curve isogenous to E over $\mathbb{Q}$, and J is the Jacobian of a certain Shimura curve X. The precise definitions of X, J, η_f and $\tilde{E}$ are given at the end of section 4. At the cost of possibly replacing E with an isogenous curve, we assume from now on in the introduction that $E = \tilde{E}$. (This will imply that E is the "strong Weil curve" for the Shimura curve parametrization.)

A special case of our main result is:

Theorem A
The local point $\Phi_{\mathrm{Tate}}(\mathcal{L}'_p(E/K))$ in $E(K_p)$ is a global point in $E(K)$.

When $\mathcal{L}_p'(E/K)$ is non-trivial, theorem A gives a construction of a rational point on $E(K)$ from the first derivative of the anticyclotomic p-adic L-function of E/K, in much the same way that the derivative at $s = 0$ of the Dedekind zeta-function of a real quadratic field leads to a solution of Pell's equation. A similar kind of phenomenon was discovered by Rubin [Ru] for elliptic curves with complex multiplication, with the exponential map on the formal group of E playing the role of the Tate parametrization. See also a recent result of Ulmer [U] for the universal elliptic curve over the function field of modular curves over finite fields.

We now state theorem A more precisely. In section 5, a Heegner point $\alpha_K \in E(K)$ is defined as the image by η_f of certain divisors supported on CM points of X. Let $\bar{\alpha}_K$ be the complex conjugate of α_K.

Theorem B
Let $w = 1$ (resp. $w = -1$) if $E/\mathbb{Q}_p$ has split (resp. non-split) multiplicative reduction. Then

$$\Phi_{\mathrm{Tate}}(\mathcal{L}_p'(E/K)) = \alpha_K - w\bar{\alpha}_K.$$

Theorem B, which relates the Heegner point α_K to the first derivative of a p-adic L-function, can be viewed as an analogue in the p-adic setting of the theorem of Gross-Zagier, and also of the p-adic formula of Perrin-Riou [PR]. Unlike these results, it does not involve heights of Heegner points, and gives instead a p-adic analytic construction of a Heegner point.

Observe that G_∞ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}/(p+1)\mathbb{Z}$, so that its torsion subgroup is of order $p + 1$. Choosing an anticyclotomic logarithm λ mapping G_∞ onto $\mathbb{Z}_p$ determines a map from $\mathbb{Z}[\![G_\infty]\!]$ to the formal power series ring $\mathbb{Z}_p[\![T]\!]$. Let $L_p(E/K)$ be the image of $\mathcal{L}_p(E/K)$ in $\mathbb{Z}_p[\![T]\!]$, and $L_p'(E/K)$ the derivative of $L_p(E/K)$ with respect to T evaluated at $T = 0$. Since Φ_{Tate} is injective on $K_{p,1}^\times$, theorem B implies:

Corollary C
The derivative $L_p'(E/K)$ is non-zero if and only if the point $\alpha_K - w\bar{\alpha}_K$ is of infinite order.

Corollary C gives a criterion in terms of the first derivative of a p-adic L-function for a Heegner point coming from a Shimura curve parametrization to be of infinite order. Work in progress of Keating and Kudla suggests that a similar criterion (involving the Heegner point α_K itself) can be formulated in terms of the first derivative of the classical L-function, in the spirit of the Gross-Zagier formula.

The work of Kolyvagin [Ko] shows that if α_K is of infinite order, then $E(K)$ has rank 1 and $\text{Ш}(E/K)$ is finite. By combining this with corollary C, one obtains

Corollary D
If $L_p'(E/K)$ is non-zero, then $E(K)$ has rank 1 and $\text{Ш}(E/K)$ is finite.

The formula of theorem B is a consequence of the more general result given in section 7, which relates certain Heegner divisors on jacobians of Shimura curves to derivatives of p-adic L-functions. The main ingredients in the proof of this theorem are (1) a construction, based on ideas of Gross, of the anticyclotomic p-adic L-function of E/K, (2) the explicit construction of [GVdP] of the p-adic Abel-Jacobi map for Mumford curves, and (3) the Cerednik-Drinfeld theory of p-adic uniformization of Shimura curves.

1 Quaternion algebras, upper half planes, and trees

Definite quaternion algebras

Let N^- be a product of an odd number of distinct primes, and let B be the (unique, up to isomorphism) definite quaternion algebra of discriminant N^-. Fix a maximal order $R \subset B$. (There are only finitely many such maximal orders, up to conjugation by $B^\times$.)

For each prime ℓ, we choose certain local orders in $B_\ell := B \otimes \mathbb{Q}_\ell$, as follows.

1. If ℓ is any prime which does not divide N^-, then B_ℓ is isomorphic to the algebra of 2×2 matrices $M_2(\mathbb{Q}_\ell)$ over $\mathbb{Q}_\ell$. Any maximal order of B_ℓ is isomorphic to $M_2(\mathbb{Z}_\ell)$, and all maximal orders are conjugate by $B_\ell^\times$. We fix the maximal order

$$R_\ell := R \otimes \mathbb{Z}_\ell.$$

2. If ℓ is a prime dividing N^-, then B_ℓ is the (unique, up to isomorphism) quaternion division ring over $\mathbb{Q}_\ell$. We let

$$R_\ell := R \otimes \mathbb{Z}_\ell,$$

as before. The valuation on $\mathbb{Z}_\ell$ extends uniquely to R_ℓ, and the residue field of R_ℓ is isomorphic to $\mathbb{F}_{\ell^2}$, the finite field with ℓ^2 elements. We fix an *orientation* of R_ℓ, i.e., an algebra homomorphism

$$\mathfrak{o}_\ell^- : R_\ell \longrightarrow \mathbb{F}_{\ell^2}.$$

Note that there are two possible choices of orientation for R_ℓ.

3. For each prime ℓ which does not divide N^-, and each integer $n \geq 1$, we also choose certain *oriented Eichler orders* of level ℓ^n. These are Eichler orders $\underline{R}_\ell^{(n)}$ of level ℓ^n contained in R_ℓ, together with an *orientation* of level ℓ^n, i.e., an algebra homomorphism

$$\mathfrak{o}_\ell^+ : \underline{R}_\ell^{(n)} \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z}.$$

We will sometimes write $\underline{R}_\ell$ for the oriented Eichler order $\underline{R}_\ell^{(1)}$ of level ℓ.

For each integer $M = \prod_i \ell_i^{n_i}$ which is prime to N^-, let $R(M)$ be the (oriented) Eichler order of level M in R associated to our choice of local Eichler orders:

$$R(M) := B \cap (\prod_{\ell \nmid M} R_\ell \prod_{\ell_i} \underline{R}_{\ell_i}^{(n_i)}).$$

We view $R(M)$ as endowed with the various local orientations $\mathfrak{o}_\ell^+$ and $\mathfrak{o}_\ell^-$ for the primes ℓ which divide MN^-, and call such a structure an *orientation* on $R(M)$. *We will usually view $R(M)$ as an oriented Eichler order, in what follows.*

Let $\hat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$ be the profinite completion of $\mathbb{Z}$, and let

$$\hat{B} := B \otimes \hat{\mathbb{Z}} = \prod_\ell B_\ell$$

be the adelization of B. Likewise, if R_0 is any order in B (not necessarily maximal), let $\hat{R}_0 := R_0 \otimes \hat{\mathbb{Z}}$.

The multiplicative group $\hat{B}^\times$ acts (on the left) on the set of all oriented Eichler orders of a given level M by the rule

$$b * R_0 := B \cap (b\hat{R}_0 b^{-1}), \quad b \in \hat{B}^\times, \quad R_0 \subset B.$$

(Note that $b * R_0$ inherits a natural orientation from the one on R_0.) This action of $\hat{B}^\times$ is transitive, and the stabilizer of the oriented order $R(M)$ is precisely $\hat{R}(M)^\times$. Hence the choice of $R(M)$ determines a description of the set of all oriented Eichler orders of level M, as the coset space $\hat{R}(M)^\times \backslash \hat{B}^\times$. Likewise, the conjugacy classes of oriented Eichler orders of level M are in bijection with the double coset space $\hat{R}(M)^\times \backslash \hat{B}^\times / B^\times$.

Let N^+ be an integer which is prime to N^-, and let p be a prime which does not divide N^+N^-. We set

$$N = N^+N^-p.$$

Let Γ be the group of elements in $R(N^+)[\frac{1}{p}]^\times$ of reduced norm 1. Of course, the definition of Γ depends on our choice of local orders, but:

Lemma 1.1
The group Γ depends on the choice of the R_ℓ and $\underline{R}_\ell^{(n)}$, only up to conjugation in $B^\times$.

Proof. This follows directly from strong approximation ([Vi], p. 61).

The p-adic upper half plane attached to B
Fix an unramified quadratic extension K_p of $\mathbb{Q}_p$. Define the *p-adic upper half plane* (attached to the quaternion algebra B) as follows:

$$\mathcal{H}_p := \mathrm{Hom}(K_p, B_p).$$

Remark. The group $\mathrm{GL}_2(\mathbb{Q}_p)$ acts naturally on $\mathbb{P}^1(K_p)$ by Möbius transformations, and the choice of an isomorphism $\eta : B_p \longrightarrow M_2(\mathbb{Q}_p)$ determines an identification of $\mathcal{H}_p$ with $\mathbb{P}^1(K_p) - \mathbb{P}^1(\mathbb{Q}_p)$. This identification sends $\psi \in \mathcal{H}_p$ to one of the two fixed points for the action of $\eta\psi(K_p^\times)$ on $\mathbb{P}^1(K_p)$. More precisely, it sends ψ to the unique fixed point $P \in \mathbb{P}^1(K_p)$ such that the induced action of $K_p^\times$ on the tangent line $T_P(\mathbb{P}^1(K_p)) = K_p$ is via the character $z \mapsto \frac{z}{\bar{z}}$. More generally, a choice of an embedding $B_p \longrightarrow M_2(K_p)$ determines an isomorphism of $\mathcal{H}_p$ with a domain Ω in $\mathbb{P}^1(K_p)$. In the literature, the p-adic upper half plane is usually defined to be $\mathbb{P}^1(\mathbb{C}_p) - \mathbb{P}^1(\mathbb{Q}_p) = \mathbb{C}_p - \mathbb{Q}_p$, where $\mathbb{C}_p$ is the completion of (an) algebraic closure of $\mathbb{Q}_p$. From this point of view, it might be more appropriate to think of $\mathcal{H}_p$ as the K_p-rational points of the p-adic upper half plane. But in this work, the role of the complex numbers in the p-adic context is always played, not by $\mathbb{C}_p$, but simply (and more naively) by the quadratic extension K_p.

We will try as much to possible to work with the more "canonical" definition of the upper half plane, which does not depend on a choice of embedding of B_p into $M_2(K_p)$. The upper half plane $\mathcal{H}_p$ is endowed with the following natural structures.

1. The group $B_p^\times$ acts naturally on the left on $\mathcal{H}_p$, by conjugation. This induces a natural action of the discrete group Γ on $\mathcal{H}_p$.

2. An involution $\psi \mapsto \bar{\psi}$, defined by the formula:

$$\bar{\psi}(z) := \psi(\bar{z}),$$

where $z \mapsto \bar{z}$ is the complex conjugation on K_p.

The Bruhat-Tits tree attached to B.

Let $\mathcal{T}$ be the Bruhat-Tits tree of $B_p^\times/\mathbb{Q}_p^\times$. The vertices of $\mathcal{T}$ correspond to maximal orders in B_p, and two vertices are joined by an edge if the intersection of the corresponding orders is an Eichler order of level p. An edge of $\mathcal{T}$ is a set of two adjacent vertices on $\mathcal{T}$, and an *oriented* edge of $\mathcal{T}$ is an ordered pair of adjacent vertices of $\mathcal{T}$. We denote the set of edges (resp. oriented edges) of $\mathcal{T}$ by $\mathcal{E}(\mathcal{T})$ (resp. $\vec{\mathcal{E}}(\mathcal{T})$).

The edges of $\mathcal{T}$ correspond to Eichler orders of level p, and the oriented edges are in bijection with the oriented Eichler orders of level p.

Since $\mathcal{T}$ is a tree, there is a distance function defined on the vertices of $\mathcal{T}$ in a natural way. We define the distance between a vertex v and an edge e to be the distance between v and the furthest vertex of e.

The group $B_p^\times$ acts on $\mathcal{T}$ via the rule

$$b * R_0 := bR_0b^{-1}, \quad b \in B_p^\times, \ R_0 \in \mathcal{T}.$$

This action preserves the distance on $\mathcal{T}$. In particular, the group Γ acts on $\mathcal{T}$ by isometries.

Fix a base vertex v_0 of $\mathcal{T}$. A vertex is said to be *even* (resp. *odd*) if its distance from v_0 is even (resp. odd). This notion determines an orientation on the edges of $\mathcal{T}$, by requiring that an edge always go from the even vertex to the odd vertex. The action of the group $B_p^\times$ does not preserve the orientation, but the subgroup of elements of norm 1 (or, more generally, of elements whose norm has even p-adic valuation) sends odd vertices to odd vertices, and even ones to even ones. In particular, the group Γ preserves the orientation we have defined on $\mathcal{T}$.

The reduction map

Let $\mathcal{O}_p$ be the ring of integers of K_p. Given $\psi \in \mathcal{H}_p$, the image $\psi(\mathcal{O}_p)$ is contained in a *unique* maximal order R_ψ of B_p. In this way, any $\psi \in \mathcal{H}_p$ determines a vertex R_ψ of $\mathcal{T}$. We call the map $\psi \mapsto R_\psi$ the *reduction map* from $\mathcal{H}_p$ to $\mathcal{T}$, and denote it

$$r : \mathcal{H}_p \longrightarrow \mathcal{T}.$$

For an alternate description of the reduction map r, note that the map ψ from K_p to B_p determines an action of $K_p^\times$ on the tree $\mathcal{T}$. The vertex $r(\psi)$ is the unique vertex which is fixed under this action.

