

STARK–HEEGNER POINTS ON MODULAR JACOBIANS

BY SAMIT DASGUPTA

ABSTRACT. – We present a construction which lifts Darmon’s Stark–Heegner points from elliptic curves to certain modular Jacobians. Let N be a positive integer and let p be a prime not dividing N . Our essential idea is to replace the modular symbol attached to an elliptic curve E of conductor Np with the universal modular symbol for $\Gamma_0(Np)$. We then construct a certain torus T over \mathbf{Q}_p and lattice $L \subset T$, and prove that the quotient T/L is isogenous to the maximal toric quotient $J_0(Np)^{p\text{-new}}$ of the Jacobian of $X_0(Np)$. This theorem generalizes a conjecture of Mazur, Tate, and Teitelbaum on the p -adic periods of elliptic curves, which was proven by Greenberg and Stevens. As a by-product of our theorem, we obtain an efficient method of calculating the p -adic periods of $J_0(Np)^{p\text{-new}}$.

© 2005 Elsevier SAS

RÉSUMÉ. – Nous donnons une construction qui relève celle des points de Stark–Heegner de Darmon des courbes elliptiques à certaines variétés jacobiniennes de courbes modulaires. Soit N un entier strictement positif et p un nombre premier ne divisant pas N . Notre idée principale est de remplacer le symbole modulaire attaché à une courbe elliptique E de conducteur Np par le symbole modulaire universel de $\Gamma_0(Np)$. Nous construisons alors un certain tore T sur \mathbf{Q}_p et un réseau $L \subset T$, et nous montrons que le quotient T/L est isogène au quotient torique maximal $J_0(Np)^{p\text{-new}}$ de la variété jacobienne de $X_0(Np)$. Ce théorème généralise une conjecture de Mazur, Tate et Teitelbaum sur les périodes p -adiques des courbes elliptiques, qui a été démontré par Greenberg et Stevens. En à-côté de notre théorème, nous obtenons une méthode efficace de calcul des périodes p -adiques de $J_0(Np)^{p\text{-new}}$.

© 2005 Elsevier SAS

Contents

1	Introduction	428
2	Previous uniformization results	429
2.1	Archimedean uniformization	429
2.2	Non-Archimedean uniformization	431
2.3	Generalities on p -adic measures	433
2.4	The Manin–Drinfeld theorem	434
3	An arithmetic uniformization and Stark–Heegner points	435
3.1	The universal modular symbol	436
3.2	Statement of the uniformization	437
3.3	Stark–Heegner points	440
4	Combinatorial observations	443
4.1	The p -adic valuation of the integration map	443
4.2	Hecke actions	444
4.3	The lattice L	446
5	Proof of Theorem 3.3	447

5.1	Connection with the Mazur–Tate–Teitelbaum conjecture	450
5.2	Hida families and the definition of \mathcal{L}_p	452
5.3	Proof of Proposition 5.1	453
5.4	Proof of Proposition 5.4	461
6	Computational examples	464
6.1	Genus one	465
6.2	Genus two	465
6.3	Genus three	466
	Appendix A. Hecke equivariance of the integration map	466
	References	467

1. Introduction

The theory of complex multiplication allows the construction of a collection of points on arithmetic curves over \mathbf{Q} , defined over Abelian extensions of quadratic imaginary fields. Foremost among these are Heegner points on modular curves, as described for example in [20]. By embedding a modular curve in its Jacobian (typically by sending a rational cusp to the origin), one may transfer Heegner points on the curve to each factor of its Jacobian. A study of the arithmetic properties of the points constructed in this fashion has yielded many striking results, most notably, the theorems of Gross and Zagier [21], Kolyvagin [26], and Kolyvagin and Logachëv [27].

The goal of [6] was to define certain points on elliptic curves analogous to Heegner points, except that they would be defined over Abelian extensions of real quadratic fields instead of imaginary quadratic fields. In the setting considered, the existence of such points is predicted by the conjecture of Birch and Swinnerton-Dyer. Darmon constructs these “Stark–Heegner points” analytically by replacing complex integration with a certain p -adic integral. The conjecture that Stark–Heegner points are defined over global number fields remains open.

The goal of the present article is to lift the construction of Stark–Heegner points from elliptic curves to certain modular Jacobians. Let N be a positive integer and let p be a prime not dividing N . Our essential idea is to replace the modular symbol attached to an elliptic curve E of conductor Np (a key tool in [6]) with the universal modular symbol for $\Gamma_0(Np)$. We then construct a certain torus T over \mathbf{Q}_p and lattice $L \subset T$, and prove that the quotient T/L is isogenous to the maximal toric quotient $J_0(Np)^{p\text{-new}}$ of the Jacobian of $X_0(Np)$. This theorem generalizes a conjecture of Mazur, Tate, and Teitelbaum [32] on the p -adic periods of elliptic curves, which was proven by Greenberg and Stevens [16,17]. Indeed, our proof borrows greatly from theirs.

Our isogeny theorem allows us to define Stark–Heegner points on the Abelian variety $J_0(Np)^{p\text{-new}}$. The points we define map to the Stark–Heegner points on E under the projection $J_0(Np)^{p\text{-new}} \rightarrow E$. We conjecture that they satisfy the same algebraicity properties. One interesting difference from the case of classical Heegner points is that our points, while lying on modular Jacobians, do not appear to arise from points on the modular curves themselves.

Although the construction of Stark–Heegner points is the most significant arithmetic application of our isogeny theorem, the result is interesting in its own right because it allows the practical computation of the p -adic periods of $J_0(Np)^{p\text{-new}}$.

In Section 2 we summarize known uniformization results, beginning with the complex analytic construction of $J_0(N)$ and classical Heegner points. We then discuss p -adic uniformization of Mumford curves via Schottky groups, and present the Manin–Drinfeld theorem on the uniformization of the Jacobian of a Mumford curve in the language of p -adic integration. In Section 3 we construct our analytic space T/L and state the isogeny theorem. We then use the isogeny theorem to define Stark–Heegner points on $J_0(Np)^{p\text{-new}}$. The remainder of the

article is devoted to proving the isogeny theorem. Section 5.1 describes precisely how our result generalizes the Mazur–Tate–Teitelbaum conjecture.

There are some differences to note between our presentation and that of [16]. First, by dealing with the entire Jacobian rather than a component associated to a particular newform, we avoid some technicalities arising in Hida theory. Furthermore, the role of $-2a'_p(2)$ in [16] is played by

$$\mathcal{L}_p := \text{the “derivative” of } 1 - U_p^2,$$

as defined in Section 5.2; accordingly we treat the cases of split and non-split reduction simultaneously. The proof that the \mathcal{L} -invariant of T/L is equal to \mathcal{L}_p is somewhat different from (though certainly bears commonalities with) what appears in [16]. Indeed, the space T/L is constructed from the group

$$\Gamma := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PSL}_2(\mathbf{Z}[1/p]) \text{ such that } N|c \right\}$$

and a study of its cohomology. The construction of Stark–Heegner points is contingent on the splitting of a certain 2-cocycle for Γ , which is proven by lifting measures on $\mathbf{P}^1(\mathbf{Q}_p)$ to the \mathbf{Z}_p^\times -bundle $\mathbf{X} = (\mathbf{Z}_p \times \mathbf{Z}_p)'$ of primitive vectors over this space. The connection between integrals on \mathbf{X} and p -adic L -functions is described in [2,7].

In Section 6, we give some computational data to demonstrate how the isogeny theorem may be used to calculate the p -adic periods of $J_0(Np)^{p\text{-new}}$.

2. Previous uniformization results

The classical theory of Abel–Jacobi gives a complex analytic uniformization of the Jacobian of a nonsingular proper curve over \mathbf{C} . We begin this section by recalling this construction for $X_0(N)$ and giving the definition of Heegner points on $J_0(N)$ using this uniformization. Manin and Drinfeld have also given a p -adic uniformization for the Jacobians of Mumford curves. We give a restatement of their result in the language of p -adic integration, which may thus be viewed as a p -adic Abel–Jacobi theory. Unfortunately, the p -adic uniformization of $J_0(p)$ that arises in this fashion does not allow the natural construction of Heegner-type points in an obvious manner. The constructions which occupy the remainder of this paper remedy this problem by finding an alternate p -adic uniformization of $J_0(Np)^{p\text{-new}}$. This section is entirely expository and only provides motivation for what follows.

2.1. Archimedean uniformization

The Abel–Jacobi theorem states that the Jacobian of a nonsingular proper curve X over \mathbf{C} is analytically isomorphic to the quotient of the dual of its space of 1-forms by the image of the natural integration map from $H_1(X(\mathbf{C}), \mathbf{Z})$. To execute this uniformization in practice, one often wants to understand the space of 1-forms and the first homology group of X explicitly. A general approach to this problem is given by Schottky uniformization. (See [37] for the original work and [23] for a modern summary and generalization.) The “retrosection” theorem of [25] states that there exists a Schottky group $\Gamma \subset \mathbf{PGL}_2(\mathbf{C})$ and an open set $\mathcal{H}_\Gamma \subset \mathbf{P}^1(\mathbf{C})$ such that $X(\mathbf{C})$ is analytically isomorphic to $\Gamma \backslash \mathcal{H}_\Gamma$. Among its other properties, the group Γ is free of rank g , the genus of the curve X . Under certain convergence conditions, one may describe the Jacobian of X as the quotient of a split torus $(\mathbf{C}^\times)^g$ by the image of an explicit homomorphism from Γ .

While Schottky uniformization is useful as a general theory, it does not necessarily provide a method of constructing rational points on X or its Jacobian in cases of arithmetic interest. Furthermore, if the parameterizing group Γ cannot be found explicitly, one may not even be able to calculate the periods of X in practice.