The lattice $\mathcal{M}$

Let $\mathcal{G} := \mathcal{T}/\Gamma$ be the quotient graph. Since the action of Γ is orientation preserving, the graph $\mathcal{G}$ inherits an orientation from $\mathcal{T}$. Let $\mathcal{E}(\mathcal{G})$ be the set of (unordered) edges of $\mathcal{G}$, and let $\mathcal{V}(\mathcal{G})$ be its set of vertices. Write $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ and $\mathbb{Z}[\mathcal{V}(\mathcal{G})]$ for the modules of formal $\mathbb{Z}$-linear combinations edges and vertices of $\mathcal{G}$, respectively.

There is a natural boundary map ∂_* (compatible with our orientation)

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

which sends an edge $\{a, b\}$ to $a - b$, with the convention that a is the odd vertex and b is the even vertex in $\{a, b\}$. There is also a coboundary map

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

defined by

$$\partial^*(v) = \pm \sum_{\tilde{v} \in e} e,$$

where the sum is taken over the images in $\mathcal{E}(\mathcal{G})$ of the $p+1$ edges of $\mathcal{T}$ containing an arbitrary lift $\tilde{v}$ of v to $\mathcal{T}$. The sign in the formula for ∂^* is $+1$ if v is odd, and -1 if v is even.

Recall the canonical pairings defined by Gross [Gr] on $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ and on $\mathbb{Z}[\mathcal{V}(\mathcal{G})]$. If e is an edge (resp. v is a vertex) define w_e (resp. w_v) to be the order of the stabilizer for the action of Γ of (some) lift of e (resp. v) to $\mathcal{T}$. Then

$$\langle e_i, e_j \rangle = w_{e_i} \delta_{ij},$$

$$\langle\langle v_i, v_j \rangle\rangle = w_{v_i} \delta_{ij}.$$

Extend these pairings by linearity to the modules $\mathbb{Z}[(\mathcal{E}(\mathcal{G})]$ and $\mathbb{Z}[\mathcal{V}(\mathcal{G})]$.

Lemma 1.2
The maps ∂_* and ∂^* are adjoint with respect to the pairings $\langle\ ,\ \rangle$ and $\langle\langle\ ,\ \rangle\rangle$, i.e.,

$$\langle e, \partial^* v \rangle = \langle\langle \partial_* e, v \rangle\rangle.$$

Proof. By direct computation.

Define the module $\mathcal{M}$ as the quotient

$$\mathcal{M} := \mathbb{Z}[\mathcal{E}(\mathcal{G})]/\mathrm{image}(\partial^*).$$

Given two vertices a and b of $\mathcal{T}$, they are joined by a unique path, which may be viewed as an element of $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$ in the natural way. Note that because of our convention for orienting $\mathcal{T}$, if a and b are even vertices (say) joined by 4 consecutive edges e_1, e_2, e_3 and e_4, then the path from a to b is the formal sum

$$\mathrm{path}(a, b) = e_1 - e_2 + e_3 - e_4 \in \mathbb{Z}[\mathcal{E}(\mathcal{G})].$$

Note that we have the following properties of the path function:

$$\mathrm{path}(a, b) = -\mathrm{path}(b, a), \quad \mathrm{path}(a, b) + \mathrm{path}(b, c) = \mathrm{path}(a, c).$$

Also, if a and b are Γ-equivalent, then $\mathrm{path}(a, b)$ belongs to $H_1(\mathcal{G}, \mathbb{Z}) \subset \mathbb{Z}[\mathcal{E}(\mathcal{G})]$.

Proposition 1.3
The map from $\mathcal{M}$ to $\mathrm{Hom}(\Gamma, \mathbb{Z})$ which sends $m \in \mathcal{M}$ to the function

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

is injective and has finite cokernel.

Proof. The pairing $\langle\ ,\ \rangle$ gives an injective map with finite cokernel

$$\mathcal{M} \longrightarrow \mathrm{Hom}(\ker(\partial_*), \mathbb{Z}).$$

But

$$\ker(\partial_*) = H_1(\mathcal{G}, \mathbb{Z}).$$

Let Γ^{ab} denote the abelianization of Γ. Then the map of Γ^{ab} to $H_1(\mathcal{G}, \mathbb{Z})$ which sends γ to $\mathrm{path}(v_0, \gamma v_0)$ is an isomorphism modulo torsion (cf. [Se]). The proposition follows.

Relation of $\mathcal{M}$ with double cosets

We now give a description of $\mathcal{M}$ in terms of double cosets which was used in [BD1], sec. 1.4.

More precisely, let

$$J_{N^+p,N^-} = \mathbb{Z}[\hat{R}(N^+p)^\times \backslash \hat{B}^\times / B^\times]$$

be the lattice defined in [BD1], sec. 1.4. (By previous remarks, the module J_{N^+p,N^-} is identified with the free $\mathbb{Z}$-module

$$\mathbb{Z}R_1 \oplus \cdots \oplus \mathbb{Z}R_t$$

generated by the conjugacy classes of oriented Eichler orders of level N^+p in the quaternion algebra B.) Likewise, let

$$J_{N^+,N^-} = \mathbb{Z}[\hat{R}(N^+)^\times \backslash \hat{B}^\times / B^\times].$$

In [BD1], sec. 1.7, we defined two natural degeneracy maps

$$J_{N^+,N^-} \longrightarrow J_{N^+p,N^-},$$

and a module $J^{p-\mathrm{new}}_{N^+p,N^-}$ to be the quotient of J_{N^+p,N^-} by the image of $J_{N^+,N^-} \oplus J_{N^+,N^-}$ under these degeneracy maps.

Proposition 1.4
The choice of the oriented Eichler order $R(N^+p)$ determines an isomorphism between $\mathcal{M}$ and $J^{p-\mathrm{new}}_{N^+p,N^-}$.

The proof of proposition 1.4 uses the following lemma:

Lemma 1.5
There exists an element $\gamma \in R(N^+)[\frac{1}{p}]^\times$ whose reduced norm is an odd power of p.

Proof. Let F be an auxiliary imaginary quadratic field of prime discriminant such that all primes dividing N^+ are split in F and all primes dividing N^- are inert in F. Such an F exists, by Dirichlet's theorem on primes in arithmetic progressions. By genus theory, F has odd class number, and hence its ring of integers $\mathcal{O}_F$ contains an element a of norm p^k, with k odd. Fix an embedding of $\mathcal{O}_F$ in the Eichler order $R(N^+)$, and let γ be the image of a in $R(N^+)[\frac{1}{p}]^\times$.

Proof of proposition 1.4.
Recall that $\underline{R}_p \subset B_p$ denotes our fixed local Eichler order of level p. By strong approximation, we have

$$\hat{R}(N^+p)^\times \backslash \hat{B}^\times / B^\times = \underline{R}_p^\times \mathbb{Q}_p^\times \backslash B_p^\times / R(N^+)[\frac{1}{p}]^\times.$$

The group $\underline{R}_p^\times \mathbb{Q}_p^\times$ is the stabilizer of an ordered edge of $\mathcal{T}$. Hence $\underline{R}_p^\times \mathbb{Q}_p^\times \backslash B_p^\times$ is identified with the set $\vec{\mathcal{E}}(\mathcal{T})$ of ordered edges on $\mathcal{T}$, and the double coset space $R_p^\times \mathbb{Q}_p^\times \backslash B_p^\times / R(N^+)[\frac{1}{p}]^\times$ is identified with the set of ordered edges $\vec{\mathcal{E}}(\mathcal{G}_+)$ on the quotient graph $\mathcal{G}_+ := \mathcal{T}/R(N^+)[\frac{1}{p}]^\times$.

But the map which sends $\{x, y\} \in \mathcal{E}(\mathcal{G})$ to $(x, y) \in \vec{\mathcal{E}}(\mathcal{G}_+)$ if x is even, and to (y, x) if x is odd, is a bijection between $\mathcal{E}(\mathcal{G})$ and $\vec{\mathcal{E}}(\mathcal{G}_+)$. For, if $\{x, y\}$ and $\{x', y'\}$ have the same image in $\vec{\mathcal{E}}(\mathcal{G}_+)$, then there is an element of $R(N^+)[\frac{1}{p}]^\times$ which sends the odd vertex in $\{x, y\}$ to the odd vertex in $\{x', y'\}$ and the even vertex in $\{x, y\}$ to the even vertex in $\{x', y'\}$. This element is necessarily in Γ, since it sends an odd vertex to an odd vertex. Hence the edges $\{x, y\}$ and $\{x', y'\}$ are Γ-equivalent, and our map is one-one. To check surjectivity, let γ be the element of $R(N^+)[\frac{1}{p}]^\times$ given by lemma 1.5. Then the element (x, y) of $\vec{\mathcal{E}}(\mathcal{G}_+)$ is the image of $\{x, y\}$ if x is even and y is odd, and is the image of $\{\gamma x, \gamma y\}$ if x is odd and y is even. To sum up, we have shown that the choice of the Eichler order $R(N^+p)$ determines a canonical bijection between J_{N^+p,N^-} and $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$. Likewise, one shows that the Eichler order $R(N^+)$ determines a canonical bijection between J_{N^+,N^-} and the set of vertices $\mathcal{V}(\mathcal{G}_+)$, and between $J_{N^+,N^-} \oplus J_{N^+,N^-}$ and $\mathbb{Z}[\mathcal{V}(\mathcal{G})]$. (The resulting map from $\mathbb{Z}[\mathcal{V}(\mathcal{G}_+)] \oplus \mathbb{Z}[\mathcal{V}(\mathcal{G}_+)]$ to $\mathbb{Z}[\mathcal{V}(\mathcal{G})]$ sends a pair (v, w) to $v_+ - w_-$, where where v_+ and w_- are lifts of v and w to vertices of $\mathcal{G}$, which are even and odd respectively.) Finally, from the definition of the degeneracy maps given in [BD1] one checks that the following diagram commutes up to sign:

$$\begin{array}{ccc} J_{N^+,N^-} \oplus J_{N^+,N^-} & \longrightarrow & \mathbb{Z}[\mathcal{V}(\mathcal{G})] \\ \downarrow & & \downarrow \partial^* \\ J_{N^+p,N^-} & \longrightarrow & \mathbb{Z}[\mathcal{E}(\mathcal{G})] \end{array},$$

where the horizontal maps are the identifications we have just established, and the left vertical arrow is the difference of the two degeneracy maps. (Which is only well-defined up to sign). From this, it follows that $\mathcal{M} = \mathbb{Z}[\mathcal{E}(\mathcal{G})]/\mathrm{image}(\partial^*)$ is identified with the module

$$J_{N^+p,N^-}^{p-\mathrm{new}} = J_{N^+p,N^-}/\mathrm{image}(J_{N^+,N^-} \oplus J_{N^+,N^-})$$

of [BD1].

Hecke operators

The lattice $\mathcal{M}$ is equipped with a natural Hecke action, coming from its description in terms of double cosets. (Cf. [BD1], sec. 1.5.) Let $\mathbb{T}$ be the Hecke algebra acting on $\mathcal{M}$. Recall that $N = N^+N^-p$. The following is a consequence of the Eichler trace formula, and is a manifestation of the Jacquet-Langlands correspondence between automorphic forms on GL_2 and quaternion algebras.

Proposition 1.6

If $\phi : \mathbb{T} \longrightarrow \mathbb{C}$ is any algebra homomorphism, and $a_n = \phi(T_n)$ (for all n with $\gcd(n, N^-p) = 1$), then the a_n are the Fourier coefficients of a normalized eigenform of weight 2 for $\Gamma_0(N)$. Conversely, every normalized eigenform of weight 2 on $\Gamma_0(N)$ which is new at p and at the primes dividing N^- corresponds in this way to a character ϕ.

Given a normalized eigenform f on $X_0(N)$, denote by $\mathcal{O}_f$ the order generated by the Fourier coefficients of f and by K_f the fraction field of $\mathcal{O}_f$. Assuming that f is new at p and at N^-, let $\pi_f \in \mathbb{T} \otimes K_f$ be the idempotent associated to f by proposition 1.6. Let $n_f \in \mathcal{O}_f$ be such that $\eta_f := n_f\pi_f$ belongs to $\mathbb{T} \otimes \mathcal{O}_f$.

Let $\mathcal{M}^f \subset \mathcal{M} \otimes \mathcal{O}_f$ be the sublattice on which $\mathbb{T}$ acts via the character associated to f. The endomorphism η_f induces a map, still denoted η_f by an abuse of notation,

$$\eta_f : \mathcal{M} \to \mathcal{M}^f.$$

In particular, if f has integer Fourier coefficients, then $\mathcal{M}^f$ is isomorphic to $\mathbb{Z}$. Fixing such an isomorphism (i.e., choosing a generator of M^f), we obtain a map

$$\eta_f : \mathcal{M} \to \mathbb{Z},$$

which is well-defined up to sign.

2 The p-adic L-function

We recall the notations and assumptions of the introduction: E is a modular elliptic curve of conductor N, associated to an eigenform f on $\Gamma_0(N)$; K is a quadratic imaginary field of discriminant D relatively prime to N. Furthermore:

1. the curve E has good or multiplicative reduction at all primes which are inert in $K/\mathbb{Q}$;
2. there is at least one prime, p, which is inert in K and for which E has multiplicative reduction;
3. the sign in the functional equation for $L(E/K, s)$ is -1.

Write

$$N = N^+ N^- p,$$

where N^+, resp. N^- is divisible only by primes which are split, resp. inert in K. Note that by our assumptions, N^- is square-free and not divisible by p.

Lemma 2.1
Under our assumptions, N^- is a product of an odd number of primes.

Proof. By page 71 of [GZ], the sign in the functional equation of the complex L-function $L(E/K,s)$ is $(-1)^{\#\{\ell | N^- p\}+1}$. The result follows.

Let c be an integer prime to N. We modify slightly the notations of the introduction, letting H denote now the ring class field of K of conductor c, and H_n the ring class field of conductor cp^n. We write $H_\infty = \bigcup H_n$, and set

$$G_n := \mathrm{Gal}(H_n/H), \quad \tilde{G}_n := \mathrm{Gal}(H_n/K),$$

$$G_\infty := \mathrm{Gal}(H_\infty/H), \quad \tilde{G}_\infty := \mathrm{Gal}(H_\infty/K), \quad \Delta := \mathrm{Gal}(H/K).$$

(Thus, the situation considered in the introduction corresponds to the special case where $c = 1$.) There is an exact sequence of Galois groups

$$0 \longrightarrow G_\infty \longrightarrow \tilde{G}_\infty \longrightarrow \Delta \longrightarrow 0,$$

and, by class field theory, G_∞ is canonically isomorphic to $K_p^\times/\mathbb{Q}_p^\times \mathcal{O}_K^\times$.

The completed integral group rings $\mathbb{Z}[\![G_\infty]\!]$ and $\mathbb{Z}[\![\tilde{G}_\infty]\!]$ are defined as the inverse limits of the integral group rings $\mathbb{Z}[G_n]$ and $\mathbb{Z}[\tilde{G}_n]$ under the natural projection maps. We set

$$\mathcal{M}[G_n] := \mathcal{M} \otimes \mathbb{Z}[G_n],$$
$$\mathcal{M}[\![G_\infty]\!] := \lim_{\substack{\leftarrow \\ n}} \mathcal{M}[G_n] = \mathcal{M} \otimes \mathbb{Z}[\![G_\infty]\!],$$

and likewise for G_n and G_∞ replaced by $\tilde{G}_n$ and $\tilde{G}_\infty$. The groups G_∞ and $\tilde{G}_\infty$ act naturally on $\mathcal{M}[\![G_\infty]\!]$ and $\mathcal{M}[\![\tilde{G}_\infty]\!]$ by multiplication on the right.

In this section, we review the construction of a p-adic L-function $\mathcal{L}_p(\mathcal{M}/K)$, in a form adapted to the calculations we will perform later. A slightly modified version of this construction is given in section 2.7 of [BD1]. It is based on results of Gross [Gr] on special values of the complex L-functions attached to E/K, and on their generalization by Daghigh [Dag].

Let

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

be the complex period associated to the cusp form f. Write d for the discriminant of the order $\mathcal{O}$ of conductor c, u for one half the order of the group of units of $\mathcal{O}$ and n_f for the integer defined at the end of section 1 by the relation $\eta_f = n_f \pi_f$.

Theorem 2.2
There is an element $\mathcal{L}_p(\mathcal{M}/K) \in \mathcal{M}[\![\tilde{G}_\infty]\!]$, well-defined up to right multiplication by $\tilde{G}_\infty$, with the property that

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

for all finite order complex characters χ of $\tilde{G}_\infty$ and all modular forms f associated to $\mathbb{T}$ as in proposition 1.6.

Proof. See [Gr], [Dag] and [BD1], sec. 2.7.

Corollary 2.3
Setting

$$\mathcal{L}_p(E/K) := \eta_f(\mathcal{L}_p(\mathcal{M}/K)) \in \mathbb{Z}[\![\tilde{G}_\infty]\!],$$

where f is the modular form associated to E, one has

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

for all finite order characters χ of $\tilde{G}_\infty$.

Remark. One sees that the interpolation property of corollary 2.3 determines $\mathcal{L}_p(E/K)$ uniquely, up to right multiplication by elements in $\tilde{G}_\infty$, if it exists. The existence amounts to a statement of rationality and integrality for the special values $L(E/K,\chi,1)$. The construction of $\mathcal{L}_p(\mathcal{M}/K)$ (and hence, of $\mathcal{L}_p(E/K)$) is based on the notion of *Gross points* of conductor c and cp^n.

Gross points of conductor c

Recall that $\mathcal{O}$ is the order of conductor c in the maximal order $\mathcal{O}_K$, where we assume that c is prime to N. We equip $\mathcal{O}$ with an *orientation* of level N^+N^-, i.e., for each $\ell^n \| N^+$, an algebra homomorphism

$$\mathfrak{o}_\ell^+ : \mathcal{O} \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z},$$

and for each $\ell | N^-$, an algebra homomorphism

$$\mathfrak{o}_\ell^- : \mathcal{O} \longrightarrow \mathbb{F}_{\ell^2}.$$

An embedding $\xi : \mathcal{O} \longrightarrow R_\xi$ of $\mathcal{O}$ into an oriented Eichler order R_ξ of level dividing N^+ is called an *oriented embedding* if it respects the orientations on $\mathcal{O}$ and on R_ξ, i.e., if the diagrams

$$\begin{array}{ccc} \mathcal{O} & \xrightarrow{\xi} & R_\xi \\ \downarrow \mathfrak{o}_\ell^+ & & \downarrow \mathfrak{o}_\ell^+ \\ \mathbb{Z}/\ell^n\mathbb{Z} & = & \mathbb{Z}/\ell^n\mathbb{Z} \end{array} \qquad \begin{array}{ccc} \mathcal{O} & \xrightarrow{\xi} & R_\xi \\ \downarrow \mathfrak{o}_\ell^- & & \downarrow \mathfrak{o}_\ell^- \\ \mathbb{F}_{\ell^2} & = & \mathbb{F}_{\ell^2} \end{array}$$

commute, for all ℓ which divide N^+N^-.

The embedding ξ is called *optimal* if it does not extend to an embedding of any larger order into R_ξ. The group $B^\times$ acts naturally on the set of oriented optimal embeddings of conductor c, by conjugation:

$$b(R_\xi,\xi) := (bR_\xi b^{-1}, b\xi b^{-1}).$$

Definition 2.4

A *Gross point* of conductor c and level N^+N^- is a pair (R_ξ, ξ) where R_ξ is an oriented Eichler order of level N^+ in B, and ξ is an oriented optimal embedding of $\mathcal{O}$ into R_ξ, taken modulo conjugation by $B^\times$.

We denote by $\mathrm{Gr}(c)$ the set of all Gross points of conductor c and level N^+N^-.

Given $\xi \in \mathrm{Hom}(K, B)$, we denote by $\hat{\xi} \in \mathrm{Hom}(\hat{K}, \hat{B})$ the natural extension of scalars.

The group

$$\Delta = \mathrm{Pic}(\mathcal{O}) = \hat{\mathcal{O}}^\times \backslash \hat{K}^\times / K^\times$$

acts on the Gross points, by the rule

$$\sigma(R_\xi, \xi) := (\hat{\xi}(\sigma) * R_\xi, \xi).$$

Lemma 2.5
The group Δ acts simply transitively on the Gross points of conductor c.

Proof. See [Gr], sec. 3.

One says that (R_ξ, ξ) is in *normal form* if

$$\begin{aligned}
&R_\xi \otimes \mathbb{Z}_\ell = R_\ell \quad \text{for all } \ell \not| Np, \\
&R_\xi \otimes \mathbb{Z}_\ell = \underline{R}_\ell^{(n)} \quad \text{as oriented Eichler orders,} \quad \text{for all } \ell^n \| N^+, \\
&R_\xi \otimes \mathbb{Z}_\ell = R_\ell \quad \text{as oriented orders,} \quad \text{for all } \ell | N^-.
\end{aligned}$$

(Note in particular that we have imposed no condition on $R_\xi \otimes \mathbb{Z}_p$ in this definition.) Choose representatives (R_1, ψ_1), (R_2, ψ_2), ..., (R_h, ψ_h) for the Gross points of conductor c, written in normal form. (This can always be done, by strong approximation.) Note that

$$R_i[\frac{1}{p}] = R[\frac{1}{p}] \quad \text{as oriented Eichler orders,}$$

and that the orders R_i are completely determined by the local order $R_i \otimes \mathbb{Z}_p$. Let $v_1, \ldots, v_h$ be the vertices on $\mathcal{T}$ associated to the maximal orders $R_1 \otimes \mathbb{Z}_p$, ..., $R_h \otimes \mathbb{Z}_p$. The vertex v_i is equal to $r(\psi_i)$, i.e., it is the image of ψ_i (viewed as a point on $\mathcal{H}_p$ in the natural way) by the reduction map to $\mathcal{T}$.

Gross points of conductor cp^n

Let $n \geq 1$, and let $\mathcal{O}_n$ denote the order of K of conductor cp^n.

Definition 2.6
A *Gross point* of conductor cp^n and level N is a pair (R_ξ, ξ) where R_ξ is an oriented Eichler order of level N^+p in B, and ξ is an oriented optimal embedding of $\mathcal{O}_n$ into R_ξ, taken modulo conjugation by $B^\times$.

To make definition 2.6 complete, we need to clarify what we mean by an orientation at p of the optimal embedding ξ. (For the primes which divide N^+N^-, the meaning is exactly the same as before.) The oriented Eichler order $R_\xi \otimes \mathbb{Z}_p$ corresponds to an ordered edge on $\mathcal{T}$, whose source and target correspond to maximal orders R_1 and R_2 respectively. We require that ξ still be an optimal embedding of $\mathcal{O}_n$ into R_2. (It then necessarily extends to an optimal embedding of $\mathcal{O}_{n-1}$ into R_1.)

We let $\mathrm{Gr}(cp^n)$ be the set of Gross points of level cp^n, and we set

$$\mathrm{Gr}(cp^\infty) := \bigcup_{n=1}^{\infty} \mathrm{Gr}(cp^n).$$

The group $\tilde{G}_n = \hat{\mathcal{O}}_n^\times \backslash \hat{K}^\times / K^\times$ acts on $\mathrm{Gr}(cp^n)$ by the rule

$$\sigma(R_\xi, \xi) := (\hat{\xi}(\sigma) * R_\xi, \xi).$$

Lemma 2.7
The group $\tilde{G}_n$ acts simply transitively on $\mathrm{Gr}(cp^n)$.

Proof. See [Gr], sec. 3.

In particular, the group $\tilde{G}_\infty$ acts transitively on $\mathrm{Gr}(cp^\infty)$. As before, we say that a Gross point (R_ξ, ξ) of conductor cp^n is in *normal form* if

$$\begin{aligned}
&R_\xi \otimes \mathbb{Z}_\ell = R_\ell \quad \text{for all} \quad \ell \not| Np, \\
&R_\xi \otimes \mathbb{Z}_\ell = \underline{R}_\ell^{(n)} \quad \text{as oriented Eichler orders,} \quad \text{for all} \quad \ell^n \| N^+, \\
&R_\xi \otimes \mathbb{Z}_\ell = R_\ell \quad \text{as oriented orders,} \quad \text{for all} \quad \ell | N^-.
\end{aligned}$$

Recall the representatives (R_1, ψ_1), ...,(R_h, ψ_h) for the Gross points of conductor c that were chosen in the previous paragraph.

Lemma 2.8
Every point in $\mathrm{Gr}(cp^\infty)$ is equivalent to an element in normal form, and can be written as (R_0, ψ_i), where $\psi_i \in \{\psi_1, \ldots, \psi_h\}$, and $R_0 \otimes \mathbb{Z}_p$ is an oriented Eichler order of level p. A point in $\mathrm{Gr}(cp^\infty)$ described by a pair (R_0, ψ_i) is of level cp^n, where n is the distance between the edge associated to R_0 on $\mathcal{T}$, and the vertex associated to R_i.

Proof. The first statement follows from strong approximation, and the second from a direct calculation.

By lemma 2.8, the set $\mathrm{Gr}(cp^\infty)$ can be described by the system of representatives

$$\mathcal{E}(\mathcal{T}) \times \{\psi_1, \ldots, \psi_h\}.$$

The action of $G_\infty = K_p^\times / \mathbb{Q}_p^\times$ on $\mathrm{Gr}(cp^\infty)$ in this description is simply

$$\sigma(R_0, \psi_i) := (\hat{\psi}_i(\sigma) * R_0, \psi_i).$$

Construction of $\mathcal{L}_p(\mathcal{M}/K)$

Choose one of the representatives of $\mathrm{Gr}(c)$, say, (v_1, ψ_1). Choose an *end* of $\mathcal{T}$ originating from v_1, i.e., a sequence $e_1, e_2, \ldots, e_n, \ldots$ of consecutive edges originating from v_1. By lemma 2.8, the Gross points (e_n, ψ_1) are a sequence of Gross points of conductor cp^n. Consider the formal expression

$$(-1)^n \sum_{\sigma \in \tilde{G}_n} \sigma(e_n, \psi_1) \cdot \sigma^{-1}$$

and let $\mathcal{L}_{p,n}(\mathcal{M}/K)$ denote its natural image in $\mathcal{M}[\tilde{G}_n]$.

Lemma 2.9

The elements $\mathcal{L}_{p,n}(\mathcal{M}/K)$ $(n \geq 1)$ are compatible under the natural projection maps $\mathcal{M}[\tilde{G}_{n+1}] \longrightarrow \mathcal{M}[\tilde{G}_n]$.

Proof. This follows directly from the definiton of the action of $\tilde{G}_n$ on $\mathrm{Gr}(cp^n)$ given above, and from the definition of the coboundary map ∂^*. They yield that the formal expression $\mathrm{Norm}_{K_{n+1}/K_n}(e_{n+1}, \psi_1) + (e_n, \psi_1)$ is in the image of the coboundary map ∂^*, and hence is zero in $\mathcal{M}$. The lemma follows.

Lemma 2.9 implies that we can define an element

$$\mathcal{L}_p(\mathcal{M}/K) \in \mathcal{M}[\![\tilde{G}_\infty]\!]$$

by taking inverse limit of the $\mathcal{L}_{p,n}(\mathcal{M}/K)$ via the projections $\mathcal{M}[G_{n+1}] \to \mathcal{M}[G_n]$.