In our case of study, namely the modular curves $X_0(N)$, it is essential to exploit the “arithmeticity” given by modularity. By its moduli description, the set of complex points of $X_0(N)$ can be identified with the quotient of the extended upper half plane $\mathcal{H}^* = \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$ by the discrete group $\Gamma_0(N)$ acting on the left via linear fractional transformations:

$$(1) \quad X_0(N)(\mathbf{C}) \cong \Gamma_0(N) \backslash \mathcal{H}^*.$$

Denote by g the genus of $X_0(N)$, and let $\mathcal{S}_2(N)$ denote the space of cusp forms of level N . For any $\tau_1, \tau_2 \in \mathcal{H}^*$, we can define a homomorphism denoted $\int_{\tau_1}^{\tau_2}$ from $\mathcal{S}_2(N)$ to \mathbf{C} via a complex line integral:

$$\int_{\tau_1}^{\tau_2} : f \mapsto 2\pi i \int_{\tau_1}^{\tau_2} f(z) dz.$$

Since f is a modular form of level N , this value is unchanged if τ_1 and τ_2 are replaced by $\gamma\tau_1$ and $\gamma\tau_2$, respectively, for $\gamma \in \Gamma_0(N)$. Thus if $\text{Div}_0 \mathcal{H}^*$ denotes the group of degree-zero divisors on the points of the extended upper half plane, we obtain a homomorphism

$$(2) \quad (\text{Div}_0 \mathcal{H}^*)_{\Gamma_0(N)} \rightarrow \text{Hom}(\mathcal{S}_2(N), \mathbf{C})$$

$$[\tau_1] - [\tau_2] \mapsto \left(f \mapsto 2\pi i \int_{\tau_2}^{\tau_1} f(z) dz \right).$$

The short exact sequence

$$0 \rightarrow \text{Div}_0 \mathcal{H}^* \rightarrow \text{Div} \mathcal{H}^* \rightarrow \mathbf{Z} \rightarrow 0$$

gives rise to a boundary map in homology:

$$(3) \quad \delta : H_1(\Gamma_0(N), \mathbf{Z}) \rightarrow (\text{Div}_0 \mathcal{H}^*)_{\Gamma_0(N)}.$$

Denote the composition of the maps in (2) and (3) by

$$\Phi_1 : H_1(\Gamma_0(N), \mathbf{Z}) \rightarrow \text{Hom}(\mathcal{S}_2(N), \mathbf{C}),$$

and let L denote the image of Φ_1 . The group L is free Abelian of rank $2g$ and is Hecke-stable. For $x \in \mathcal{H}^*$, let \tilde{x} represent the image of x in $X_0(N)(\mathbf{C}) = \Gamma_0(N) \backslash \mathcal{H}^*$. Under these notations, the Abel–Jacobi theorem may be stated as follows:

THEOREM 2.1. – *The map $[\tilde{x}] - [\tilde{y}] \mapsto \int_y^x$ induces a complex analytic uniformization of the Jacobian of $X_0(N)$:*

$$J_0(N)(\mathbf{C}) \cong \text{Hom}(\mathcal{S}_2(N), \mathbf{C})/L.$$

Let $\tau \in \mathcal{H}^*$ lie in an imaginary quadratic subfield K of \mathbf{C} . Then

$$P_\tau := \int_{\infty}^{\tau} \in \text{Hom}(\mathcal{S}_2(N), \mathbf{C})/L = J_0(N)(\mathbf{C})$$

is a *Heegner point* on $J_0(N)$. The theory of complex multiplication shows that this analytically defined point is actually defined over an Abelian extension of K , and it furthermore prescribes the action of the Galois group of K on this point.

The goal of the remainder of this section is to present the theory of p -adic uniformization of Jacobians of degenerating curves via Schottky groups, as studied by Tate, Mumford, Manin, and Drinfeld, in the language of p -adic integration. The standard presentation of this subject (see [15], for example) involves certain theta functions that often have no direct analogue in the complex analytic situation because of convergence issues. Thus our new notation, inspired by [1], allows one to draw a more direct parallel between the complex analytic and p -adic settings. (The ideas we have drawn from in [1] appear in the construction of certain p -adic L -functions.)

2.2. Non-Archimedean uniformization

Let K be a local field (a locally compact field, complete with respect to a discrete valuation). Denote by C the completion of an algebraic closure of K , and by k the residue field of K . A discrete subgroup Γ of $\mathbf{PGL}_2(K)$ is called a Schottky group if it is finitely generated and has no nontrivial elements of finite order; such a group is necessarily free. The group Γ acts on $\mathbf{P}^1(K)$ by linear fractional transformations. The set of limit points \mathcal{L} of Γ is defined to be the set of $P \in \mathbf{P}^1(K)$ such that there exist $Q \in \mathbf{P}^1(K)$ and distinct $\gamma_n \in \Gamma$ with $\gamma_n Q$ converging to P . For any extension $F \subset C$ of K , define $\mathcal{H}_\Gamma(F) = \mathbf{P}^1(F) - \mathcal{L}$.

A curve X over K is called a Mumford curve if the stable reduction of X contains only rational curves that intersect at normal crossings defined over k . The curve $X_0(p)$ over the quadratic unramified extension of \mathbf{Q}_p is such a curve. Mumford has proven that for every Mumford curve X , there exists a Schottky group $\Gamma \subset \mathbf{PGL}_2(K)$ and a $\text{Gal}(C/K)$ -equivariant rigid analytic isomorphism

$$(4) \quad X(C) \cong \Gamma \backslash \mathcal{H}_\Gamma(C).$$

Furthermore, the Schottky group Γ satisfying (4) is unique up to conjugation in $\mathbf{PGL}_2(K)$. It is free of rank g , the genus of X .

To proceed onwards to a p -adic uniformization of the Jacobian of X , we must first present an analogue of the complex line integrals appearing in Theorem 2.1. Let \mathcal{L} have the induced topology from $\mathbf{P}^1(K)$.

DEFINITION 2.1. – Let H be a free Abelian group of finite rank. The group $\text{Meas}(\mathcal{L}, H)$ of additive measures on \mathcal{L} with values in H is the group of maps μ which assign to each compact open subset U of \mathcal{L} an element $\mu(U)$ of H , such that

- $\mu(U) + \mu(V) = \mu(U \cup V)$ for disjoint open compacts U and V , and
- $\mu(\mathcal{L}) = 0$.

The group $\text{Meas}(\mathcal{L}, H)$ has a natural Γ action, given by $(\gamma\mu)(U) := \mu(\gamma^{-1}U)$. Let μ denote a Γ -invariant element of $\text{Meas}(\mathcal{L}, H)$.

DEFINITION 2.2. – Let $d \in \text{Div}_0 \mathcal{H}_\Gamma(C)$ be a degree-zero divisor. Choose a rational function f_d on $\mathbf{P}^1(C)$ with divisor d , and define the *multiplicative integral*:

$$(5) \quad \int_d \omega_\mu := \int_{\mathcal{L}} f_d(t) d\mu(t) \\ := \lim_{\|\mathcal{U}\| \rightarrow 0} \prod_{U \in \mathcal{U}} f_d(t_U) \otimes \mu(U) \in C^\times \otimes_{\mathbf{Z}} H.$$

Here the limit is taken over uniformly finer disjoint covers \mathcal{U} of \mathcal{L} by nonempty open compact subsets U , and t_U is an arbitrarily chosen point of U .

Remark 2.2. – The products in (5) are finite since \mathcal{L} is compact. The limit converges since μ is a measure. Also, since $\mu(\mathcal{L}) = 0$, the multiplicative integral on \mathcal{L} of a constant (with respect to μ) vanishes, so Definition 2.2 is independent of the choice of f_d .

For a complete field extension F of K lying in C , denote by $\mathcal{H}_\Gamma(F)$ the space $\mathbf{P}^1(F) - \mathcal{L}$. It is clear that if $d \in \text{Div}_0 \mathcal{H}_\Gamma(F)$, then

$$\int_d \omega_\mu \in F^\times \otimes H.$$

The Γ -invariance of μ implies:

PROPOSITION 2.3. – *The multiplicative integral is Γ -invariant:*

$$\int_d \omega_\mu = \int_{\gamma d} \omega_\mu \in C^\times \otimes H$$

for $d \in \mathcal{H}_\Gamma(C)$ and $\gamma \in \Gamma$.

Thus the multiplicative integral defines a map

$$(6) \quad \int \omega_\mu : (\text{Div}_0 \mathcal{H}_\Gamma)_\Gamma \rightarrow \mathbf{G}_m \otimes H.$$

Here we view \mathcal{H}_Γ and \mathbf{G}_m as functors on the category of complete field extensions of K contained in C . Let T denote the torus $\mathbf{G}_m \otimes H$.

Remark 2.4. – If $\tau_1, \tau_2 \in \mathcal{H}_\Gamma(C)$ and $\tau_i \neq \infty$, we write

$$\int_{\tau_1}^{\tau_2} \omega_\mu = \int_{[\tau_2]-[\tau_1]} \omega_\mu = \int_{\mathcal{L}} \left(\frac{t - \tau_2}{t - \tau_1} \right) d\mu(t)$$

as in [6].

As we saw in (3) above, there is a canonical map

$$(7) \quad H_1(\Gamma, \mathbf{Z}) \rightarrow (\text{Div}_0 \mathcal{H}_\Gamma)_\Gamma,$$

which composed with (6) yields

$$\Phi_1 : H_1(\Gamma, \mathbf{Z}) \rightarrow T.$$

Let L denote the image of Φ_1 .

As we will describe, there is a universal group H admitting a Γ -invariant measure μ , in the sense that if $\mu' \in \text{Meas}(\mathcal{L}, H')^\Gamma$, then there exists a homomorphism $f : H \rightarrow H'$ such that $\mu'(U) = f(\mu(U))$ for all compact opens $U \subset \mathcal{L}$. To properly express this fact, we introduce the Bruhat–Tits tree associated to \mathcal{L} . We then analyze the rigid analytic space T/L in the universal setting.

2.3. Generalities on p -adic measures

We begin by recalling the Bruhat–Tits tree \mathcal{T} of $\mathbf{PGL}_2(K)$ (see [15] for a general reference). Denote by \mathcal{O} the ring of integers of K , by π a uniformizer of \mathcal{O} , and by $k = \mathcal{O}/\pi\mathcal{O}$ the residue field of K . The vertices of \mathcal{T} are equivalence classes of free rank two \mathcal{O} -submodules of $K \oplus K$, where two such modules are considered equivalent if they are homothetic by an element of K^\times . Two vertices are connected by an edge if they can be represented by modules M and N with $N \subset M$ and $M/N \cong k$; this is clearly a symmetric relation. The unoriented graph \mathcal{T} which results from these definitions is a regular tree of degree $\#P^1(k)$. The group $\mathbf{PGL}_2(K)$ acts naturally on the tree.

Let v^* denote the vertex corresponding to $\mathcal{O} \oplus \mathcal{O}$ and let w^* denote the vertex corresponding to $\mathcal{O} \oplus \pi\mathcal{O}$. The stabilizer of v^* in $\mathbf{PGL}_2(K)$ is $\mathbf{PGL}_2(\mathcal{O})$. The matrix $P = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}$ sends w^* to v^* , and hence the stabilizer of w^* is $P^{-1}\mathbf{PGL}_2(\mathcal{O})P$. Let e^* denote the oriented edge from w^* to v^* . The stabilizer of e^* in $\mathbf{PGL}_2(K)$ is the intersection of the stabilizers of v^* and w^* , namely, the set of matrices of $\mathbf{PGL}_2(\mathcal{O})$ that are upper triangular modulo π . This group equals the stabilizer of \mathcal{O} in $\mathbf{PGL}_2(K)$ under linear fractional transformations. Thus if we associate to the oriented edge e^* the compact open set $U_{e^*} := \mathcal{O} \subset P^1(K)$, this extends to an assignment of a compact open subset of $P^1(K)$ to each oriented edge of the tree via $\mathbf{PGL}_2(K)$ -invariance:

$$U_{\gamma e^*} := \gamma\mathcal{O} \quad \text{for all } \gamma \in \mathbf{PGL}_2(K).$$

We note some essential properties of this assignment:

- For an oriented edge e , the oppositely oriented edge \bar{e} satisfies $U_{\bar{e}} = P^1(K) - U_e$.
- For each vertex v , the sets U_e as e ranges over the edges emanating from v form a disjoint cover of $P^1(K)$.
- The sets U_e form a basis of compact open subsets of $P^1(K)$.

Let us now return to our Schottky group Γ .

DEFINITION 2.3. – The *Bruhat–Tits tree of Γ* is the subtree $\mathcal{T}_\Gamma \subset \mathcal{T}$ spanned by all edges such that both open sets corresponding to the two possible orientations of the edge contain an element of \mathcal{L} .