The element $\mathcal{L}_p(\mathcal{M}/K)$ satisfies the conclusions of theorem 2.2. It should be thought of as a p-adic L-function (or rather, the square root of a p-adic L-function) over K, associated to modular forms for $\mathbb{T}$. If f is any such modular form, then the element $\eta_f \mathcal{L}_p(\mathcal{M}/K)$ is equal to the element $\theta_{N_*^+, N_*^-}$ defined in [BD1], sec. 5.3 (in the special case when f has rational coefficients).

Note that $\mathcal{L}_p(\mathcal{M}/K)$ depends on the choice of the initial point (v_1, ψ_1), and on the end $e_1, \ldots, e_n, \ldots$ of $\mathcal{T}$ originating from v_1, but only up to multiplication (on the right) by an element of $\tilde{G}_\infty$.

Recall the augmentation ideal I of $\mathbb{Z}[\![\tilde{G}_\infty]\!]$ described in the introduction. More generally, let I_Δ be the kernel of the augmentation map $\mathbb{Z}[\![\tilde{G}_\infty]\!] \longrightarrow \mathbb{Z}[\Delta]$.

Lemma 2.10

$\mathcal{L}_p(\mathcal{M}/K)$ belongs to $\mathcal{M} \otimes I$. In fact, $\mathcal{L}_p(\mathcal{M}/K)$ belongs to $\mathcal{M} \otimes I_\Delta$.

Proof. Since Δ acts simply transitively on $(v_1, \psi_1), \ldots, (v_h, \psi_h)$, let σ_i be the element such that

$$\sigma_i v_1 = v_i.$$

Let I_Δ denote, by abuse of notation, the image of I_Δ in $\mathbb{Z}[\tilde{G}_n]$. Note that we have the canonical isomorphisms

$$\mathbb{Z}[\![\tilde{G}_\infty]\!]/I_\Delta = \mathbb{Z}[\tilde{G}_n]/I_\Delta = \mathbb{Z}[\Delta].$$

By the compatibility lemma 2.9, the image of $\mathcal{L}_p(\mathcal{M}/K)$ in $\mathcal{M}[[\tilde{G}_\infty]]/I_\Delta$ is equal to the image of $\mathcal{L}_{p,1}(\mathcal{M}/K)$ in $\mathcal{M}[G_1]/I_\Delta = \mathcal{M}[\Delta]$, which is equal to:

$$\sum_{i=1}^{h} (\sum_{v_i \in e} e) \cdot \sigma_i^{-1}.$$

But each of the terms in the inner sum belongs to the image of ∂^*, and hence is 0 in $\mathcal{M}$. Thus, $\mathcal{L}_p(\mathcal{M}/K)$ belongs to $\mathcal{M}\otimes I_\Delta$, and also to $\mathcal{M}\otimes I$, since $I_\Delta\subset I$.

Remark. If χ is any character of Δ and f is any modular form attached to $\mathbb{T}$, then the functional equation of $L(f/K,\chi,s)$ has sign -1, and hence $L(f/K,\chi,1)=0$ for all such characters. The interpolation formula of theorem 2.2 implies then that $\mathcal{L}_p(\mathcal{M}/K)$ belongs to I_Δ. The point of the proof of lemma 2.10 is that the construction of $\mathcal{L}_p(\mathcal{M}/K)$ also implies this directly, without using the relation with L-function values.

Let

$$\mathcal{L}'_p(\mathcal{M}/K)\in\mathcal{M}\otimes(I/I^2)=\mathcal{M}\otimes\tilde{G}_\infty$$

and

$$\mathcal{L}'_p(\mathcal{M}/H)\in\mathcal{M}\otimes(I_\Delta/I_\Delta^2)=\mathcal{M}[\Delta]\otimes G_\infty=\mathcal{M}[\Delta]\otimes(K_{p,1}^\times)$$

be the natural images of the element $\mathcal{L}_p(\mathcal{M}/K)$. Since $\mathcal{L}_p(\mathcal{M}/K)$ is well-defined up to right multiplication by $\tilde{G}_\infty$, the element $\mathcal{L}'_p(\mathcal{M}/K)$ is canonical, and does not depend on the choice of (v_1,ψ_1) or on the choice of the end of $\mathcal{T}$ originating from v_1. The element $\mathcal{L}'_p(\mathcal{M}/H)$ is well defined, up to right multiplication by an element of Δ.

We now give an explicit description of $\mathcal{L}'_p(\mathcal{M}/K)$ and $\mathcal{L}'_p(\mathcal{M}/H)$ in $\mathrm{Hom}(\Gamma,K_{p,1}^\times)$ which will be used in the calculations of section 6 and 7. Let ψ be any point in $\mathcal{H}_p$, corresponding to a local embedding of K_p into B_p. The embedding ψ gives rise to an action of $K_p^\times/\mathbb{Q}_p^\times$ on the tree $\mathcal{T}$ by multiplication on the right, fixing the vertex $v_0:=r(\psi)$. Choose a sequence of ends $e_1,\ldots,e_n,\ldots$ originating from v_0, and let

$$\mathcal{L}'_{p,n}(\psi)=(-1)^n\sum_{\sigma\in G_n}\psi(\sigma)(e_n)\otimes\sigma^{-1}$$

be the element of $\mathcal{M}\otimes G_n$ (here we denote by e_n the element in $\mathcal{M}$ associated to the edge e_n). The elements $\mathcal{L}'_{p,n}(\psi)$ are compatible under the obvious projection maps $\mathcal{M}\otimes G_{n+1}\longrightarrow\mathcal{M}\otimes G_n$, and hence the element $\mathcal{L}'_p(\psi)\in\mathcal{M}\otimes G_\infty$ can be defined as the inverse limit of the $\mathcal{L}'_{p,n}(\psi)$ under the natural projections. By proposition 1.3, we may view $\mathcal{L}'_p(\psi)$ as an element of $\mathrm{Hom}(\Gamma,K_{p,1}^\times)$, given by

$$\mathcal{L}'_p(\psi)(\delta)=\lim_{\substack{\leftarrow\\ n}}\langle\mathrm{path}(v_0,\delta v_0),\mathcal{L}'_{p,n}(\psi)\rangle\in G_\infty=K_{p,1}^\times,\qquad\forall\delta\in\Gamma.$$

In this notation, we have

$$\mathcal{L}'_p(\mathcal{M}/K)=\sum_{i=1}^h\mathcal{L}'_p(\psi_i),$$

$$\mathcal{L}'_p(\mathcal{M}/H)=\sum_{\sigma\in\Delta}\mathcal{L}'_p(\psi_1^\sigma)\sigma^{-1}.$$

3 Generalities on Mumford curves

Following [Jo-Li], we call a smooth complete curve X over K_p an *admissible curve over* K_p if it admits a model $\mathcal{X}$ over the ring of integers $\mathcal{O}_p$ of K_p, such that:

(i) the scheme $\mathcal{X}$ is proper and flat over $\mathcal{O}_p$;

(ii) the irreducible components of the special fiber $\mathcal{X}_{(p)}$ are rational and defined over $\mathcal{O}_p/(p) \simeq \mathbb{F}_{p^2}$, and the singularities of $\mathcal{X}_{(p)}$ are ordinary double points defined over $\mathcal{O}_p/(p)$;

(iii) if $x \in \mathcal{X}_{(p)}$ is a singular point, then the completion $\hat{\mathcal{O}}_{\mathcal{X},x}$ of the local ring $\mathcal{O}_{\mathcal{X},x}$ is $\mathcal{O}$-isomorphic to the completion of the local ring $\mathcal{O}[\![X,Y]\!]/(XY-p^m)$ for a positive integer m.

Let Γ be a finitely generated subgroup of $\mathrm{PGL}_2(K_p)$, acting on $\mathbb{P}^1(\mathbb{C}_p)$ by Möbius transformations. A point $z \in \mathbb{P}^1(\mathbb{C}_p)$ is said to be a *limit point* for the action of Γ if it is of the form $z = \lim g_n(z_0)$ for a sequence of distinct elements g_n of Γ. Let $\mathcal{I} \subset \mathbb{P}^1(\mathbb{C}_p)$ denote its set of limit points and let $\Omega_p = \mathbb{P}^1(K_p) - \mathcal{I}$. The group Γ is said to act *discontinuously*, or to be a *discontinuous group*, if $\Omega_p \neq \emptyset$. A fundamental result of Mumford, extended by Kurihara, establishes a 1-1 correspondence between conjugacy classes of discontinuous groups and admissible curves.

Theorem 3.1
Given an admissible curve X over K_p, there exists a discontinuous group $\Gamma \subset \mathrm{PGL}_2(K_p)$, unique up to conjugation, such that $X(K_p)$ is isomorphic to Ω_p/Γ. Conversely, any such quotient is an admissible curve over K_p.

Proof. See [Mu] and [Ku].

If $D = P_1 + \cdots + P_r - Q_1 - \cdots - Q_r \in \mathrm{Div}^0(\Omega_p)$ is a divisor of degree zero on Ω_p, define the theta function

$$\theta(z; D) = \prod_{\gamma\in\Gamma} \frac{(z-\gamma P_1)\cdots(z-\gamma P_r)}{(z-\gamma Q_1)\cdots(z-\gamma Q_r)},$$

with the convention that $z - \infty = 1$.

Let $\Gamma_{\mathrm{ab}} := \Gamma/[\Gamma,\Gamma]$ be the abelianization of Γ, and let $\bar{\Gamma} := \Gamma_{\mathrm{ab}}/(\Gamma_{\mathrm{ab}})_{\mathrm{tor}}$ be its maximal torsion-free quotient.

Lemma 3.2
There exists $\phi_D \in \mathrm{Hom}(\Gamma, K_p^\times)$ such that $\theta(\delta z; D) = \phi_D(\delta)\theta(z; D)$, for all δ in Γ. Furthermore, the map ϕ_D factors through $\bar{\Gamma}$, so that ϕ_D can be viewed as an element of $\mathrm{Hom}(\bar{\Gamma}, K_p^\times)$.

Proof. See [GVdP], p. 47, (2.3.1), and ch. VIII, prop. (2.3).

Let

$$\Phi_{\mathrm{AJ}} : \mathrm{Div}^0(\Omega_p) \longrightarrow \mathrm{Hom}(\bar{\Gamma}, K_p^\times)$$

be the map which associates to the degree zero divisor D the automorphy factor ϕ_D. The reader should think of this map as a p-adic Abel-Jacobi map.

Given $\delta \in \Gamma$, the number $\phi_{(z)-(\delta z)}(\beta)$ does not depend on the choice of $z \in \Omega_p$, and depends only on the image of α and β in $\bar{\Gamma}$. Hence it gives rise to a well-defined pairing

$$(\; , \;) : \bar{\Gamma} \times \bar{\Gamma} \to K_p^\times.$$

Lemma 3.3
The pairing $(\; , \;)$ *is bilinear, symmetric, and positive definite (i.e.,* $\mathrm{ord}_p \circ (\; , \;)$ *is positive definite). Hence, the induced map*

$$j : \bar{\Gamma} \to \mathrm{Hom}(\bar{\Gamma}, K_p^\times)$$

is injective and has discrete image.

Proof. See [GVdP], VI.2. and VIII.3.

Given a divisor D of degree zero on $X(K_p) = \Omega_p/\Gamma$, let $\tilde{D}$ denote an arbitrary lift to a degree zero divisor on Ω_p. Let $\Lambda := j(\bar{\Gamma})$. The automorphy factor $\phi_{\tilde{D}}$ depends on the choice of $\tilde{D}$, but its image in $\mathrm{Hom}(\bar{\Gamma}, K_p^\times)/\Lambda$ depends only on D. Thus Φ_{AJ} induces a map $\mathrm{Div}^0(X(K_p)) \longrightarrow \mathrm{Hom}(\bar{\Gamma}, K_p^\times)/\Lambda$, which we also call Φ_{AJ} by abuse of notation.

Proposition 3.4
The map $\mathrm{Div}^0(X(K_p)) \longrightarrow \mathrm{Hom}(\bar{\Gamma}, K_p^\times)/\Lambda$ *defined above is trivial on the group of principal divisors, and induces an identification of the* K_p*-rational points of the jacobian* J *of* X *over* K_p *with* $\mathrm{Hom}(\bar{\Gamma}, K_p^\times)/\Lambda$.

Proof. See [GVdP], VI.2. and VIII.4.

To sum up, we have:

Corollary 3.5
The diagram

$$\begin{array}{ccc} \mathrm{Div}^0(\Omega_p) & \xrightarrow{\Phi_{\mathrm{AJ}}} & \mathrm{Hom}(\bar{\Gamma}, K_p^\times) \\ \downarrow & & \downarrow \\ \mathrm{Div}^0(X(K_p)) & \xrightarrow{\Phi_{\mathrm{AJ}}} & J(K_p) \end{array}$$

commutes.

4 Shimura curves

Let $\mathcal{B}$ be the indefinite quaternion algebra of discriminant N^-p, and let $\mathcal{R}$ be an (oriented) maximal order in $\mathcal{B}$ (which is unique up to conjugation). Likewise, for each M prime to N^-p, choose an oriented Eichler order $\mathcal{R}(M)$ of level M contained in $\mathcal{R}$.

Let X be the Shimura curve associated to the Eichler order $\mathcal{R}(N^+)$, as in [BD1], sec. 1.3.

I Moduli description of X

The curve $X/\mathbb{Q}$ is a moduli space for abelian surfaces with quaternionic multiplication and N^+-level structure. More precisely, the curve $X/\mathbb{Q}$ coarsely represents the functor $\mathcal{F}_\mathbb{Q}$ which associates to every scheme S over $\mathbb{Q}$ the set of isomorphism classes of triples (A, i, C), where

1. A is an abelian scheme over S of relative dimension 2;
2. $i : \mathcal{R} \to \mathrm{End}_S(A)$ is an inclusion defining an action of $\mathcal{R}$ on A;
3. C is an N^+-level structure, i.e., a subgroup scheme of A which is locally isomorphic to $\mathbb{Z}/N^+\mathbb{Z}$ and is stable and locally cyclic under the action of $\mathcal{R}(N^+)$.