The group Γ acts on the tree \mathcal{T}_Γ . To each oriented edge e of \mathcal{T}_Γ we associate the compact open set $U_e(\Gamma) = U_e \cap \mathcal{L}$. The sets $U_e(\Gamma)$ satisfy the properties above with $P^1(K)$ replaced by \mathcal{L} .

An *end* of a tree is a path without backtracking that is infinite in exactly one direction, modulo the relation that two such paths are equivalent if they are eventually equal.¹ The ends of \mathcal{T}_Γ are naturally in bijection with \mathcal{L} , by sending an end to the unique point in the intersection of all $U_e(\Gamma)$ for the oriented edges e of the end.

The space \mathcal{H}_Γ may be viewed as a thickening of the tree \mathcal{T}_Γ by means of the reduction map

$$\text{red} : \mathcal{H}_\Gamma \rightarrow \mathcal{T}_\Gamma.$$

We will define the reduction map only on the points of \mathcal{H}_Γ defined over finite unramified extensions F of K . In this case, the tree \mathcal{T} of $\mathbf{PGL}_2(K)$ is naturally a subtree of the Bruhat–Tits tree \mathcal{T}_F of $\mathbf{PGL}_2(F)$, and hence the tree \mathcal{T}_Γ may be viewed as a subtree of \mathcal{T}_F as well. A point $u \in \mathcal{H}_\Gamma(F)$ corresponds to an end of \mathcal{T}_F ; this end may be represented by a unique path originating from a vertex v_u in \mathcal{T}_Γ and intersecting \mathcal{T}_Γ only at v_u . The vertex v_u is defined to be the reduction of u .

¹ Rigorously, an end is an infinite sequence v_0, v_1, \dots of distinct vertices of the tree such that (v_i, v_{i+1}) is an oriented edge, modulo the relation that $\{v_i\} \sim \{w_i\}$ if there exist n, m such that $v_{n+i} = w_{m+i}$ for all $i \geq 0$.

The Bruhat–Tits tree of Γ allows one to understand measures on \mathcal{L} combinatorially. Denote by E_Γ (respectively V_Γ) the set of all oriented edges (respectively vertices) of the tree \mathcal{T}_Γ . Denote by C_E the group $\text{Div } E_\Gamma / (e + \bar{e})$, the Abelian group generated freely by the oriented edges of \mathcal{T}_Γ modulo the relation that oppositely oriented edges add to zero. Denote by C_V the group $\text{Div } V_\Gamma$. Define a trace map $\text{Tr} : C_V \rightarrow C_E$ by sending each vertex v to the sum of the edges of \mathcal{T}_Γ with source vertex v . The trace map is injective. The correspondence $e \mapsto U_e(\Gamma)$ shows that for each H , the group $\text{Meas}(\mathcal{L}, H)$ is the kernel of the dual of the trace map:

$$(8) \quad \text{Meas}(\mathcal{L}, H)^\Gamma = \ker(\text{Hom}(C_E, H) \xrightarrow{\text{Tr}^*} \text{Hom}(C_V, H))^\Gamma$$

$$(9) \quad = \ker(\text{Hom}((C_E)_\Gamma, H) \xrightarrow{\text{Tr}^*} \text{Hom}((C_V)_\Gamma, H)).$$

The right-hand side of (8) is called the group of Γ -invariant harmonic cocycles on \mathcal{T}_Γ with values in H . Now $(C_E)_\Gamma \cong C_{E'}$ and $(C_V)_\Gamma \cong C_{V'}$ where $C_{E'}$ and $C_{V'}$ are the corresponding groups for the finite quotient graph $\Gamma \backslash \mathcal{T}_\Gamma$. Thus from basic topology, one identifies (9) with

$$H_1(\Gamma \backslash \mathcal{T}_\Gamma, H) = \text{Hom}(H^1(\Gamma \backslash \mathcal{T}_\Gamma, \mathbf{Z}), H).$$

Since Γ acts freely on the contractible space \mathcal{T}_Γ the cohomology group $H^1(\Gamma \backslash \mathcal{T}_\Gamma, \mathbf{Z})$ is canonically identified with

$$H^1(\Gamma, \mathbf{Z}) = \text{Hom}(\Gamma, \mathbf{Z}).$$

Hence the universal free Abelian group admitting a Γ -invariant measure on \mathcal{L} is precisely the rank g group $H = \text{Hom}(\Gamma, \mathbf{Z})$. The associated universal Γ -invariant measure μ may be described explicitly as follows. Let e be an oriented edge of \mathcal{T}_Γ , and let $\gamma \in \Gamma$. Choose any vertex v of \mathcal{T}_Γ and consider the unique path P from v to γv in \mathcal{T}_Γ . For each oriented edge in the path P , count $+1$ if the edge is Γ -equivalent to e , count -1 if the edge is Γ -equivalent to \bar{e} , and count 0 otherwise. The total sum of these counts is independent of v and equals the value $\mu(U_e)(\gamma) \in \mathbf{Z}$.

2.4. The Manin–Drinfeld theorem

Let $H = \text{Hom}(\Gamma, \mathbf{Z})$ be as above and let μ be the associated universal Γ -invariant measure on \mathcal{L} . In Section 2.2 we associated to the pair (H, μ) a torus T and subgroup L of T via the technique of p -adic integration. For $x \in \mathcal{H}_\Gamma(C)$, let \tilde{x} represent the image of x in $X(C) = \mathcal{H}_\Gamma(C)/\Gamma$.

THEOREM 2.5 (Manin–Drinfeld). – *The map*

$$[\tilde{x}] - [\tilde{y}] \mapsto \int_y^x \omega_\mu$$

induces a $\text{Gal}(C/K)$ -equivariant rigid analytic isomorphism between the rigid analytic space associated to the C -valued points of the Jacobian of the curve X and $T(C)/L$.

Proof. – The original statement of the Manin–Drinfeld theorem is given in terms of automorphic functions for the group Γ . Recall from [15, §II.2] the definition of the theta function $\Theta(a, b; z)$ for $a, b, z \in \mathcal{H}_\Gamma(C)$, and $z \notin \Gamma a, \Gamma b$:

$$\Theta(a, b; z) = \prod_{\gamma \in \Gamma} \frac{z - \gamma a}{z - \gamma b} \in C^\times.$$

(One must assume that ∞ is not a limit point of Γ to ensure convergence of the product above.)

The following result relates our multiplicative integral to values of theta functions, and allows one to derive our version of Theorem 2.5 from the original statement [15,29].

PROPOSITION 2.6. – *Let a, b be elements of $\mathcal{H}_\Gamma(F)$. Viewing the universal multiplicative integral as a homomorphism from Γ to F^\times , we have*

$$(10) \quad \left(\int_b^a \omega_\mu \right) (\delta) = \frac{\Theta(a, b; \delta z)}{\Theta(a, b; z)}$$

for any $z \in \mathcal{H}_\Gamma(C) - (\Gamma a \cup \Gamma b)$ and $\delta \in \Gamma$. (The automorphy properties of Θ imply that the right-hand side is independent of z .)

The proof of this proposition is given in [10, Proposition 2.3.1], but the ideas of the proof are present already in [1].

Theorem 2.5 is the p -adic analogue of the Abel–Jacobi theorem. However, it does not allow for the obvious construction of any Heegner-type points in the case $X = X_0(p)$. In fact, since Mumford’s group Γ is not given in an explicit way and is probably not an arithmetic group, it appears unclear how to calculate the periods of $J_0(p)$ (i.e. calculate L) using this uniformization. (See [14] for the calculation of L modulo p using this theory, however.) Accordingly, one needs to find an alternative uniformization for modular Jacobians which uses arithmetic groups in a crucial way; this is taken up in the next section.

3. An arithmetic uniformization and Stark–Heegner points

Let p be a prime number and $N \geq 1$ an integer not divisible by p . Write $M = Np$. In this section we will present a p -adic uniformization of the maximal quotient of $J_0(M)$ with toric reduction at p . A key idea, suggested by the definitions of [6], is that the p -adic arithmetic of $J_0(M)$ is intimately linked with the group

$$(11) \quad \Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PSL}_2(\mathbf{Z}[1/p]) \text{ such that } N|c \right\}$$

and its homology. The group Γ is not discrete as a subgroup of $\mathbf{PGL}_2(\mathbf{Q}_p)$ and hence acts with dense orbits on \mathbf{P}^1 . In this setting, with $K = \mathbf{Q}_p$, the limit point set equals $\mathcal{L} := \mathbf{P}^1(\mathbf{Q}_p)$. (Since Γ is not discrete, if the ground field K is enlarged then the limit point set $\mathcal{L}(K) = \mathbf{P}^1(K)$ is enlarged as well; thus our definition of $\mathcal{L} = \mathbf{P}^1(\mathbf{Q}_p)$ is slightly ad hoc.) We also have

$$\mathcal{H}_\Gamma(\mathbf{C}_p) = \mathcal{H}_p := \mathbf{P}^1(\mathbf{C}_p) - \mathbf{P}^1(\mathbf{Q}_p),$$

where \mathbf{C}_p is the completion of an algebraic closure of \mathbf{Q}_p .

A measure on $\mathbf{P}^1(\mathbf{Q}_p)$ is given by a harmonic cocycle on the entire Bruhat–Tits tree \mathcal{T} of $\mathbf{PGL}_2(\mathbf{Q}_p)$. Repeating the analysis of Section 2.3, one finds that there are no non-trivial Γ -invariant measures on $\mathbf{P}^1(\mathbf{Q}_p)$. This problem can be remedied by introducing a Γ -invariant measure-valued modular symbol as follows.

Let $\mathcal{M} := \text{Div}_0 \mathbf{P}^1(\mathbf{Q})$ be the group of degree-zero divisors on $\mathbf{P}^1(\mathbf{Q})$, viewed as cusps of the complex upper half plane. The group \mathcal{M} is defined by the exact sequence

$$(12) \quad 0 \rightarrow \mathcal{M} \rightarrow \text{Div } \mathbf{P}^1(\mathbf{Q}) \rightarrow \mathbf{Z} \rightarrow 0.$$

The group Γ acts on \mathcal{M} via its action on $\mathbf{P}^1(\mathbf{Q})$ by linear fractional transformations. For a free Abelian group H , a $\text{Meas}(\mathbf{P}^1(\mathbf{Q}_p), H)$ -valued modular symbol is a homomorphism

$$\mathcal{M} \rightarrow \text{Meas}(\mathbf{P}^1(\mathbf{Q}_p), H), \quad m \mapsto \mu_m.$$

The group of modular symbols μ has a Γ -action given by

$$(\gamma^{-1}\mu)_m(U) = \mu_{\gamma m}(\gamma U).$$

Motivated by Sections 2.3 and 2.4, we will explore the universal Γ -invariant modular symbol of measures on $\mathbf{P}^1(\mathbf{Q}_p)$.