See [BC], ch. III and [Rob] for more details.

Remarks

1. The datum of the level N^+ structure is equivalent to the data, for each $\ell^n \| N^+$, of a subgroup C_ℓ which is locally isomorphic to $\mathbb{Z}/\ell^n\mathbb{Z}$ and is locally cyclic for the action of $\mathcal{R}(N^+)$.

2. For each ℓ dividing N^-p, let $I \subset \mathcal{R}_\ell$ be the maximal ideal of $\mathcal{R}_\ell$. The subgroup scheme A_I of points in A killed by I is a free $\mathcal{R}_\ell/I \simeq \mathbb{F}_{\ell^2}$-module of rank one, and the orientation $\mathfrak{o}_\ell^- : \mathcal{R}_\ell \longrightarrow \mathbb{F}_{\ell^2}$ allows us to view A_I canonically as a one-dimensional $\mathbb{F}_{\ell^2}$-vector space.

II Complex analytic description of X

Let

$$\mathcal{B}_\infty := \mathcal{B} \otimes \mathbb{R} \simeq M_2(\mathbb{R}).$$

Define the *complex upper half plane* associated to $\mathcal{B}$ to be

$$\mathcal{H}_\infty := \mathrm{Hom}(\mathbb{C}, \mathcal{B}_\infty).$$

Note that a choice of isomorphism $\eta : \mathcal{B}_\infty \longrightarrow M_2(\mathbb{R})$ determines an isomorphism of $\mathcal{H}_\infty$ with the union $\mathbb{C} - \mathbb{R}$ of the "usual" complex upper half plane

$$\{z \in \mathbb{C} : \mathrm{Im} z > 0\}$$

with the complex lower half plane, by sending $\psi \in \mathrm{Hom}(\mathbb{C}, \mathcal{B}_\infty)$ to the unique fixed point P of $\eta\psi(\mathbb{C}^\times)$ such that the induced action of $\mathbb{C}^\times$ on the complex tangent line $T_P(\mathbb{C} - \mathbb{R}) = \mathbb{C}$ is by the character $z \mapsto \frac{z}{\bar{z}}$.

Let $\Gamma_\infty = \mathcal{R}(N^+)^\times$ be the group of invertible elements in $\mathcal{R}(N^+)$ (i.e., having reduced norm equal to ± 1). This group acts naturally on $\mathcal{H}_\infty$ via the action of $\mathcal{B}_\infty^\times$ by conjugation.

Proposition 4.1
The Shimura curve X over $\mathbb{C}$ is isomorphic to the quotient of the complex upper half plane $\mathcal{H}_\infty$ attached to $\mathcal{B}_\infty$ by the action of Γ_∞, i.e.,

$$X(\mathbb{C}) = \mathcal{H}_\infty/\Gamma_\infty.$$

Proof. See [BC], ch. III, and [Rob].

In particular, an abelian surface A over $\mathbb{C}$ with quaternionic multiplications by $\mathcal{R}$ and level N^+ structure determines a point $\psi \in \mathcal{H}_\infty = \mathrm{Hom}(\mathbb{C}, \mathcal{B}_\infty)$ which is well-defined modulo the natural action of Γ_∞. We will now give a description of the assignment $A \mapsto \psi$. Although not used in the sequel, this somewhat non-standard description of the complex uniformization is included to motivate the description of the p-adic uniformization of X which follows from the work of Cerednik and Drinfeld.

The complex upper half plane as a moduli space. We first give a "moduli" description of the complex upper half plane $\mathcal{H}_\infty := \mathrm{Hom}(\mathbb{C}, \mathcal{B}_\infty)$ as classifying complex vector spaces with quaternionic action and a certain "rigidification".

Definition 4.2
A *quaternionic space* (attached to $\mathcal{B}_\infty$) is a two-dimensional complex vector space V equipped with a (left) action of $\mathcal{B}_\infty$, i.e., an injective homomorphism $i : \mathcal{B}_\infty \longrightarrow \mathrm{End}_{\mathbb{C}}(V)$.

Let $V_{\mathbb{R}}$ be the 4-dimensional real vector space underlying V.

Lemma 4.3
The algebra $\mathrm{End}_{\mathcal{B}_\infty}(V_{\mathbb{R}})$ *is isomorphic (non-canonically) to* $\mathcal{B}_\infty$.

Proof. The natural map

$$\mathcal{B}_\infty \otimes \mathrm{End}_{\mathcal{B}_\infty}(V_{\mathbb{R}}) \longrightarrow \mathrm{End}_{\mathbb{R}}(V_{\mathbb{R}}) \simeq M_4(\mathbb{R})$$

is an isomorphism, and hence $\mathrm{End}_{\mathcal{B}_\infty}(V_{\mathbb{R}})$ is abstractly isomorphic to the algebra $\mathcal{B}_\infty$.

Definition 4.4
A *rigidification* of the quaternionic space V is an isomorphism

$$\rho : \mathcal{B}_\infty \longrightarrow \mathrm{End}_{\mathcal{B}_\infty}(V_{\mathbb{R}}).$$

A pair (V, ρ) consisting of a quaternionic space V and a rigidification ρ is called a *rigidified quaternionic space.*

There is a natural notion of isomorphism between rigidified quaternionic spaces.

Proposition 4.5
There is a canonical bijection betwen $\mathcal{H}_\infty$ *and the set of isomorphism classes of rigidified quaternionic spaces.*

Proof. Given $\psi \in \mathcal{H}_\infty = \mathrm{Hom}(\mathbb{C}, \mathcal{B}_\infty)$, we define a rigidified quaternionic space as follows. Let $V = \mathcal{B}_\infty$, viewed as a two-dimensional complex vector space by the rule

$$\lambda v := v\psi(\lambda), \qquad v \in V, \quad \lambda \in \mathbb{C}.$$

The left multiplication by $\mathcal{B}_\infty$ on V endows V with the structure of quaternionic space. The right multiplication of $\mathcal{B}_\infty$ on V is then used to define the rigidification $\mathcal{B}_\infty \longrightarrow \mathrm{End}_{\mathcal{B}_\infty}(V_\mathbb{R})$.

Conversely, given a rigidified quaternionic space (V, ρ), one recovers the point ψ in $\mathcal{H}_\infty$ by letting $\psi(\lambda)$ be $\rho^{-1}(m_\lambda)$, where m_λ is the endomorphism in $\mathrm{End}_{\mathcal{B}_\infty}(V_\mathbb{R})$ induced by multiplication by the complex number λ.

One checks that these two assignments are bijections between $\mathcal{H}_\infty$ and the set of isomorphism classes of rigidified quaternionic spaces, and that they are inverses of each other.

We now describe the isomorphism $X(\mathbb{C}) = \mathcal{H}_\infty/\Gamma_\infty$ given in proposition 4.1. Let A be an abelian surface over $\mathbb{C}$ with quaternionic multiplication by $\mathcal{R}$ and level N^+ structure. Then the Lie algebra $V = \mathrm{Lie}(A)$ is a quaternionic space in a natural way. (The quaternionic action of $\mathcal{B}_\infty$ is induced by the action of $\mathcal{R}$ on the tangent space, by extension of scalars from $\mathbb{Z}$ to $\mathbb{R}$.) Moreover, V is equipped with an $\mathcal{R}$-stable sublattice Λ which is the kernel of the exponential map $V \longrightarrow A$.

Lemma 4.6

1. The endomorphism ring $\mathrm{End}_\mathcal{R}(\Lambda)$ *is isomorphic (non-canonically) to* $\mathcal{R}$.

2. The set of endomorphisms in $\mathrm{End}_\mathcal{R}(\Lambda)$ *which preserve the level* N^+*-structure on* Λ *is isomorphic (non-canonically) to the Eichler order* $\mathcal{R}(N^+)$.

Proof. The natural map

$$\mathcal{B} \otimes (\mathrm{End}_\mathcal{R}(\Lambda) \otimes \mathbb{Q}) \longrightarrow \mathrm{End}_\mathbb{Q}(\Lambda \otimes \mathbb{Q}) \simeq M_4(\mathbb{Q})$$

is an isomorphism, and hence $\mathrm{End}_\mathcal{R}(\Lambda) \otimes \mathbb{Q}$ is abstractly isomorphic to the quaternion algebra $\mathcal{B}$. Furthermore, the natural map

$$\mathrm{End}_\mathcal{R}(\Lambda) \longrightarrow \mathrm{End}_\mathbb{Z}(\Lambda)$$

has torsion-free cokernel, and hence $\mathrm{End}_\mathcal{R}(\Lambda)$ is a maximal order in $\mathcal{B}$. Likewise, one sees that the subalgebra of $\mathrm{End}_\mathcal{R}(\Lambda)$ preserving the level N^+ structure (viewed as a submodule of $\frac{1}{N^+}\Lambda/\Lambda$) is an Eichler order of level N^+.

Fix an isomorphism

$$\rho_0 : \mathcal{R} \longrightarrow \mathrm{End}_\mathcal{R}(\Lambda),$$

having the following properties.

1. For each $\ell^n \| N^+$, $\rho_0(\mathcal{R}(N^+)) \otimes \mathbb{Z}_\ell$ preserves the subgroup C_ℓ (viewed as a subgroup of $\frac{1}{\ell^n}\Lambda/\Lambda$). By the remark 1 above, $\mathcal{R}(N^+)$ operates on C_ℓ via a homomorphism $\mathcal{R}(N^+) \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z}$. In addition, we require that this homomorphism be equal to the orientation $\mathfrak{o}_\ell^+$.

2. For all $\ell | N^- p$, the algebra $\mathcal{R}_\ell$ acts on $\frac{1}{\ell}\Lambda/\Lambda$, and stabilizes the subspace V corresponding to A_I (where I is the maximal ideal of $\mathcal{R}_\ell$). By the remark 2 above, V is equipped with a canonical $\mathbb{F}_{\ell^2}$-vector space structure, and $\rho_0(\mathcal{R}_\ell)$ acts $\mathbb{F}_{\ell^2}$-linearly on it. We require that the resulting homomorphism $\mathcal{R}_\ell \longrightarrow \mathbb{F}_{\ell^2}$ be equal to the orientation $\mathfrak{o}_\ell^-$.

With these conventions, the homomorphism ρ_0 is well-defined, up to conjugation by elements in Γ_∞. Let $\rho : \mathcal{B}_\infty \longrightarrow \mathrm{End}_{\mathcal{B}_\infty}(V_\mathbb{R})$ be the map induced from ρ_0 by extension of scalars from $\mathbb{Z}$ to $\mathbb{R}$. The pair (V, ρ) is a rigidified quaternionic space, which depends only on the isomorphism class of A, up to the action of Γ_∞ on ρ by conjugation. The pair (V, ρ) thus gives a well-defined point on $\mathcal{H}_\infty/\Gamma_\infty$ associated to A.

It is a worthwhile exercise for the reader to check that this complex analytic description of the moduli of abelian varieties with quaternionic multiplications corresponds to the usual description of the moduli space of elliptic curves as $\mathcal{H}_\infty/\mathrm{SL}_2(\mathbb{Z})$, in the case where the quaternion algebra $\mathcal{B}$ is $M_2(\mathbb{Q})$.

III p-adic analytic description of X

The fundamental theorem of Cerednik and Drinfeld states that X is an admissible curve over $\mathbb{Q}_p$ and gives an explicit description of the discrete subgroup attached to X by theorem 3.1. More precisely, let B, R, and $\Gamma \subset R(N^+)[\frac{1}{p}]^\times$ be as in section 1. (So that B is the definite quaternion algebra obtained from $\mathcal{B}$ by the Cerednik "interchange of invariants" at p.) Then we have:

Theorem 4.7 (Cerednik-Drinfeld)
The set of K_p-rational points of the Shimura curve X is isomorphic to the quotient of the p-adic upper half plane $\mathcal{H}_p$ attached to B by the natural action of Γ, i.e.,

$$X(K_p) = \mathcal{H}_p/\Gamma.$$

Under this identification, the involution $\psi \mapsto \bar{\psi}$ of $\mathcal{H}_p$ corresponds to the involution τw_p of $X(K_p)$, where τ is the complex conjugation in $\mathrm{Gal}(K_p/\mathbb{Q}_p)$, and w_p is the Atkin-Lehner involution of X at p.

Proof. See [C], [Dr] and [BC].

In particular, an abelian surface A over K_p with quaternionic multiplications by $\mathcal{R}$ and level N^+ structure determines a point $\psi \in \mathcal{H}_p = \mathrm{Hom}(K_p, B_p)$ which is well-defined modulo the natural action of Γ. We will now give a precise description of the assignment $A \mapsto \psi$. Crucial to this description is Drinfeld's theorem that the p-adic upper half plane $\mathcal{H}_p$ parametrizes isomorphism classes of certain formal groups with a quaternionic action, and a suitable "rigidification".

The p-adic upper half plane as a moduli space. We review Drinfeld's moduli interpretation of the (K_p-rational points of the) p-adic upper half plane $\mathcal{H}_p$. Roughly speaking, $\mathcal{H}_p$ classifies formal groups of dimension 2 and height 4 over $\mathcal{O}_p$, equipped with an action of our fixed local order $\mathcal{R}_p$ and with a "rigidification" of their reduction modulo p.

In order to make this precise, we begin with a few definitions. Let as usual k be $\mathcal{O}_p/(p)(\simeq \mathbb{F}_{p^2})$.

Definition 4.8
A 2-dimensional commutative formal group V over $\mathcal{O}_p$ is a *formal $\mathcal{R}_p$-module* (for brevity, a *FR-module*) if it has height 4 and there is an embedding

$$i : \mathcal{R}_p \to \mathrm{End}(V).$$

The FR-modules play the role of the quaternionic spaces of the previous section. Let $\bar{V}$ be the formal group over k deduced from V by extension of scalars from $\mathcal{O}_p$ to k. It is equipped with the natural action of $\mathcal{R}_p$ given by reduction of endomorphisms. Let $\mathrm{End}^0(\bar{V}) := \mathrm{End}(\bar{V}) \otimes \mathbb{Q}_p$ be the algebra of quasi-endomorphisms of $\bar{V}$, and let $\mathrm{End}^0_{\mathcal{B}_p}(\bar{V})$ be the subalgebra of quasi-endomorphisms which commute with the action of $\mathcal{B}_p$.

Lemma 4.9
1. The algebra $\mathrm{End}^0(\bar{V})$ *is isomorphic (non-canonically) to* $M_2(\mathcal{B}_p)$.
2. The algebra $\mathrm{End}^0_{\mathcal{B}_p}(\bar{V})$ *is isomorphic (non-canonically) to the matrix algebra* B_p *over* $\mathbb{Q}_p$.

Proof. The formal group $\bar{V}$ is isogenous to the formal group of a product of two supersingular elliptic curves in characteristic p. Part 1 follows. Part 2 can then be seen by noting that the natural map

$$\mathcal{B}_p \otimes \mathrm{End}^0_{\mathcal{B}_p}(\bar{V}) \longrightarrow \mathrm{End}^0(\bar{V}) \simeq M_2(\mathcal{B}_p)$$

is an isomorphism, so that $\mathrm{End}^0_{\mathcal{B}_p}(\bar{V})$ is abstractly isomorphic to the matrix algebra B_p.

Denote by $B_{p,u}^\times$ the subgroup of elements of $B_p^\times$ whose reduced norm is a p-adic unit.

Definition 4.10
1. A *rigidification* of the FR-module V is an isomorphism

$$\rho : B_p \longrightarrow \mathrm{End}^0_{\mathcal{B}_p}(\bar{V}),$$

subject to the condition of being "positively oriented at p", i.e., that the two maximal orders R_p and $\rho^{-1}(\mathrm{End}_{\mathcal{R}_p}(\bar{V}))$ of B_p are conjugated by an element of $B_{p,u}^\times$.
2. A pair (V, ρ) consisting of an FR-module V and a rigidification ρ is called a *rigidified FR-module.*
3. Two rigidified modules (V, ρ) and (V', ρ') are said to be isomorphic if there is an isomorphism $\phi : V \to V'$ of formal groups over $\mathcal{O}_p$, such that the induced isomorphism

$$\phi^* : \mathrm{End}^0_{\mathcal{B}_p}(\bar{V}) \to \mathrm{End}^0_{\mathcal{B}_p}(\bar{V}')$$

satisfies the relation $\phi^* \circ \rho = \rho'$.

Remark. In [Dr] and [BC], a rigidification of a FR-module V is defined to be a quasi-isogeny of height zero from a fixed FR-module $\bar{\Phi}$ to the reduction $\bar{V}$ modulo p of V. This definition is equivalent to the one we have given, once one has fixed an isomorphism between B_p and $\mathrm{End}^0_{\mathcal{B}_p}(\bar{\Phi})$. The definition given above is in a sense "base-point free".

Recall that $B_{p,u}^\times$ acts (on the left) on $\mathcal{H}_p$ via the natural action of $B_p^\times$ on $\mathcal{H}_p$ by conjugation. Note that $B_{p,u}^\times$ acts on the left on (the isomorphism classes of) rigidified FR-modules, by

$$b(V, \rho) := (V, \rho^b) \text{ for } b \text{ in } B_{p,u}^\times,$$

where $\rho^b(x)$ is equal to $\rho(b^{-1}xb)$ for x in B_p.

Theorem 4.11 (Drinfeld)
1. The p-adic upper half plane $\mathcal{H}_p$ is a moduli space for the isomorphism classes of rigidified FR-modules over $\mathcal{O}_p$. In particular, there is a bijective map

$$\Psi : \{(V,\rho) :\ (V,\rho)\ \text{ a rigidified } FR\text{−module}\} / (\text{isomorphisms}) \xrightarrow{\sim} \mathrm{Hom}(K_p, B_p).$$

2. The map Ψ is $B_{p,u}^{\times}$-equivariant.

Proof. See [Dr] and [BC], chapters I and II. For part 2, see in particular [BC], ch. II, sec. 9.

Corollary 4.12
All FR-modules have formal multiplication by $\mathcal{O}_p$.

Proof. If V is a FR-module, equip V with a rigidification ρ. By theorem 4.11, the pair (V,ρ) determines a point $P_{(V,\rho)}$ of the p-adic upper half plane $\mathcal{H}_p$. Note that the stabilizer of $P_{(V,\rho)}$ for the action of $B_{p,u}^{\times}$ is isomorphic to $\mathcal{O}_p^{\times}$. The claim now follows from part 2 of theorem 4.11.

Remark. As we will explain in the next paragraph, if V is an FR-module, there exists an abelian surface A over $\mathcal{O}_p$ with quaternionic multiplication by $\mathcal{R}$, whose formal group $\hat{A}$ (with the induced action of $\mathcal{R}_p$) is isomorphic to V. Of course, quite often one has $\mathrm{End}_{\mathcal{R}}(A) \simeq \mathbb{Z}$, even though $\mathrm{End}_{\mathcal{R}}(V)$ contains $\mathcal{O}_p$ by corollary 4.12. In fact, combining Drinfeld's theory with the theory of complex multiplication shows the existence of an uncountable number of such abelian surfaces such that (i) $\mathrm{End}_{\mathcal{R}}(A) = \mathbb{Z}$; (ii) $\mathrm{End}_{\mathcal{R}_p}(\hat{A}) \simeq \mathcal{O}_p$. (A similar phenomenon for elliptic curves has been observed by Lubin and Tate [LT].)

We give a description of the bijection Ψ, which follows directly from Drinfeld's theorem. By lemma 4.12, identify $\mathrm{End}_{\mathcal{R}_p}(V)$ with $\mathcal{O}_p$. Let $\psi : K_p \longrightarrow B_p$ be the map induced by the composition

$$\mathcal{O}_p \longrightarrow \mathrm{End}^0_{\mathcal{B}_p}(\bar{V}) \longrightarrow B_p,$$

where the first map is given by the reduction modulo p of endomorphisms, and the second map is just ρ^{-1}. Then $\Psi(V,\rho) = \psi$.

We now use Drinfeld's theorem to describe the p-adic uniformization of the K_p-rational points of the Shimura curve X, i.e., the isomorphism

$$X(K_p) = \mathcal{H}_p/\Gamma.$$

The curve X has a model $\mathcal{X}$ over $\mathbb{Z}_p$. Given a point in $X(K_p)$, we may extend it to a point in $\mathcal{X}(\mathcal{O}_p)$. In other words, given a pair (A,i,C), where A is an abelian surface over K_p with quaternionic action by i, and C is a level N^+-structure, we may extend it to a similar pair $(\underline{A},\underline{i},\underline{C})$ of objects over $\mathcal{O}_p$. We write $(\bar{A},\bar{\imath},\bar{C})$ for the reduction modulo p of $(\underline{A},\underline{i},\underline{C})$. A p-quasi endomorphism of $\bar{A}$ is an element in $\mathrm{End}(\bar{A})\otimes\mathbb{Z}[\frac{1}{p}]$. The algebra of all p-quasi endomorphisms is denoted by $\mathrm{End}^{(p)}(\bar{A})$. Likewise, we denote by $\mathrm{End}^{(p)}_{\mathcal{R}}(\bar{A})$ the algebra of p-quasi-endomorphisms which commute with the action of $\mathcal{R}$. Let $B_{p\infty}$ be the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞, and let $R_{p\infty}$ be a maximal order of $B_{p\infty}$.

Lemma 4.13
1. The algebra $\mathrm{End}^{(p)}(\bar{A})$ *is isomorphic to* $M_2(R_{p\infty}[\frac{1}{p}])$.
2. The algebra $\mathrm{End}^{(p)}_{\mathcal{R}}(\bar{A})$ *is isomorphic to* $R[\frac{1}{p}]$.
3. The subalgebra of endomorphisms preserving the level N^+*-structure* $\bar{C}$ *on* $\bar{A}$ *is isomorphic to the Eichler order* $R(N^+)[\frac{1}{p}]$.

Proof.
1. The abelian variety $\bar{A}$ is p-isogenous to a product of a supersingular elliptic curve in characteristic p with itself. Part 1 follows. To see part 2, observe that the natural map

$$\mathcal{R}[\frac{1}{p}] \otimes \mathrm{End}^{(p)}_{\mathcal{R}}(\bar{A}) \longrightarrow \mathrm{End}^{(p)}(\bar{A}) \simeq M_2(R_{p\infty}[\frac{1}{p}])$$

is an isomorphism, and hence $\mathrm{End}^{(p)}_{\mathcal{R}}(\bar{A})\otimes\mathbb{Q}$ is abstractly isomorphic to the quaternion algebra B. Furthermore, the natural map

$$\mathrm{End}^{(p)}_{\mathcal{R}}(\bar{A}) \longrightarrow \mathrm{End}^{(p)}(\bar{A})$$

has torsion-free cokernel, and hence $\mathrm{End}^{(p)}_{\mathcal{R}}(\bar{A})$ is a maximal $\mathbb{Z}[\frac{1}{p}]$-order in B. Likewise, one sees that the subalgebra of $\mathrm{End}^{(p)}_{\mathcal{R}}(\bar{A})$ preserving the level N^+ structure $\bar{C}$ is abstractly isomorphic to the Eichler order $R(N^+)[\frac{1}{p}]$.

Fix an isomorphism

$$\rho_0 : R[\frac{1}{p}] \longrightarrow \mathrm{End}^{(p)}_{\mathcal{R}}(\bar{A}),$$

having the following properties.

1. For each $\ell^n \| N^+$, we require that $\rho_0(R(N^+)) \otimes \mathbb{Z}_\ell$ preserves the subgroup C_ℓ, so that it operates on it via a homomorphism $R(N^+) \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z}$. We impose, in addition, that this homomorphism be equal to the orientation $\mathfrak{o}^+_\ell$.

2. For all $\ell | N^-$, the algebra R_ℓ acts on $\bar{A}_\ell$ via ρ_0, and stabilizes the subspace corresponding to A_I (where I is the maximal ideal of $\mathcal{R}_\ell$.) By remark 2 in part I of this section, A_I is equipped with a canonical $\mathbb{F}_{\ell^2}$-vector space structure, and $\rho_0(R_\ell)$ acts $\mathbb{F}_{\ell^2}$-linearly on it. We require that the resulting homomorphism $R_\ell \longrightarrow \mathbb{F}_{\ell^2}$ be equal to the orientation $\mathfrak{o}^-_\ell$.

3. Let $\bar{V}$ be the formal group of $\bar{A}$, and let $\rho : B_p \longrightarrow \mathrm{End}^0_{\mathcal{B}_p}(\bar{V})$ be the map induced by ρ_0 by extension of scalars from $\mathbb{Z}[\frac{1}{p}]$ to $\mathbb{Q}_p$. We require that $\rho^{-1}(\mathrm{End}_{\mathcal{R}_p}(\bar{V}))$ be conjugate to R_p by an element of $B^\times_{p,u}$.

With these conventions, the homomorphism ρ_0 is well-defined, up to conjugation by elements in Γ. The pair (V, ρ) is a rigidified FR-module, which is completely determined by the isomorphism class of A, up to the action of Γ on ρ by conjugation. Thus, (V, ρ) gives a well-defined point on $\mathcal{H}_p/\Gamma$ associated to A.

IV Shimura curve parametrizations

We denote by π_{CD} the Cerednik-Drinfeld p-adic analytic uniformization

$$\pi_{CD} : \mathcal{H}_p \longrightarrow X(K_p),$$

which induces a map $\mathrm{Div}^0(\mathcal{H}_p) \longrightarrow \mathrm{Div}^0(X(K_p))$, also denoted π_{CD} by abuse of notation. The Jacobian J of $X_{/K_p}$ is therefore uniformized by a p-adic torus, and by proposition 3.4 and corollary 3.5, we have:

Corollary 4.14
The map π_{CD} induces a p-adic uniformization

$$\Phi_{CD} : \mathrm{Hom}(\bar{\Gamma}, K_p^\times) \longrightarrow J(K_p),$$

such that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Div}^0(\mathcal{H}_p) & \xrightarrow{\Phi_{AJ}} & \mathrm{Hom}(\bar{\Gamma}, K_p^\times) \\ \pi_{CD} \downarrow & & \downarrow \Phi_{CD} \\ \mathrm{Div}^0(X(K_p)) & \xrightarrow{\Phi_{AJ}} & J(K_p). \end{array}$$

Combining this corollary with the canonical inclusion of $\mathcal{M}$ into $\mathrm{Hom}(\Gamma, \mathbb{Z})$ given by proposition 1.3, yields a natural p-adic uniformization

$$\Phi_{CD} : \mathcal{M} \otimes K_p^\times \longrightarrow J(K_p),$$

which will also be denoted Φ_{CD} by abuse of notation.

The Shimura curve X is equipped with natural Hecke correspondences (cf. [BD1], sec. 1.5), and the Hecke algebra acting on J is isomorphic to the Hecke algebra $\mathbb{T}$ acting on $\mathcal{M}$, in such a way that the actions of $\mathbb{T}$ on $\mathcal{M}$ and on J are compatible with the inclusion of $\mathcal{M}$ into the dual of the character group of J over k. (See [BC], ch. III, sec. 5.)

Recall the endomorphism $\eta_f \in \mathbb{T}$ attached to f which was used to define the map $\mathcal{M} \longrightarrow \mathbb{Z}$. This endomorphism also acts on $\mathrm{Pic}(X)$, and induces a (generically) surjective map

$$\eta_f : \mathrm{Pic}(X) \to \tilde{E},$$

where $\tilde{E}$ is a subabelian variety of J isogenous to E. From now on we will assume that $E = \tilde{E}$.