3.1. The universal modular symbol

One can interpret the group of co-invariants

$$\mathcal{M}_{\Gamma_0(M)} = H_0(\Gamma_0(M), \mathcal{M})$$

geometrically as follows. Given a divisor $[x] - [y] \in \mathcal{M}$, consider a path from x to y in \mathcal{H}^* . If we make the identification $\Gamma_0(M)\backslash\mathcal{H}^* = X_0(M)(\mathbf{C})$, the image of this path gives a well defined element of $H_1(X_0(M), \text{cusps}, \mathbf{Z})$, the singular homology of the Riemann surface $X_0(M)(\mathbf{C})$ relative to the cusps. Manin [28] proves that this map induces an isomorphism between $H_1(X_0(M), \text{cusps}, \mathbf{Z})$ and the maximal torsion-free quotient of $\mathcal{M}_{\Gamma_0(M)}$. This maximal torsion-free quotient will be denoted $H_0(\Gamma_0(M), \mathcal{M})_T$. The torsion of $H_0(\Gamma_0(M), \mathcal{M})$ is finite and supported at 2 and 3. The projection

$$\mathcal{M} \rightarrow \mathcal{M}_{\Gamma_0(M)} \rightarrow H_1(X_0(M), \text{cusps}, \mathbf{Z})$$

is called the *universal modular symbol* for $\Gamma_0(M)$.

The points of $X_0(M)$ over \mathbf{C} correspond to isomorphism classes of pairs (E, C_M) of generalized elliptic curves E/C equipped with a cyclic subgroup $C_M \subset E$ of order M . To such a pair we can associate two points of $X_0(N)$, namely the points corresponding to the pairs (E, C_N) and $(E/C_p, C_M/C_p)$, where C_p and C_N are the subgroups of C_M of order p and N , respectively. This defines two morphisms of curves

$$(13) \quad f_1 : X_0(M) \rightarrow X_0(N) \quad \text{and} \quad f_2 : X_0(M) \rightarrow X_0(N),$$

each of which is defined over \mathbf{Q} . The map f_2 is the composition of f_1 with the Atkin–Lehner involution W_p on $X_0(M)$. Write $f_* = f_{1*} \oplus f_{2*}$ and $f^* = f_1^* \oplus f_2^*$ (respectively \overline{f}_* and \overline{f}^*) for the induced maps on (relative) singular homology:

$$\begin{aligned} f_* &: H_1(X_0(M), \mathbf{Z}) \rightarrow H_1(X_0(N), \mathbf{Z})^2, \\ f^* &: H_1(X_0(N), \mathbf{Z})^2 \rightarrow H_1(X_0(M), \mathbf{Z}), \\ \overline{f}_* &: H_1(X_0(M), \text{cusps}, \mathbf{Z}) \rightarrow H_1(X_0(N), \text{cusps}, \mathbf{Z})^2, \\ \overline{f}^* &: H_1(X_0(N), \text{cusps}, \mathbf{Z})^2 \rightarrow H_1(X_0(M), \text{cusps}, \mathbf{Z}). \end{aligned}$$

Via the universal modular symbol, the last two maps are identified with maps²

²In purely homological terms, f_{1*} is corestriction, and f_{2*} is the composition $f_{1*} \circ W_p$; similarly for f^* and restriction.

$$\begin{aligned} \overline{f}_* &: H_0(\Gamma_0(M), \mathcal{M}) \rightarrow H_0(\Gamma_0(N), \mathcal{M})^2, \\ \overline{f}^* &: H_0(\Gamma_0(N), \mathcal{M})^2 \rightarrow H_0(\Gamma_0(M), \mathcal{M}). \end{aligned}$$

Define

$$(14) \quad \overline{H} := (H_1(X_0(M), \text{cusps}, \mathbf{Z}) / \overline{f}^*(H_1(X_0(N), \text{cusps}, \mathbf{Z})^2))_T$$

$$(15) \quad \cong (H_0(\Gamma_0(M), \mathcal{M}) / \overline{f}^*(H_0(\Gamma_0(N), \mathcal{M})^2))_T;$$

$$(16) \quad H := (H_1(X_0(M), \mathbf{Z}) / f^*(H_1(X_0(N), \mathbf{Z})^2))_T.$$

PROPOSITION 3.1. – *Let \overline{H} be as in (15). There is a unique Γ -invariant $\text{Meas}(\mathbf{P}^1(\mathbf{Q}_p), \overline{H})$ -valued modular symbol $\overline{\mu}$ such that $\overline{\mu}_m(\mathbf{Z}_p) = m$ for all $m \in \mathcal{M}$. Furthermore, the pair $(\overline{H}, \overline{\mu})$ is universal.*

Proof. – Let C_E denote the free Abelian group on the oriented edges of \mathcal{T} modulo the relation $e + \overline{e} = 0$ for all edges, and let C_V denote the free Abelian group on the vertices of \mathcal{T} . Let $\text{Tr}: C_V \rightarrow C_E$ denote the trace map which sends a vertex v to the sum of the oriented edges with source vertex v . The correspondence between harmonic cocycles and measures shows that a Γ -invariant modular symbol of measures on $\mathbf{P}^1(\mathbf{Q}_p)$ with values in a group A is equivalent to an element of

$$\ker(\text{Hom}(C_E \otimes \mathcal{M}, A) \xrightarrow{\text{Tr}^*} \text{Hom}(C_V \otimes \mathcal{M}, A))^\Gamma.$$

Hence there is a universal such modular symbol taking values in

$$(17) \quad (C_E \otimes \mathcal{M})_\Gamma / \text{Tr}(C_V \otimes \mathcal{M})_\Gamma.$$

The action of Γ on the tree \mathcal{T} is particularly easy to describe [38, §II]. Each oriented edge of \mathcal{T} is equivalent to either e^* or \overline{e}^* ; each vertex is equivalent to either v^* or w^* . The stabilizers of v^* and w^* in Γ are $\Gamma_0(N)$ and $P^{-1}\Gamma_0(N)P$, respectively, where P is the matrix $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. The stabilizer of e^* is the intersection of these, namely $\Gamma_0(M)$; also, $U_{e^*} = \mathbf{Z}_p$. Shapiro’s Lemma identifies (17) with

$$(18) \quad \mathcal{M}_{\Gamma_0(M)} / \text{Tr}(\mathcal{M}_{\Gamma_0(N)} \oplus \mathcal{M}_{P^{-1}\Gamma_0(N)P}).$$

Noting that the map $m \mapsto Pm$ defines an isomorphism

$$H_*(P^{-1}\Gamma_0(N)P, \mathcal{M}) \rightarrow H_*(\Gamma_0(N), \mathcal{M})$$

and that the map Tr in (18) is nothing but the map denoted \overline{f}^* in (15) proves the result. \square

3.2. Statement of the uniformization

The Abelian variety $J_0(M)^{p\text{-new}}$ is defined to be the quotient of $J_0(M)$ by the sum of the images of the Picard maps on Jacobians associated to the maps f_1 and f_2 of (13). This is the Abelian variety with purely toric reduction at p for which we will provide a uniformization (up to isogeny).

PROPOSITION 3.2. – *If we write g for the dimension of $J_0(M)^{p\text{-new}}$, the free Abelian groups H and \overline{H} have ranks $2g$ and $2g + 1$ respectively, and the natural map $H \rightarrow \overline{H}$ is an injection.*

Proof. – It is well known that f^* is injective and that H has rank $2g$. Consider the following commutative diagram of relative homology sequences:

$$(19) \quad \begin{array}{ccccccc} 0 & \longrightarrow & H_1(X_0(N), \mathbf{Z})^2 & \longrightarrow & H_1(X_0(N), \text{cusps}, \mathbf{Z})^2 & \longrightarrow & C(N)^2 \longrightarrow 0 \\ & & \downarrow f^* & & \downarrow \overline{f^*} & & \downarrow \\ 0 & \longrightarrow & H_1(X_0(M), \mathbf{Z}) & \longrightarrow & H_1(X_0(M), \text{cusps}, \mathbf{Z}) & \longrightarrow & C(M) \longrightarrow 0 \end{array}$$

Here $C(N)$ and $C(M)$ denote the groups of degree-zero divisors on the set of cusps of $X_0(N)$ and $X_0(M)$, respectively. If c denotes the number of cusps of $X_0(N)$, these are free Abelian groups of rank $c - 1$ and $2c - 1$, respectively. Above each cusp of $X_0(N)$ (under the map f_1) lie two cusps of $X_0(M)$, one of which has ramification index p and the other one of which is unramified. The map W_p on $X_0(M)$ interchanges these two cusps. This implies that the map $C(N)^2 \rightarrow C(M)$ of (19) is injective and that the torsion subgroup of its cokernel has exponent dividing $p^2 - 1$. Since H and \overline{H} are the cokernels of f^* and $\overline{f^*}$, the snake lemma yields the proposition. (Note that we have also shown that $\overline{f^*}$ is injective.) \square

To define a modular symbol that takes values in H rather than \overline{H} , we choose a map

$$\psi: \overline{H} \rightarrow H.$$

We will require two properties of the map ψ , whose uses will later become evident:

- The groups \overline{H} and H have natural Hecke actions described in Section 4.2. We assume that the map ψ is Hecke-equivariant.
- We assume that the composition of ψ with the inclusion $H \subset \overline{H}$ is an endomorphism of H with finite cokernel.

Let $\overline{\mu}$ be the universal Γ -invariant modular symbol of measures on $\mathbf{P}^1(\mathbf{Q}_p)$ from Proposition 3.1, and define $\mu := \psi \circ \overline{\mu}$. Then μ is a Γ -invariant $\text{Meas}(\mathbf{P}^1(\mathbf{Q}_p), H)$ -valued modular symbol.

DEFINITION 3.1. – Let $d \in \text{Div}_0 \mathcal{H}_p$ be a degree-zero divisor, and let $m \in \mathcal{M}$. Choose a rational function f_d on $\mathbf{P}^1(\mathbf{C}_p)$ with divisor d , and define the *multiplicative double integral*:

$$(20) \quad \begin{aligned} \int_d \int_m \omega_\mu &:= \int_{\mathbf{P}^1(\mathbf{Q}_p)} f_d(t) d\mu_m(t) \\ &:= \lim_{\|\mathcal{U}\| \rightarrow 0} \prod_{U \in \mathcal{U}} f_d(t_U) \otimes \mu_m(U) \in \mathbf{C}_p^\times \otimes_{\mathbf{Z}} H, \end{aligned}$$

with the notation as in Definition 2.2.

The Γ -invariance of μ implies that this integral is Γ -invariant:

$$\int_{\gamma d} \int_{\gamma m} \omega_\mu = \int_d \int_m \omega_\mu \quad \text{for } \gamma \in \Gamma.$$

Letting T denote the torus $T = \mathbf{G}_m \otimes_{\mathbf{Z}} H$, we obtain a homomorphism

$$(21) \quad ((\text{Div}_0 \mathcal{H}_p) \otimes \mathcal{M})_\Gamma \rightarrow T.$$

Consider the short exact sequence of Γ -modules defining $\text{Div}_0 \mathcal{H}_p$:

$$0 \rightarrow \text{Div}_0 \mathcal{H}_p \rightarrow \text{Div} \mathcal{H}_p \rightarrow \mathbf{Z} \rightarrow 0.$$

After tensoring with \mathcal{M} , the long exact sequence in homology gives a boundary map

$$(22) \quad \delta: H_1(\Gamma, \mathcal{M}) \rightarrow ((\text{Div}_0 \mathcal{H}_p) \otimes \mathcal{M})_{\Gamma}.$$

The long exact sequence in homology associated to the sequence (12) defining \mathcal{M} gives a boundary map

$$(23) \quad \delta: H_2(\Gamma, \mathbf{Z}) \rightarrow H_1(\Gamma, \mathcal{M}).$$

Denote the composition of the homomorphisms in (21) and (22) by

$$\Phi_1: H_1(\Gamma, \mathcal{M}) \rightarrow T(\mathbf{C}_p),$$

and the further composition with (23) by

$$\Phi_2: H_2(\Gamma, \mathbf{Z}) \rightarrow T(\mathbf{C}_p).$$

Each element in the image of Φ_1 may be expressed in terms of double integrals involving divisors d supported on $\mathcal{H}_{\Gamma}(F)$ for any nontrivial extension F of \mathbf{Q}_p . By the independence of the integral from the choice of F , it follows that the image of Φ_1 , and hence Φ_2 as well, lies in $T(\mathbf{Q}_p)$.