Proposition 4.15
The p-adic uniformizations Φ_{Tate} and Φ_{CD} of Tate and Cerednik-Drinfeld are related by the following diagram which commutes up to sign.

$$\begin{array}{ccc} \mathcal{M} \otimes K_p^\times & \xrightarrow{\Phi_{CD}} & J(K_p) \\ \eta_f \otimes \mathrm{id} \downarrow & & \eta_f \downarrow \\ K_p^\times & \xrightarrow{\Phi_{\mathrm{Tate}}} & E(K_p) \end{array}$$

(Note that both of the maps η_f that appear in this diagram are only well-defined up to sign.)

5 Heegner points

I Moduli description

We give first a moduli definition of Heegner points. Let c be as before an integer prime to N, and let $\mathcal{O}$ be the order of K of conductor c.

Given an abelian surface A with quaternionic multplication and level N^+ structure, we write $\underline{\mathrm{End}}(A)$ to denote the algebra of endomorphisms of A (over an algebraic closure of $\mathbb{Q}$) which commute with the quaternionic multiplications and respect the level N^+ structure.

Definition 5.1

A *Heegner point of conductor* c on X (attached to K) is a point on X corresponding to an abelian surface A with quaternionic multiplication and level N^+ structure, such that

$$\underline{\mathrm{End}}(A) \simeq \mathcal{O}.$$

It follows from the theory of complex multiplication that the Heegner points on X of conductor c are all defined over the ring class field of K of conductor c. (Cf. [ST].)

II Complex analytic description

For the convenience of the reader we recall now how to define Heegner points using the complex analytic uniformization. (This material will not be used in our proofs, but is quite parallel to the p-adic theory, which we do use extensively.)

Given an embedding ψ of K into $\mathcal{B}$, let ψ denote also, by abuse of notation, its natural image by extension of scalars in $\mathcal{H}_\infty = \mathrm{Hom}(\mathbb{C}, \mathcal{B}_\infty)$. An embedding $\psi : K \longrightarrow \mathcal{B}$ is said to be an *optimal embedding of conductor* c (relative to the Eichler order $\mathcal{R}(N^+)$ if it maps $\mathcal{O}$ to $\mathcal{R}(N^+)$ and does not extend to an embedding of any larger order into $\mathcal{R}(N^+)$.

Let $P \in X(H)$ be a Heegner point of conductor c, corresponding to a quaternionic surface A over H. By choosing a complex embedding $H \longrightarrow \mathbb{C}$, the point P gives rise to a point $P_{\mathbb{C}}$ in $X(\mathbb{C})$, which corresponds to the abelian surface $A_{\mathbb{C}}$ obtained from A by extension of scalars from H to $\mathbb{C}$, via our chosen complex embedding. Let $\tilde{P}$ be a lift of $P_{\mathbb{C}}$ to $\mathcal{H}_\infty$ by the complex analytic uniformization of proposition 4.1.

Theorem 5.2

The Heegner point $\tilde{P} \in \mathcal{H}_\infty$ corresponds to an optimal embedding $\psi : K \longrightarrow \mathcal{B}$ of conductor c.

Proof. Let $V = \mathrm{Lie}(A)$, and let the isomorphism $\rho_0 : \mathcal{R} \longrightarrow \mathrm{End}_{\mathcal{R}}(\Lambda)$ be chosen as in the discussion following lemma 4.6. The action of $\mathbb{C}$ by multiplication on V arises by extension of scalars from the action of the order $\mathcal{O}$ of conductor c on A, and hence the point ψ necessarily comes (by extension of scalars) from a global embedding of $\mathcal{O}$ to $R(N^+)$ which is optimal.

III p-adic analytic description

Let H be the ring class field of conductor c, and let $P = (A, i, C)$ be a Heegner point of conductor c. By fixing an embedding $H \to K_p$, we may view P as a point of $X(K_p)$. We want to describe the Heegner points of conductor c as elements of the quotient $\mathcal{H}_p/\Gamma$. Recall the Gross points of conductor c represented by the oriented optimal embeddings

$$\psi_i : \mathcal{O} \to R[\frac{1}{p}], \quad i = 1, \ldots, h$$

fixed in section 2. By lemma 2.5, the group Δ acts simply transitively on these points. The embeddings ψ_i determine local embeddings (which we denote in the same way by an abuse of notation)

$$\psi_i : K_p \to B_p.$$

Theorem 5.3
The classes modulo Γ of the local embeddings ψ_i correspond via the Cerednik-Drinfeld uniformization to distinct Heegner points on X of conductor c, in such a way that the natural Galois action of Δ on these Heegner points is compatible with the action of Δ on the Gross points represented by the ψ_i.

Proof. If $P \in X(K_p)$ is a Heegner point of conductor c, let $\bar{P} \in X(k)$ denote the reduction modulo p of P. By our description of the p-adic uniformization, the point P corresponds to the class modulo Γ of a local embedding $\psi : K_p \to B_p$ defined in the following way. Let

$$\psi_0 : \mathcal{O} = \mathrm{End}(P) \to \mathrm{End}(\bar{P})$$

be the map obtained by reduction modulo p of endomorphisms. Identify $\mathrm{End}(\bar{P})[\frac{1}{p}]$ with $R[\frac{1}{p}]$ by using the conventions of section 4, so that ψ_0 gives rise to a map from $\mathcal{O}$ to $R[\frac{1}{p}]$. Then ψ is obtained from ψ_0 by extension of scalars from $\mathbb{Z}$ to $\mathbb{Q}_p$.

By proposition 7.3 of [GZ], ψ_0 is an optimal embedding. Moreover, ψ_0 is Γ-conjugate to one of the ψ_i. Finally, the proof of the compatibility under the action of the group Δ is similar to that of proposition 4.2 of [BD2].

6 Computing the p-adic Abel-Jacobi map

Let $\psi \in \mathcal{H}_p = \mathrm{Hom}(K_p, B_p)$ be a point on the p-adic upper half plane, and let $\bar{\psi}$ be its conjugate, defined by

$$\bar{\psi}(z) = \psi(\bar{z}).$$

The divisor $(\psi) - (\bar{\psi})$ is a divisor of degree 0 on $\mathcal{H}_p$.

Recall the canonical element $\mathcal{L}'_p(\psi) \in \mathcal{M} \otimes K^\times_{p,1}$ associated to ψ in section 2, using the action of $K_p^\times$ induced by ψ on the Bruhat Tits tree $\mathcal{T}$. When needed, we will identify $\mathcal{L}'_p(\psi)$ with its natural image in $\mathrm{Hom}(\Gamma, K_p^\times)$, by an abuse of notation.

Recall also the p-adic Abel Jacobi map

$$\Phi_{AJ} : \mathrm{Div}^0(\mathcal{H}_p) \longrightarrow \mathrm{Hom}(\Gamma, K_p^\times)$$

defined in sections 3 and 4 by considering automorphy factors of p-adic theta-functions.

The main result of this section is:

Theorem 6.1

$$\Phi_{AJ}((\psi)-(\bar{\psi}))=\mathcal{L}'_p(\psi).$$

The rest of this section is devoted to the proof of theorem 6.1. We begin by giving explicit descriptions, and elucidating certain extra structures, which the fixing of the point $\psi \in \mathcal{H}_p$ gives rise to.

The algebra B_p

We give an explicit description of the algebra B_p, which depends on the embedding ψ. Identify K_p with its image in B_p by ψ, and choose an element $u \in B_p$ so that $B_p = K_p \oplus K_p u$ and u anticommutes with the elements of K_p, i.e., $uz = \bar{z}u$ for all $z \in K_p$. Note that u^2 belongs to $\mathbb{Q}_p$, and is a norm from K_p to $\mathbb{Q}_p$, since the quaternion algebra B is split at p. Moreover, the element u^2 is well-defined up to multiplication by norms from K_p to $\mathbb{Q}_p$. We may and will fix u so that $u^2 = 1$. From now on, write elements of B_p as $a+bu$, with a and b in K_p. The conjugate of $a+bu$ under the canonical anti-involution of B_p is $\bar{a}-bu$. The reduced trace and norm are given by the formulae

$$Tr(a+bu)=Tr_{K/\mathbb{Q}}(a), \qquad N(a+bu)=N_{K/\mathbb{Q}}(a)-N_{K/\mathbb{Q}}(b).$$

The embedding ψ allows us to view B_p as a two-dimensional vector space over K_p, on which B_p acts by multiplication on the right. This yields a local embeding $B_p \longrightarrow M_2(K_p)$, defined by:

$$a+bu \mapsto \begin{pmatrix} a & b \\ \bar{b} & \bar{a} \end{pmatrix}.$$

This embedding allows us to define an action of $B_p^\times$ on the projective line $\mathbb{P}^1(K_p)$ (or $\mathbb{P}^1(\mathbb{C}_p)$) by fractional linear transformations, by setting

$$\gamma(z) := \frac{az+b}{\bar{b}z+\bar{a}}, \quad \text{if} \quad \gamma = a+bu \in B_p^\times, \quad z \in \mathbb{P}^1(K_p).$$

This induces an action of the group Γ on $\mathbb{P}^1(K_p)$.

The domain Ω_p

Let

$$S^1 = \{z \in K_p \;\mid\; z\bar{z}=1\}$$

be the p-adic "circle" of radius 1, and let $\Omega_p = \mathbb{P}^1(K_p) - S^1$.

Lemma 6.2

The limit set of Γ acting on $\mathbb{P}^1(K_p)$ is equal to S^1. In particular, the group Γ acts discontinuously on $\mathbb{P}^1(K_p)$.

Proof. To compute the limit set of Γ, observe that if γ_n is a sequence of distinct elements of Γ, then one can write

$$\gamma_n = \frac{a_n+b_n u}{p^{e_n}},$$

with $a_n, b_n \in \mathcal{O}_p^\times$, and $\lim_{n\longrightarrow\infty} e_n = \infty$. Hence

$$N_{K_p/\mathbb{Q}_p}(\frac{a_n}{\bar{b}_n}) \equiv 1 \pmod{p^{2e_n}},$$

so that the limit $\lim \gamma_n z_0$, if it exists, must belong to S^1. Conversely, let z be an element of S^1, and let b_n be a sequence of elements in $B_p^\times$ satisfying

$$\lim_{n\longrightarrow\infty}(b_n^{-1}\infty) = z.$$

By the finiteness of the double coset space $R_p^\times\backslash B_p^\times/\Gamma$, which follows from strong approximation, there is an element $b \in B_p^\times$ such that, for infinitely many n

$$b_n = r_n b\gamma_n,$$

where r_n belongs to $R_p^\times$ and γ_n belongs to Γ. Assume without loss of generality (by extracting an appropriate subsequence) that this equation holds for all n. Then we have

$$z = \lim(\gamma_n^{-1}b^{-1}r_n^{-1}\infty).$$

But the sequence $b^{-1}r_n^{-1}\infty$ is contained in a compact set, and hence has a convergent subsequence $b^{-1}r_{k_n}^{-1}\infty$ which tends to some $z_0 \in \mathbb{P}^1(K_p)$. Hence $z = \lim \gamma_{k_n}^{-1} z_0$ is a limit point for Γ. Lemma 6.2 follows.

Using the embedding ψ, the "abstract" upper half plane $\mathcal{H}_p$ now becomes identified with the domain Ω_p.

The tree $\mathcal{T}$

Let $v_0 = r(\psi)$ be the vertex on $\mathcal{T}$ which is fixed by $\psi(K_p)$. This vertex corresponds to the maximal order

$$R_p = \mathcal{O}_p \oplus \mathcal{O}_p u,$$

where $\mathcal{O}_p$ is the ring of integers of K_p. The vertices of $\mathcal{T}$ are in bijection with the coset space $R_p^\times\mathbb{Q}_p^\times\backslash B_p^\times$, by assigning to $b \in B_p^\times$ the vertex $b^{-1} * v_0$.

We say that a vertex v of $\mathcal{T}$ has *level* n, and write $\ell(v) = n$, if its distance from v_0 is equal to n. A vertex is of level n if and only if it can be represented by an element of the form $a + bu$, where a and b belong to $\mathcal{O}_p$ and at least one of a or b is in $\mathcal{O}_p^\times$, and $n = \mathrm{ord}_p(N(a+bu)) = \mathrm{ord}_p(N_{K_p/\mathbb{Q}_p}(a) - N_{K_p/\mathbb{Q}_p}(b))$.

Likewise, we say that an edge e of $\mathcal{T}$ has level n, and we write $\ell(e) = n$, if the distance of its furthest vertex from v_0 is equal to n.

The reduction map

We use our identification of $\mathcal{H}_p$ with Ω_p to obtain a reduction map

$$r : \Omega_p \longrightarrow \mathcal{T}$$

from Ω_p to the tree of B_p.

Lemma 6.3

The divisor $(\psi) - (\bar{\psi})$ on $\mathcal{H}_p$ corresponds to the divisor $(0) - (\infty)$ on Ω_p under our identification of Ω_p with $\mathcal{H}_p$.

Proof. The group $\psi(K_p^\times)$ acting on Ω_p by Möbius transformations fixes the points 0 and ∞, and acts on the tangent line at 0 by the character $z \mapsto \frac{z}{\bar{z}}$.

In general, if z is a point of Ω_p and $b \in B_p^\times$ is such that $b^{-1}0 = z$, then $r(z)$ is equal to b. This implies directly part 1 and 2 of the next lemma.