Denote by L the image of Φ_2 . The torus T inherits a Hecke action from H . We may now state our main result.

THEOREM 3.3. – *Let K_p denote the quadratic unramified extension of \mathbf{Q}_p . The group L is a discrete, Hecke-stable subgroup of $T(\mathbf{Q}_p)$ of rank $2g$. The quotient T/L admits a Hecke-equivariant isogeny over K_p to the rigid analytic space associated to the product of two copies of $J_0(M)^{p\text{-new}}$.*

During the course of proving Theorem 3.3, we will give some control over the set of primes appearing in the degree of this isogeny. Also, we will see that if one lets the nontrivial element of $\text{Gal}(K_p/\mathbf{Q}_p)$ act on T/L by the Hecke operator U_p (defined in Section 4.2), this isogeny is defined over \mathbf{Q}_p .

Remark 3.4. – If we had not used the auxiliary projection $\psi: \overline{H} \rightarrow H$ and continued our construction with integrals valued in $\mathbf{G}_m \otimes \overline{H}$, the corresponding quotient $\overline{T}/\overline{L}$ would be isogenous to two copies of $J_0(M)^{p\text{-new}}$, with one copy of \mathbf{G}_m , arising from the rank one quotient \overline{H}/H . However, as the projections to this \mathbf{G}_m of the Stark–Heegner points we will define later bear little arithmetic interest (see [10, Chapter 8]), we lose little in employing the projection ψ in exchange for the technical simplicity gained. The Eisenstein quotient \overline{H}/H has eigenvalue $+1$ for complex conjugation. In [7], partial modular symbols are used to construct Eisenstein quotients where complex conjugation acts as -1 , and the resulting projections of the Stark–Heegner points to \mathbf{G}_m are related to the p -units arising in Gross’s variant of Stark’s Conjectures [19].

Remark 3.5. – The module H can be expressed up to finite index as a sum $H^+ \oplus H^-$, where the modules H^+ and H^- are the subgroups on which complex conjugation (denoted W_{∞}) acts as 1 or -1 , respectively; these each have rank g over \mathbf{Z} . This decomposition of H explains the two components of T/L described in Theorem 3.3.

Remark 3.6. – In Section 5.1, we will show how Theorem 3.3 is a generalization of the Mazur–Tate–Teitelbaum conjecture [32, Conjecture II.13.1] proven by Greenberg and Stevens [16,17].

Granting Theorem 3.3, we next describe the construction of Stark–Heegner points on $J_0(M)^{p\text{-new}}$.

3.3. Stark–Heegner points

Fix $\tau \in \mathcal{H}_p$ and $x \in \mathbf{P}^1(\mathbf{Q})$. Consider the 2-cocycle in $Z^2(\Gamma, T(\mathbf{C}_p))$ given by

$$(24) \quad d_{\tau,x}(\gamma_1, \gamma_2) := \int_{\tau}^{\gamma_1\tau} \int_{\gamma_1x}^{\gamma_1\gamma_2x} \omega_{\mu} := \int_{\tau}^{\gamma_1\tau} \int_{[\gamma_1x]-[\gamma_1\gamma_2x]} \omega_{\mu},$$

where here as always Γ acts trivially on T . It is an easy verification that the image d of $d_{\tau,x}$ in $H^2(\Gamma, T(\mathbf{C}_p))$ is independent of the choice of τ and x . Since $T(\mathbf{C}_p)$ is divisible and $H_1(\Gamma, \mathbf{Z})$ is finite (see Proposition 3.7 below), the universal coefficient theorem identifies d with a homomorphism

$$H_2(\Gamma, \mathbf{Z}) \rightarrow T(\mathbf{C}_p);$$

this homomorphism is precisely Φ_2 . Thus L , which was defined to be the image of Φ_2 , is the minimal subgroup of $T(\mathbf{C}_p)$ such that the image of d in $H^2(\Gamma, T(\mathbf{C}_p)/L)$ is trivial.

Thus there exists a map $\beta_{\tau,x} : \Gamma \rightarrow T/L$ such that

$$(25) \quad \beta_{\tau,x}(\gamma_1\gamma_2) - \beta_{\tau,x}(\gamma_1) - \beta_{\tau,x}(\gamma_2) = \int_{\tau}^{\gamma_1\tau} \int_{\gamma_1x}^{\gamma_1\gamma_2x} \omega_{\mu} \pmod{L}.$$

The 1-cochain $\beta_{\tau,x}$ is defined uniquely up to an element of $\text{Hom}(\Gamma, T/L)$. The following proposition allows us to deal with this ambiguity.

PROPOSITION 3.7. – *The abelianization of Γ is finite, and every prime dividing its size divides $6\varphi(N)(p^2 - 1)$.*

Proof. – This is a result of Ihara [24]; we provide a quick sketch. In (33) we described an exact sequence that identifies $H_1(\Gamma, \mathbf{Z})$ with the cokernel of the natural map

$$H_1(\Gamma_0(M), \mathbf{Z}) \rightarrow H_1(\Gamma_0(N), \mathbf{Z})^2.$$

Since $\Gamma_0(N)$ acts on the complex upper half plane \mathcal{H} with isotropy groups supported at the primes 2 and 3, the group $H_1(\Gamma_0(N), \mathbf{Z})$ may be identified with the corresponding singular homology of $Y_0(N)(\mathbf{C}) = \Gamma_0(N) \backslash \mathcal{H}$ outside of a finite torsion group supported at 2 and 3. Hence we must show that

$$(26) \quad f_*^Y : H_1(Y_0(M), \mathbf{Z}) \rightarrow H_1(Y_0(N), \mathbf{Z})^2$$

has finite cokernel.

Poincaré duality identifies $H_1(Y_0(N), \mathbf{Z})$ with the \mathbf{Z} -dual of the relative homology group $H_1(X_0(N), \text{cusps}, \mathbf{Z})$. We are thus led to reconsider the diagram (19) of Proposition 3.2. The injectivity of f^* implies that the cokernel of (26) is finite; furthermore, this cokernel is

isomorphic to a subgroup of the cokernel of $\overline{f^*}$. A result of Ribet [36] implies that the torsion subgroup of the cokernel of f^* is supported on the set of primes dividing $\varphi(N)$. We saw in the proof of Proposition 3.2 that the torsion subgroup of the cokernel of $C(N)^2 \rightarrow C(M)$ has exponent $p^2 - 1$. The snake lemma completes the proof. \square

We may now define Stark–Heegner points on $J_0(M)^{p\text{-new}}$. Define the ring

$$(27) \quad R := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}[1/p]) \text{ such that } N \text{ divides } c \right\}.$$

Let K be a real quadratic field such that p is inert in K ; choose an embedding σ of K into \mathbf{R} , and also an embedding of K into \mathbf{C}_p . For each $\tau \in \mathcal{H}_p \cap K$, consider the collection \mathcal{O}_τ of matrices $g \in R$ satisfying

$$(28) \quad g \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \lambda_g \begin{pmatrix} \tau \\ 1 \end{pmatrix} \quad \text{for some } \lambda_g \in K.$$

The ring \mathcal{O}_τ is isomorphic to a $\mathbf{Z}[1/p]$ -order in K , via the map $g \mapsto \lambda_g = c\tau + d$. The group of units in \mathcal{O}_τ^\times of norm 1 is a free Abelian group of rank 1. Let γ_τ be the generator such that $\sigma(\lambda_{\gamma_\tau}) > 1$ if $\sigma(\tau) > \sigma(\tau')$, and such that $\sigma(\lambda_{\gamma_\tau}) < 1$ if $\sigma(\tau) < \sigma(\tau')$. Here τ' denotes the conjugate of τ over \mathbf{Q} ; the definition of γ_τ is independent of choice of σ . Finally, choose an $x \in \mathbf{P}^1(\mathbf{Q})$, and let t denote the exponent of the abelianization of Γ .

DEFINITION 3.2. – The *Stark–Heegner point associated to τ* is given by

$$\Phi(\tau) := t \cdot \beta_{\tau,x}(\gamma_\tau) \in T(K_p)/L.$$

Multiplication by t ensures that this definition is independent of choice of $\beta_{\tau,x}$ satisfying (25), and one also checks that $\Phi(\tau)$ is independent of x . Furthermore, the point $\Phi(\tau)$ depends only on the Γ -orbit of τ , so we obtain a map

$$\Phi : \Gamma \backslash (\mathcal{H}_p \cap K) \rightarrow T(K_p)/L.$$

Let us now denote by ν_\pm the two maps $T/L \rightarrow J_0(M)^{p\text{-new}}$ of Theorem 3.3, where the \pm sign denotes the corresponding eigenvalue of complex conjugation on H . Composing Φ with the maps ν_\pm , we obtain

$$\Phi_\pm : \Gamma \backslash (\mathcal{H}_p \cap K) \rightarrow J_0(M)^{p\text{-new}}(K_p).$$

The images of Φ_\pm are the Stark–Heegner points on $J_0(M)^{p\text{-new}}$.