Lemma 6.4
1. We have $r(\infty) = r(0) = v_0$. More generally, if $z \in \Omega_p \subset K_p \cup \infty$ does not belong to $\mathcal{O}_p^\times$, then $r(z) = v_0$.
2. If z belongs to $\mathcal{O}_p^\times$, then the level of the vertex $r(z)$ is equal to $\mathrm{ord}_p(z\bar{z} - 1)$.
3. If z_1 and $z_2 \in \Omega_p$ map under the reduction map to adjacent vertices on $\mathcal{T}$ of level n and $n+1$, then

$$z_1 \equiv z_2 \pmod{p^n}.$$

Proof. We prove part 3. Choose representatives b_1 and b_2 in $B_p^\times$ for $r(z_1)$ and $r(z_2)$, with the properties

$$b_i = x_i + y_i u, \qquad \text{with } \ x_i, y_i \in \mathcal{O}_p \quad \text{and} \quad \gcd(x_i, y_i) \in \mathcal{O}_p^\times.$$

Since the vertices corresponding to b_1 and b_2 are adjacent, it follows that $b_2 b_1^{-1} = b_2 \bar{b}_1 / p^n$ has norm p and level 1. Since

$$b_2 \bar{b}_1 = (x_2 + y_2 u)(\bar{x}_1 - y_1 u) = (x_2 \bar{x}_1 - y_2 \bar{y}_1) - (y_1 x_2 - x_1 y_2) u,$$

it follows that

$$\frac{x_1}{y_1} \equiv \frac{x_2}{y_2} \pmod{p^n},$$

so that $b_1^{-1}0 \equiv b_2^{-1}0 \pmod{p^n}$. This proves the lemma.

Let $\phi_{(0)-(\infty)} \in \mathrm{Hom}(\Gamma, K_p^\times)$ be the automorphy factor of the p-adic theta-function associated to the divisor $(0) - (\infty)$ as in section 3. By the results of section 3, we have

$$\Phi_{AJ}((\psi) - (\bar{\psi})) = \phi_{(0)-(\infty)}.$$

By definition, for $\delta \in \Gamma$ one has

$$\phi_{(0)-(\infty)}(\delta) = \prod_{\gamma \in \Gamma} \frac{\gamma\delta(z_0)}{\gamma(z_0)},$$

where z_0 is any element in the domain Ω_p. Suppose that $r(z_0) = v_0$. Let

$$\mathrm{path}(v_0, \delta v_0) = e_1 - e_2 + \cdots + e_{s-1} - e_s.$$

(Note that s is even, since δ belongs to Γ.) Write $e_j = \{v_j^e, v_j^o\}$, where v_j^e is the even vertex of e_j, and v_j^o is the odd vertex of e_j. Note that we have

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

Thus we may choose elements z_j^o and z_j^e in $\Omega_p(K_p)$ 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

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

so that

$$\begin{aligned} \phi_{(0)-(\infty)}(\delta) &= \prod_{\gamma \in \Gamma} \left(\frac{\gamma z_1^o}{\gamma z_1^e} \right) \left(\frac{\gamma z_2^o}{\gamma z_2^e} \right)^{-1} \cdots \left(\frac{\gamma z_{s-1}^o}{\gamma z_{s-1}^e} \right) \left(\frac{\gamma z_s^o}{\gamma z_s^e} \right)^{-1} \\ &= \prod_{\gamma \in \Gamma} \left(\frac{\gamma z_1^o}{\gamma z_1^e} \right) \prod_{\gamma \in \Gamma} \left(\frac{\gamma z_2^o}{\gamma z_2^e} \right)^{-1} \cdots \prod_{\gamma \in \Gamma} \left(\frac{\gamma z_{s-1}^o}{\gamma z_{s-1}^e} \right) \prod_{\gamma \in \Gamma} \left(\frac{\gamma z_s^o}{\gamma z_s^e} \right)^{-1}, \end{aligned}$$

where the last equality follows from part 3 of lemma 6.4. Fix a large *odd* integer n. For each $1 \leq j \leq s$, let $\Gamma(j)$ be the set of elements γ in Γ such that the set γe_j has level $\leq n$. By lemma 6.4, we have

$$(\dagger) \quad \phi_{(0)-(\infty)}(\delta) \equiv \prod_{\gamma \in \Gamma(1)} \left(\frac{\gamma z_1^o}{\gamma z_1^e} \right) \prod_{\gamma \in \Gamma(2)} \left(\frac{\gamma z_2^o}{\gamma z_2^e} \right)^{-1} \cdots \prod_{\gamma \in \Gamma(s)} \left(\frac{\gamma z_s^o}{\gamma z_s^e} \right)^{-1} \pmod{p^n}.$$

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

$$\prod_{\Gamma(j)} \frac{\gamma z_j^o}{\gamma z_j^e} = \prod_{\ell(\gamma v_j^o) < n} \gamma z_j^o \cdot \prod_{\ell(\gamma v_j^e) < n} \gamma (z_j^e)^{-1} \cdot \prod_{\ell(\gamma e_j) = n} \gamma z_j^o.$$

The first two factors in this last expression cancel out in the formula ($\dagger$) for $\phi_{(0)-(\infty)}(\delta)$. Hence we obtain

$$\phi_{(0)-(\infty)}(\delta) \equiv \prod_{\ell(\gamma e_1) = n} \gamma z_1^o \cdot \prod_{\ell(\gamma e_2) = n} \gamma (z_2^o)^{-1} \cdots \prod_{\ell(\gamma e_s) = n} \gamma (z_s^o)^{-1} \pmod{p^n}.$$

Now, fix an edge e of level n, having v as its vertex of level n, and choose any $z \in \Omega_p$ with $r(z) = v$. If σ is a variable running over G_n (which we view as belonging to $(\mathcal{O}_p/p^n\mathcal{O}_p)^\times/(\mathbb{Z}/p^n\mathbb{Z})^\times$), write $\sigma e \equiv e_j$ if the edge σe is Γ-equivalent to e_j. Using the fact that G_n acts transitively on the set of edges of level n, we have

$$\begin{aligned} \phi_{(0)-(\infty)}(\delta) &\equiv \prod_{\sigma e \equiv e_1} (\frac{\sigma}{\bar{\sigma}} z)^{w_{e_1}} \cdot \prod_{\sigma e \equiv e_2} (\frac{\sigma}{\bar{\sigma}} z)^{-w_{e_2}} \cdots \prod_{\sigma e \equiv e_s} (\frac{\sigma}{\bar{\sigma}} z)^{-w_{e_s}} \pmod{p^n} \\ &= \prod_{\sigma e \equiv e_1} (\frac{\sigma}{\bar{\sigma}})^{w_{e_1}} \cdot \prod_{\sigma e \equiv e_2} (\frac{\sigma}{\bar{\sigma}})^{-w_{e_2}} \cdots \prod_{\sigma e \equiv e_s} (\frac{\sigma}{\bar{\sigma}})^{-w_{e_s}} \cdot (z^M), \end{aligned}$$

where $M = \langle \mathrm{path}(v_0, \delta v_0), \sum_{\sigma \in G_n} \sigma e \rangle$. Since the element $\sum_{\sigma \in G_n} \sigma e$ belongs to the image of ∂^*, and $\mathrm{path}(v_0, \delta v_0)$ is in the kernel of ∂_*, it follows that $M = 0$ so that:

$$\phi_{(0)-(\infty)}(\delta) \equiv \prod_{\sigma e \equiv e_1} (\frac{\sigma}{\bar{\sigma}})^{w_{e_1}} \cdot \prod_{\sigma e \equiv e_2} (\frac{\sigma}{\bar{\sigma}})^{-w_{e_2}} \cdots \prod_{\sigma e \equiv e_s} (\frac{\sigma}{\bar{\sigma}})^{-w_{e_s}} .$$

The reader will notice that this last expression is equal to

$$\langle \mathrm{path}(v_0, \delta v_0), \mathcal{L}'_{p,n}(\psi) \rangle.$$

Hence

$$\mathcal{L}'_p(\psi) = \phi_{(0)-(\infty)} = \Phi_{AJ}((\psi) - (\bar{\psi})),$$

and theorem 6.1 follows.

7 Proof of the main results

We now combine the results of the previous sections to give a proof of our main results. First, we introduce some notations. Having fixed an embedding $H \to K_p$, let $P_1, \ldots, P_h$ in $X(K_p)$ be the h distinct Heegner points of conductor c, corresponding via theorem 5.3 to our fixed optimal embeddings $\psi_1, \ldots, \psi_h$. Let $\sigma_1, \ldots, \sigma_h \in \Delta$ be the elements of Δ, labeled in such a way that $\sigma_i(P_1) = P_i$. By theorem 5.3, the Gross point corresponding to ψ_1 is sent by σ_i to the Gross point corresponding to ψ_i. Write $P_K \in \mathrm{Pic}(X(K_p))$ for the class of the divisor $P_1 + \ldots + P_h$. Note that P_K depends on the choice of the embedding of H into K_p, only up to conjugation in $\mathrm{Gal}(K_p/\mathbb{Q}_p)$. We denote by $\bar{P}_i$ the complex conjugate of P_i, and likewise for $\bar{P}_K$. (No confusion should arise with the use of the notation $\bar{P}$ in section 5 to indicate the reduction modulo p of the point P.) Let w_p stand for the Atkin-Lehner involution at p.

Theorem 7.1

1. $\Phi_{CD}(\mathcal{L}'_p(\mathcal{M}/K)) = \Phi_{AJ}((P_K) - (w_p \bar{P}_K))$.

2. $\Phi_{CD}(\mathcal{L}'_p(\mathcal{M}/H)) = \sum_{i=1}^h \Phi_{AJ}((P_i) - (w_p \bar{P}_i)) \cdot \sigma_i^{-1}$.

Proof. By the formula at the end of section 2,

$$\mathcal{L}'_p(\mathcal{M}/K) = \sum_{i=1}^{h} \mathcal{L}'_p(\psi_i),$$

where $\psi_1, \ldots, \psi_h$ are as above. Hence,

$$\Phi_{CD}(\mathcal{L}'_p(\mathcal{M}/K)) = \sum_{i=1}^{h} \Phi_{CD}(\mathcal{L}'_p(\psi_i)) = \sum_{i=1}^{h} \Phi_{CD}(\Phi_{AJ}((\psi_i) - (\bar{\psi}_i))),$$

where the last equality follows from theorem 6.1. By theorems 5.3 and 4.7, and by the commutative diagram of proposition 4.14, this last expression is equal to

$$\sum_{i=1}^{h} \Phi_{AJ}(\pi_{CD}((\psi_i)-(\bar{\psi}_i))) = \sum_{i=1}^{h} \Phi_{AJ}((P_i)-(w_p\bar{P}_i)) = \Phi_{AJ}((P_K)-(w_p\bar{P}_K)).$$

Part 1 follows. Part 2 is proved in a similar way.

Recall our running assumption that $E=\tilde{E}$ is the subabelian variety of the Jacobian J of the Shimura curve X, and that η_f maps J to $\tilde{E}$. Let $\alpha_i=\eta_f(P_i)\in E(K_p)$, and let $\alpha_K=\alpha_1+\cdots+\alpha_h=\mathrm{trace}_{H/K}(\alpha_1)$. Theorem 7.1 gives the following corollary, whose first part is the statement of theorem B of the introduction.

Corollary 7.2
Let $w=1$ (resp. $w=-1$) if $E/\mathbb{Q}_p$ has split (resp. non-split) multiplicative reduction. Then the following equalities hold up to sign:

$$\Phi_{\mathrm{Tate}}(\mathcal{L}'_p(E/K)) = \alpha_K - w\bar{\alpha}_K,$$

$$\Phi_{\mathrm{Tate}}(\mathcal{L}'_p(E/H)) = \sum_{i=1}^{h}(\alpha_i - w\bar{\alpha}_i)\cdot\sigma_i^{-1}.$$

Proof. Apply η_f to the equations of theorem 7.1, using the commutative diagram of proposition 4.15.

References

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

[**BD1**] M. Bertolini, H. Darmon, *Heegner points on Mumford-Tate curves,* Inv. Math., to appear.

[**BD2**] M. Bertolini, H. Darmon, *A rigid analytic Gross-Zagier formula and arithmetic applications* (With an appendix by B. Edixhoven), Annals of Math., submitted.

[**C**] I.V. Cerednik, *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)

[**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.

[**Jo-Li**] B. Jordan, R. Livné, *Local diophantine properties of Shimura curves*, Math. Ann. **270** (1985) 235-245.

[**KaMa**] N. Katz, B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Math. Studies **108**, Princeton Univ. Press

[**Ko**] V.A. Kolyvagin, *Euler Systems,* The Grothendieck Festschrift, Eds. P. Cartier, et al., vol. II, Progr. in Math. **87** Birkhäuser (1990) 435-483.

[**Ku**] A. Kurihara, *On some examples of equations defining Shimura curves and the Mumford uniformization,* J. Fac. Sci. Univ. Tokyo, sec. IA **25** (1979), 277-300.

[**LT**] J. Lubin, J. Tate, *Formal moduli for one-parameter formal Lie groups,* Bull. Soc. Math. Fr. **94**, (1966), 49-60.

[**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.

[**Mu**] D. Mumford, *An analytic construction of degenerating curves over complete local fields*, Compos. Math. **24** (1972) 129-174.

[**PR**] B. Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques*, Inv. Math. **89**, (1987) 455-510.

[**Rob**] D. Roberts, *Shimura curves analogous to* $X_0(N)$, Harvard PhD Thesis, 1989.

[**Ru**] K. Rubin, *p-adic L-functions and rational points on elliptic curves with complex multiplication*, Invent. Math. **107** (1992) 323-350.

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

[**ST**] G. Shimura, Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory,* Publ. Math. Soc. Japan **6**, (1961).

[**Te**] J. Teitelbaum, *On Drinfeld's universal formal group over the p-adic upper half-plane*, Math. Ann. **284** (1989) 647-674.

[**TW**] R. Taylor, A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** n. 3 (1995) 553- 572.

[**U**] D. Ulmer, *Local points on elliptic curves over modular curves*, Inter. Math. Res. Not. **7** (1995) 349-363.

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

[**Wi**] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math. **141**, n. 3 (1995) 443-551.