As in [6,7], we conjecture that the images of Φ_\pm satisfy explicit algebraicity properties. Fix a $\mathbf{Z}[1/p]$ -order \mathcal{O} in K ; let us assume that the discriminant of \mathcal{O} is prime to M . Let K_+^\times denote the multiplicative group of elements of K of positive norm. Define the *narrow Picard group* $\text{Pic}^+(\mathcal{O})$ to be the group of projective rank one \mathcal{O} -submodules of K modulo homothety by K_+^\times . Class field theory canonically identifies $\text{Pic}^+(\mathcal{O})$ with the Galois group of an extension H^+ of K called the *narrow ring class field* of K attached to \mathcal{O} :

$$\text{rec} : \text{Pic}^+(\mathcal{O}) \rightarrow \text{Gal}(H^+/K).$$

Denote by $\mathcal{H}_p^\mathcal{O}$ the set of $\tau \in \mathcal{H}_p \cap K$ such that $\mathcal{O}_\tau \cong \mathcal{O}$. The basic conjecture regarding Stark–Heegner points is:

CONJECTURE 3.8. – *If $\tau \in \mathcal{H}_p^\mathcal{O}$, then $\Phi_\pm(\tau) \in J_0(M)^{p\text{-new}}(H^+)$.*

We now proceed to refine this statement into a “Shimura reciprocity law” for Stark–Heegner points. A $\mathbf{Z}[1/p]$ -lattice in K is a $\mathbf{Z}[1/p]$ -submodule of K that is free of rank 2. Define

$$\Omega_N(K) = \left\{ (\Lambda_1, \Lambda_2), \quad \text{with} \quad \begin{array}{l} \Lambda_j \text{ a } \mathbf{Z}[1/p]\text{-lattice in } K, \\ \Lambda_1/\Lambda_2 \simeq \mathbf{Z}/N\mathbf{Z}. \end{array} \right\} / K_+^\times.$$

There is a natural bijection $\underline{\tau}$ from $\Omega_N(K)$ to $\Gamma \backslash (\mathcal{H}_p \cap K)$, which to $x = (\Lambda_1, \Lambda_2)$ assigns

$$\underline{\tau}(x) = \omega_1/\omega_2,$$

where $\langle \omega_1, \omega_2 \rangle$ is a $\mathbf{Z}[1/p]$ -basis of Λ_1 satisfying

$$\omega_1\omega'_2 - \omega'_1\omega_2 > 0, \quad \text{ord}_p(\omega_1\omega'_2 - \omega'_1\omega_2) \equiv 0 \pmod{2},$$

and $\Lambda_2 = \langle N\omega_1, \omega_2 \rangle$. Here we have written $\omega \mapsto \omega'$ for the action of the nontrivial automorphism of $\text{Gal}(K/\mathbf{Q})$. Denote by $\Omega_N(\mathcal{O})$ the set of pairs $(\Lambda_1, \Lambda_2) \in \Omega_N(K)$ such that \mathcal{O} is the largest $\mathbf{Z}[1/p]$ -order of K preserving both Λ_1 and Λ_2 . Note that $\underline{\tau}(\Omega_N(\mathcal{O})) = \Gamma \backslash \mathcal{H}_p^\mathcal{O}$. The group $\text{Pic}^+(\mathcal{O})$ acts naturally on $\Omega_N(\mathcal{O})$ by translation:

$$\mathfrak{a} : (\Lambda_1, \Lambda_2) \mapsto (\mathfrak{a}\Lambda_1, \mathfrak{a}\Lambda_2),$$

and hence it also acts on $\underline{\tau}(\Omega_N(\mathcal{O})) = \Gamma \backslash \mathcal{H}_p^\mathcal{O}$. Denote this latter action by

$$(\mathfrak{a}, \tau) \mapsto \mathfrak{a} \star \tau, \quad \text{for } \mathfrak{a} \in \text{Pic}^+(\mathcal{O}), \tau \in \Gamma \backslash \mathcal{H}_p^\mathcal{O}.$$

Our conjectural reciprocity law then states:

CONJECTURE 3.9. – *If $\tau \in \mathcal{H}_p^\mathcal{O}$, then $\Phi_\pm(\tau) \in J_0(M)^{p\text{-new}}(H^+)$, and*

$$\Phi_\pm(\mathfrak{a} \star \tau) = \text{rec}(\mathfrak{a})^{-1} \Phi_\pm(\tau)$$

for all $\mathfrak{a} \in \text{Pic}^+(\mathcal{O})$.

Remark 3.10. – Since H^+ is a ring class field, the complex conjugation associated to either real place of K is the same in $\text{Gal}(H^+/K)$. Let \mathfrak{a}_∞ denote an element of $\text{Pic}^+(\mathcal{O})$ corresponding to this complex conjugation. Then for either choice of sign $\epsilon = \pm$, we have

$$\Phi_\epsilon(\mathfrak{a}_\infty \star \tau) = \epsilon \Phi_\epsilon(\tau).$$

The proof of this fact is identical to Proposition 5.13 of [6], since the map ν_ϵ factors through a torus on which the Hecke operator W_∞ (see Definition 4.3) acts as ϵ .

The general conjecture that Stark–Heegner points are defined over global fields, and certainly the full Conjecture 3.9, are very much open. However, theoretical evidence is provided in [2,7]. Computational evidence is provided in [8,9,11]. Theorem 3.3 is proven over the course of the next two sections. We start with some combinatorial observations that lead to a complete understanding of the p -adic valuation of the integration map.

4. Combinatorial observations

We now review the exact sequence in homology which arises when a group acts without inversion on a tree (see [38, Chapter II, §2.8]), and apply these observations in our context. Define homomorphisms

$$(29) \quad \begin{aligned} \partial: C_E &\rightarrow C_V, & \partial([y]) &= [t(y)] - [s(y)], \\ \epsilon: C_V &\rightarrow \mathbf{Z}, & \epsilon([x]) &= 1. \end{aligned}$$

Since \mathcal{T} is a tree, the sequence

$$(30) \quad 0 \rightarrow C_E \xrightarrow{\partial} C_V \xrightarrow{\epsilon} \mathbf{Z} \rightarrow 0,$$

is exact. Let A be any Γ -module. Since \mathbf{Z} is free, we may tensor (30) with A without losing exactness, and then taking homology gives the long exact sequence

$$(31) \quad \cdots \rightarrow H_i(\Gamma, C_E \otimes A) \rightarrow H_i(\Gamma, C_V \otimes A) \rightarrow H_i(\Gamma, A) \rightarrow H_{i-1}(\Gamma, C_E \otimes A) \rightarrow \cdots.$$

As we saw from the description of the action of Γ on \mathcal{T} described in the proof of Proposition 3.1 (namely, that Γ acts on V with 2 orbits and transitively on E , with stabilizers isomorphic to $\Gamma_0(N)$ and $\Gamma_0(M)$ respectively), Shapiro’s Lemma gives natural identifications:

$$(32) \quad \begin{aligned} H_i(\Gamma, C_E \otimes A) &= H_i(\Gamma_0(M), A), \\ H_i(\Gamma, C_V \otimes A) &= H_i(\Gamma_0(N), A)^2. \end{aligned}$$

The long exact sequence (31) in conjunction with (32) yields the exact sequence:

$$(33) \quad \cdots \rightarrow H_i(\Gamma_0(M), A) \rightarrow H_i(\Gamma_0(N), A)^2 \rightarrow H_i(\Gamma, A) \rightarrow H_{i-1}(\Gamma_0(M), A) \rightarrow \cdots.$$

4.1. The p -adic valuation of the integration map

Let the valuation ord_p of \mathbf{Q}_p be normalized so that the valuation of p is 1. In this section we will analyze the composite map

$$\text{ord}_p \Phi_1 : H_1(\Gamma, \mathcal{M}) \xrightarrow{\Phi_1} \mathbf{Q}_p^\times \otimes H \xrightarrow{\text{ord}_p \otimes \text{Id}} \mathbf{Z} \otimes H = H.$$

By definition (see (15)), \overline{H} is a quotient of $H_0(\Gamma_0(M), \mathcal{M})$, so we have natural maps

$$(34) \quad H_1(\Gamma, \mathcal{M}) \xrightarrow{\phi} H_0(\Gamma_0(M), \mathcal{M}) \rightarrow \overline{H},$$

where ϕ is the last arrow of (33) with $i = 1$ and $A = \mathcal{M}$. Denote by ι the composition of the map $H_1(\Gamma, \mathcal{M}) \rightarrow \overline{H}$ in (34) with $\psi: \overline{H} \rightarrow H$.

PROPOSITION 4.1. – *The map $\text{ord}_p \Phi_1$ is equal to ι .*

We first prove a lemma.

LEMMA 4.2. – *Let $\tau_1, \tau_2 \in \mathcal{H}_p$ reduce to vertices connected by an oriented edge e of \mathcal{T} :*

$$\partial(e) = [\text{red}(\tau_2)] - [\text{red}(\tau_1)].$$

Extend the valuation ord_p to the maximal unramified extension of \mathbf{Q}_p . Then we have

$$\text{ord}_p \left(\int_{\tau_1 m}^{\tau_2} \int \omega_{\bar{\mu}} \right) = \bar{\mu}_m(U_e).$$

Proof. – The group $\mathbf{PGL}_2(\mathbf{Q}_p)$ acts transitively on the edges of its Bruhat–Tits tree, and the reduction map is $\mathbf{PGL}_2(\mathbf{Q}_p)$ -equivariant. Thus it suffices to consider the case where τ_1 reduces to the standard vertex corresponding to $\mathbf{Z}_p \oplus \mathbf{Z}_p$ and τ_2 reduces to the vertex corresponding to $\mathbf{Z}_p \oplus p\mathbf{Z}_p$. In this case, we have $U_e = \mathbf{P}^1(\mathbf{Q}_p) - \mathbf{Z}_p$. Let $\tau_1 \in \mathbf{P}^1(F)$ for an unramified extension F of \mathbf{Q}_p . The fact that τ_1 reduces to v_* implies that the image of τ_1 in $\mathbf{P}^1(k_F)$ does not equal the image of any point $t \in \mathbf{P}^1(\mathbf{Q}_p)$ in $\mathbf{P}^1(k_F)$, where k_F is the residue field of F . In particular, $\tau_1 \in \mathcal{O}_F$. Thus for $t \in \mathbf{P}^1(\mathbf{Q}_p)$, we have

$$\text{ord}_p(\tau_1 - t) = \begin{cases} 0 & \text{if } t \in \mathbf{Z}_p, \\ \text{ord}_p(t) & \text{otherwise.} \end{cases}$$

Similarly,

$$\text{ord}_p(\tau_2 - t) = \begin{cases} -1 & \text{if } t \in \mathbf{Z}_p, \\ \text{ord}_p(t) & \text{otherwise.} \end{cases}$$

Without loss of generality, in the definition of the multiplicative integral, we need consider only open coverings \mathcal{U} that refine the open covering $\{U_{\bar{e}}, U_e\}$. For each U in such a covering, the previous calculation shows that $\text{ord}_p((t_U - \tau_2)/(t_U - \tau_1))$ equals -1 or 0 according to whether $U \subset U_{\bar{e}}$ or not. Thus the valuation of each product inside the limit defining the multiplicative integral equals $-\bar{\mu}_m(U_{\bar{e}}) = \bar{\mu}_m(U_e)$. \square

Lemma 4.2 explains the p -adic valuation of the double integral in terms of the combinatorics of \mathcal{T} , and allows us to prove Proposition 4.1.

Proof. – We give a quick sketch; see [10] for a more detailed exposition. Let m be a 1-cycle representing a class in $H_1(\Gamma, \mathcal{M})$; this is a formal linear combination $\sum_{\gamma \in \Gamma} m_\gamma[\gamma]$ such that all but finitely many of the $m_\gamma \in \mathcal{M}$ are zero, and $\sum_{\gamma} (\gamma m_\gamma - m_\gamma) = 0$. Choose any $\tau \in \mathcal{H}_p$; then

$$\Phi_1(m) = \prod_{\gamma} \int_{\tau}^{\gamma^{-1}\tau} \int_{m_\gamma} \omega_{\mu} \in T(\mathbf{Q}_p).$$

Choose τ such that it reduces to the standard vertex v^* . For each γ let c_γ be the unique element of C_E such that $\partial(c_\gamma) = [\gamma^{-1}v^*] - [v^*]$. Then Lemma 4.2 implies that $\text{ord}_p \Phi_1(m)$ equals ψ applied to the image of $\sum_{\gamma} c_\gamma \otimes m_\gamma$ in \bar{H} , with \bar{H} viewed as in (17). Understanding the sequence (31) at $i = 1$ shows that this is exactly $\iota(m)$. \square

4.2. Hecke actions

Let $\Delta_{\mathbf{Q}} = \mathbf{PGL}_2(\mathbf{Q})$, and let Δ denote one of the groups Γ , $\Gamma_0(N)$, or $\Gamma_0(M)$, considered as a subgroup of $\Delta_{\mathbf{Q}}$. For $\alpha \in \Delta_{\mathbf{Q}}$, let

$$(35) \quad \Delta \alpha \Delta = \bigsqcup_i \alpha_i \Delta, \quad \alpha_i \in \Delta_{\mathbf{Q}}$$

be a decomposition of the indicated double coset into left cosets.

DEFINITION 4.1. – Let A be a $\Delta_{\mathbf{Q}}$ -module, and let $\alpha \in \Delta_{\mathbf{Q}}$. Define the *Hecke operator* $T(\alpha)$ on the group of Δ -co-invariants of A as follows. Let $m \in A$ represent the element $\tilde{m} \in H_0(\Delta, A)$, and let

$$T(\alpha)\tilde{m} := \sum_i \widetilde{\alpha_i^{-1}m} \in H_0(\Delta, A).$$

This definition is clearly independent of the choice of α_i . Also, for each $\gamma \in \Delta$ and each α_i , there exist unique j and $\gamma_i \in \Delta$ such that

$$(36) \quad \gamma^{-1}\alpha_i = \alpha_j\gamma_i^{-1}.$$

For γ fixed, the correspondence $i \mapsto j$ is a permutation. This implies that the definition of $T(\alpha)$ is independent of choice of representative m for \tilde{m} .

DEFINITION 4.2. – Define the *Hecke operator* $T(\alpha)$ on $H_1(\Delta, A)$ as follows. Let $m = \sum m_\gamma[\gamma]$ be a 1-cycle representing a class $\tilde{m} \in H_1(\Delta, A)$.

$$T(\alpha)\tilde{m} := \sum_{\gamma,i} \alpha_i^{-1}(m_\gamma)[\gamma_i],$$

where the α_i and γ_i are as in (36).

Once again one may check that this definition is independent of all choices.

Remark 4.3. – It is more natural to define Hecke operators on all the homology groups $H_i(\Delta, A)$ for $i > 0$ by “dimension shifting” with Definition 4.1 as the base case. Proceeding in this fashion gives a definition which is consistent with Definition 4.2; see [10] for details.

When $\Delta = \Gamma_0(M)$ or Γ and ℓ is prime, we write T_ℓ or U_ℓ for $T(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix})$, according to whether ℓ divides M or not. For these two groups, the situation for Hecke operators at p is subtle. Let \mathcal{N} denote the normalizer of $\Gamma_0(Np)$ in

$$(37) \quad \tilde{\Gamma} := R^\times/U = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PGL}_2(\mathbf{Z}[1/p]) \text{ such that } N \text{ divides } c \right\},$$

where $U = \mathbf{Z}[1/p]^\times$ is embedded in R^\times via scalar matrices. The determinant on $\tilde{\Gamma}$ maps to U/U^2 , which is a Klein 4-group. When restricted to \mathcal{N} , the determinant map induces an isomorphism

$$\mathcal{N}/\Gamma_0(Np) \cong U/U^2 \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

Let α_p denote any matrix in \mathcal{N} which maps to the image of p under the determinant map, and let α_∞ be any matrix which maps to the image of -1 . To be explicit, we may take

$$(38) \quad \alpha_p = \begin{pmatrix} p & y \\ Np & px \end{pmatrix} \quad \text{and} \quad \alpha_\infty = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

where $px - Ny = 1$.

DEFINITION 4.3. – Let A be a $\Delta_{\mathbf{Q}}$ -module. The *Atkin–Lehner involution at p* acting on the homology groups of $\Gamma_0(M)$ is given by $W_p := T(\alpha_p)$. The *Atkin–Lehner involution at infinity* is defined by $W_\infty := T(\alpha_\infty)$.

Remark 4.4. – If $H_0(\Gamma_0(M), \mathcal{M})_T$ is identified with $H_1(X_0(M), \text{cusps}, \mathbf{C})$, then the action of W_∞ coincides with that induced by complex conjugation on the manifold $X_0(M)(\mathbf{C})$.

LEMMA 4.5. – *The operators $T_\ell, U_\ell, U_p, W_p,$ and W_∞ preserve the kernel of $\overline{f^*}$ and the image of $\overline{f^*}$. In the induced actions on $\ker \overline{f^*}$ and $\text{coker } \overline{f^*}$, we have $U_p + W_p = 0$.*

In particular, Lemma 4.5 provides a Hecke action on \overline{H} . The subgroup $H \subset \overline{H}$ is Hecke-stable. For the group Γ , the double coset of P is the right coset of any one matrix of R^\times of determinant p . Thus the operator $U_p = W_p$ is an involution on the homology groups of Γ . Also, $U_p = -W_p$ is an involution on H . We write W for the involutions U_p on H and the homology groups of Γ .

We relegate the proof of the following proposition to Appendix A:

PROPOSITION 4.6. – *Endow T with a Hecke action via the action on H . The integration map (21)*

$$\int \omega_\mu : ((\text{Div}_0 \mathcal{H}_p) \otimes M)_\Gamma \rightarrow T$$

is equivariant for all the Hecke operators: T_ℓ for $\ell \nmid M$, U_ℓ for $\ell | N$, W , and W_∞ .

4.3. The lattice L

From (33) we have

$$(39) \quad H_1(\Gamma_0(N), \mathcal{M})^2 \rightarrow H_1(\Gamma, \mathcal{M}) \xrightarrow{\phi} H_0(\Gamma_0(M), \mathcal{M}) \xrightarrow{\overline{f^*}} H_0(\Gamma_0(N), \mathcal{M})^2.$$

The sequence (39) combined with Proposition 4.1 implies that the image of $H_1(\Gamma_0(N), \mathcal{M})^2$ in $H_1(\Gamma, \mathcal{M})$ under the integration map Φ_1 has trivial p -adic valuation. Thus, for the image of the integration map to be discrete in T , it must be the case that the image of $H_1(\Gamma_0(N), \mathcal{M})^2$ in T is finite. We will prove this by exploiting Hecke actions. We exclude the proof of the following Lemma (see [10, Section 5.3]).

LEMMA 4.7. – *The groups $H_1(\Gamma_0(N), \mathcal{M})$ and $H_1(\Gamma_0(M), \mathcal{M})$ are isomorphic to \mathbf{Z} , and are Eisenstein as Hecke modules: T_ℓ acts as $\ell + 1$ for $\ell \nmid M$ (and for $\ell = p$ on $H_1(\Gamma_0(N), \mathcal{M})$), W_∞ acts as -1 , and W acts as 1 on $H_1(\Gamma_0(M), \mathcal{M})$.*

Define a modified Eisenstein ideal \mathcal{I} of the (abstract) Hecke algebra by letting \mathcal{I} be generated by $T_\ell - (\ell + 1)$ for $\ell \nmid M$, $(p + 1)W - (p + 1)$, and $W_\infty + 1$.

LEMMA 4.8. – *The ideal \mathcal{I} annihilates the image of $H_1(\Gamma_0(N), \mathcal{M})^2$ under the integration map Φ_1 .*

Proof. – The map $H_1(\Gamma_0(N), \mathcal{M})^2 \rightarrow H_1(\Gamma, \mathcal{M})$ is Hecke-equivariant for $T_\ell, \ell \nmid M$, and W_∞ by basic computation; the boundary map $H_1(\Gamma, \mathcal{M}) \rightarrow ((\text{Div}_0 \mathcal{H}_p) \otimes M)_\Gamma$ is Hecke-equivariant by a formal computation (see [10, Lemma 5.1.3]). Thus Proposition 4.6 implies that Φ_1 is Hecke-equivariant. Also, the action of T_p on $H_1(\Gamma_0(N), \mathcal{M})$ is given by $p + 1$ matrices α_i of determinant p , hence the action of T_p on $H_1(\Gamma_0(N), \mathcal{M})$ becomes that of $(p + 1)W$ on its image in $H_1(\Gamma, \mathcal{M})$. The result now follows from Proposition 4.7. \square

Let $H^* = \text{Hom}(H, \mathbf{Z})$ denote the dual of H , so $T(\mathbf{Q}_p) = \text{Hom}(H^*, \mathbf{Q}_p^\times)$. It is a standard fact that $H^*/\mathcal{I}H^*$ is finite: after tensoring with \mathbf{C} , one obtains the space of holomorphic Eisenstein

series that are cusp forms (of which there are none).³ Thus Lemma 4.8 implies that the image of $H_1(\Gamma_0(N), \mathcal{M})^2$ under the integration map Φ_1 is finite.

PROPOSITION 4.9. – *The group of periods $L \subset T(\mathbf{Q}_p)$ is a Hecke-stable lattice of rank $2g$.*

Proof. – As already mentioned, a formal calculation (see [10, Lemma 5.1.3]) implies the Hecke-equivariance of the boundary maps

$$H_2(\Gamma, \mathbf{Z}) \rightarrow H_1(\Gamma, \mathcal{M}) \quad \text{and} \quad H_1(\Gamma, \mathcal{M}) \rightarrow H_0(\Gamma, (\text{Div}_0 \mathcal{H}_p) \otimes \mathcal{M}).$$

Hence Proposition 4.6 implies that Φ_2 is Hecke-equivariant, and thus that L is Hecke-stable.

From (39), the kernel of the map

$$H_1(\Gamma, \mathcal{M}) \rightarrow \overline{H'} := \ker \overline{f_*}$$

is the image of $H_1(\Gamma_0(N), \mathcal{M})^2$, which has finite image under the integration map. Thus it remains to show that the image of $H_2(\Gamma, \mathbf{Z})$ in $\overline{H'}$ has rank $2g$ and injects into $H \subset \overline{H}$. The group $H_2(\Gamma, \mathbf{Z})$ may be understood using the sequence (33) again:

$$(40) \quad H_2(\Gamma_0(N), \mathbf{Z})^2 \rightarrow H_2(\Gamma, \mathbf{Z}) \rightarrow H_1(\Gamma_0(M), \mathbf{Z}) \rightarrow H_1(\Gamma_0(N), \mathbf{Z})^2.$$

As in the proof of Proposition 3.7, the homology of $\Gamma_0(N)$ may be identified with that of $Y_0(N)$ outside of 2 and 3-torsion. Since $Y_0(N)$ is a noncompact Riemann surface, the group $H_2(Y_0(N), \mathbf{Z})$ vanishes. And the right-hand arrow of (40) may be identified with

$$f_*^Y : H_1(Y_0(M), \mathbf{Z}) \rightarrow H_1(Y_0(N), \mathbf{Z})^2.$$

Thus the image of $H_2(\Gamma, \mathbf{Z})$ in $\overline{H'} = \ker \overline{f_*}$ is precisely $H' := \ker f_*$. We need to show that H' injects into $H = \text{coker } f^*$ and has finite cokernel. Yet the endomorphism $f_* \circ f^*$ of $H_1(X_0(N), \mathbf{Z})^2$ can be given explicitly by the matrix

$$f_* \circ f^* = \begin{pmatrix} p+1 & T_p \\ T_p & p+1 \end{pmatrix}.$$

Since the eigenvalues of T_p are bounded by $2\sqrt{p}$, this endomorphism is injective and has finite cokernel; the result follows. \square

Remark 4.10. – The finite group H/H' reflects congruences between modular forms of level N and M . In [3], the images of Stark–Heegner points in this finite Hecke-module under the p -adic valuation map is related to special values of certain Rankin L -series.

5. Proof of Theorem 3.3

Let \mathcal{T} denote the Hecke algebra of H (that is, the subring of the ring of endomorphisms of the group H generated over \mathbf{Z} by T_ℓ for $\ell \nmid M$, U_ℓ for $\ell \mid N$, and W). In Proposition 4.1 we gave

³ In the case where $N = 1$, Mazur [30] has conducted a detailed analysis of the group $H^*/\mathcal{I}H^*$. When \mathcal{I} includes the element $W - 1$ rather than just $(p + 1)(W - 1)$ as in our setting, Mazur finds that $H^*/\mathcal{I}H^*$ is cyclic of size n , where n is the numerator of the fraction $(p - 1)/12$.

a combinatorial description of the map $\text{ord}_p : L \rightarrow H \otimes \mathbf{Z}_p$ given by

$$L \subset T(\mathbf{Q}_p) \xrightarrow{\text{ord}_p} H \otimes \mathbf{Z} \rightarrow H \otimes \mathbf{Z}_p.$$

Consider now the logarithm $\log_p : L \rightarrow H \otimes \mathbf{Z}_p$ given by

$$L \subset T(\mathbf{Q}_p) \xrightarrow{\log_p} H \otimes \mathbf{Z}_p,$$

where now and throughout this article we choose the branch of the logarithm for which $\log_p(p) = 0$.

PROPOSITION 5.1. – *There exists an element $\mathcal{L}_p \in \mathcal{T} \otimes \mathbf{Z}_p$ such that*

$$(41) \quad \mathcal{L}_p \text{ord}_p \lambda = \log_p \lambda \quad \text{for all } \lambda \in L.$$

Proposition 5.1 will be proved in Section 5.3.

DEFINITION 5.1. – The element \mathcal{L}_p is called the \mathcal{L} -invariant of T/L .

Remark 5.2. – Let $H_{\pm} = H/(W_{\infty} \mp 1)$ be the maximal quotients of H on which complex conjugation acts as a scalar ± 1 . The fact that there is an element \mathcal{L}_p in $\mathcal{T} \otimes \mathbf{Q}_p$ satisfying (41) for each of the factors $H_- \otimes \mathbf{Q}_p$ and $H_+ \otimes \mathbf{Q}_p$ follows from the fact that each of these modules is free of rank one over $\mathcal{T} \otimes \mathbf{Q}_p$ and that $\text{ord}_p : L \otimes \mathbf{Q}_p \rightarrow H_{\pm} \otimes \mathbf{Q}_p$ is surjective. The fact that the same \mathcal{L}_p works on each factor, and that this element is integral, follows from our specific construction and proof in Section 5.3.

Our goal is to connect T/L with the Abelian variety $J = J_0(M)^{p\text{-new}}$. This Abelian variety has purely toric reduction at p , and its p -adic uniformization can be described as follows. Let S denote the set of supersingular points in characteristic p on $X_0(N)$, and let $X := \text{Div}_0 S$ denote the group of degree-zero divisors on S . The group X has a natural Hecke action: by T_{ℓ} for $\ell \nmid M$ (U_{ℓ} for $\ell|N$, and U_p) by sending a supersingular point on $X_0(N)$ to the formal sum of the $\ell + 1$ (respectively $2\ell + 1$ and 1) ℓ -isogenous supersingular points, counted with multiplicity; the operator $W = U_p$ has order two and is also given by the action of $\text{Gal}(\mathbf{F}_{p^2}/\mathbf{F}_p)$ on the supersingular points. It is well known that the Hecke algebra of X equals that of H ; in other words, there is a ring homomorphism $\mathcal{T} \rightarrow \text{End}(X)$ sending $T_{\ell} \mapsto T_{\ell}$, etc.⁴ Thus we may consider X as a module for \mathcal{T} . Let $G_p = \text{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ act on X (via the $\text{Gal}(\mathbf{F}_{p^2}/\mathbf{F}_p)$ -action on S) and on $\text{Hom}(X, \overline{\mathbf{Q}}_p^{\times})$ by $\sigma(h)(x) = \sigma(h(\sigma^{-1}(x)))$. There is a rigid analytic $\mathcal{T}[G_p]$ -equivariant isomorphism

$$J(\overline{\mathbf{Q}}_p) \cong \text{Hom}(X, \overline{\mathbf{Q}}_p^{\times})/X,$$

where the inclusion

$$Q : X \rightarrow \text{Hom}(X, \mathbf{Q}_p^{\times}) = X^* \otimes \mathbf{Q}_p^{\times}$$

is given by a symmetric pairing

$$(42) \quad X \times X \rightarrow \mathbf{Q}_p^{\times}.$$

(Here we have written $X^* = \text{Hom}(X, \mathbf{Z})$.) The Hecke operators are self-adjoint for this pairing.

⁴ This is because after tensoring with \mathbf{C} , the spectrum of T_{ℓ} on X consists of the ℓ th Fourier coefficients of a basis of p -new forms of level M ; the spectrum of T_{ℓ} on H consists of each of these eigenvalues repeated twice.

Remark 5.3. – Although this description of $J(\overline{\mathbf{Q}}_p)$ seems to be well known to the experts, we could not find this description in the literature except for the case when $N = 1$ and $X_0(p)$ is a Mumford curve [13,14]. For the general case, [12, Chap VI, Theorem 6.9] describes a regular proper model for $X_0(Np)$ over \mathbf{Z}_p whose special fiber consists of two copies of $X_0(N)$ intersecting transversely at the supersingular points. From [5, Example 8] (see also [5, Corollary 9.7.2] and the comments following), this implies that the character group of the toric part of the reduction of the Néron model of $J_0(Np)$ is canonically identified with X . Sections 1 and 2 of [4] (in particular Theorems 1.2 and 2.1) combined with the self-duality of J yield our given description; the functoriality of these constructions under correspondences yields the Hecke-equivariance.

Composing (42) with the p -adic valuation gives a \mathbf{Z} -valued pairing (the “monodromy pairing”) on X which is nondegenerate,⁵ and hence yields an injection

$$\text{ord}_p Q : X \rightarrow X^*.$$

Similarly, composing Q with \log_p yields

$$\log_p Q : X \rightarrow X^* \otimes \mathbf{Z}_p.$$

PROPOSITION 5.4. – *Let \mathcal{L}_p be as in Proposition 5.1. We have*

$$\mathcal{L}_p \text{ord}_p Q(x) = \log_p Q(x) \quad \text{for all } x \in X.$$

Proposition 5.4 will be proved in Section 5.4. Propositions 5.1 and 5.4 imply Theorem 3.3 as follows. For a set of primes \mathcal{P} , we say that two analytic spaces are \mathcal{P} -isogenous if there is an isogeny between them whose degree is supported on the elements of \mathcal{P} . Let $\pi_{\pm} : H \rightarrow H_{\pm}$ denote the natural projections. Since Φ_2 is equivariant for W_{∞} , and $H \rightarrow H_- \oplus H_+$ has cokernel supported at 2, it follows that T/L is $\{2\}$ -isogenous to

$$(T/L)_- \oplus (T/L)_+ := (\mathbf{G}_m \otimes H_-) / \pi_- L \oplus (\mathbf{G}_m \otimes H_+) / \pi_+ L.$$

We will show that each of $(T/L)_{\pm}$ is isogenous to J .

Recall the Hecke-equivariant map $\psi : \overline{H} \rightarrow H$ from Section 3.2 used to define our modular symbol valued in H , and denote by $\psi_- : \overline{H}_- \rightarrow H_-$ the induced map obtained by modding out by $W_{\infty} + 1$. Recall that $H' = \ker f_*$ and let H'_- be its corresponding quotient.

Since all of the groups below are free of rank 1 over $\mathcal{T} \otimes \mathbf{Q}$ after tensoring with \mathbf{Q} , it is possible to find Hecke-equivariant maps ξ_- and ξ'_- fitting into a commutative diagram

$$(43) \quad \begin{array}{ccc} H'_- & \longrightarrow & \overline{H}_- \xrightarrow{\psi_-} H_- \\ \xi'_- \downarrow & & \downarrow \xi_- \\ X & \xrightarrow{\text{ord}_p Q} & X^* \end{array}$$

where the horizontal arrow $H'_- \rightarrow \overline{H}_-$ is the natural inclusion. Recall that

⁵ The monodromy pairing is given simply as follows: define a pairing on $\text{Div } S$ by requiring that distinct $s, t \in S$ are orthogonal, while an element s paired with itself equals $1/2$ the number of automorphisms of s ; this pairing restricted to $X = \text{Div}_0 S$ is $\text{ord}_p Q$.

- (1) The map $\Phi_2 : H_2(\Gamma, \mathbf{Z}) \rightarrow T$ factors through $\Phi_1 : H_1(\Gamma, \mathcal{M}) \rightarrow T$.
- (2) The composite

$$H_1(\Gamma_0(N), \mathcal{M})^2 \rightarrow H_1(\Gamma, \mathcal{M}) \xrightarrow{\Phi_1} T$$

has finite image.

- (3) The image of $H_2(\Gamma, \mathbf{Z})$ in $H_1(\Gamma, \mathcal{M})/H_1(\Gamma_0(N), \mathcal{M})^2$ is canonically identified with H' (see the proof of Proposition 4.9).

The identification of (43) implies that ξ'_- induces a map $H_2(\Gamma, \mathbf{Z})_- \rightarrow X$, also denoted ξ'_- . Consider the diagram

$$(44) \quad \begin{array}{ccc} H_2(\Gamma, \mathbf{Z})_- & \xrightarrow{\pi - \Phi_2} & \mathbf{Q}_p^\times \otimes H_- \\ \xi'_- \downarrow & & \downarrow \xi_- \\ X & \xrightarrow{Q} & \mathbf{Q}_p^\times \otimes X^* \end{array}$$

Proposition 4.1 implies that the composition of the top row of (44) with ord_p is equal to the composition of $H_2(\Gamma, \mathbf{Z})_- \rightarrow H'_-$ with the top row of (43). Thus the commutativity of (43) implies the commutativity of the p -adic valuation of (44). Since all the maps in (44) are Hecke-equivariant, Propositions 5.1 and 5.4 show that the commutativity of the ord_p of (44) *automatically implies* the commutativity of the \log_p of (44). Thus the diagram (44) itself commutes, up to elements in the kernel of both \log_p and ord_p ; these elements are torsion of order dividing $p - 1$ (or 2 if $p = 2$).

Hence the map

$$\text{Id} \otimes \xi_- : \mathbf{G}_m \otimes H_- \rightarrow \mathbf{G}_m \otimes X^*$$

induces an isogeny $(T/\Lambda)_- \rightarrow J$. Furthermore, the kernel of this isogeny is identified with the cokernel of

$$\xi'_- : H'_- \rightarrow X.$$

A similar argument for H_+ then proves Theorem 3.3 and furthermore bounds the primes dividing the degree of the isogeny to lie in

$$\mathcal{P} = \{ \ell : \ell \text{ divides } 2(p - 1) \text{ or the size of either coker } \xi'_\pm : H'_\pm \rightarrow X \}.$$

5.1. Connection with the Mazur–Tate–Teitelbaum conjecture

Let E be an elliptic curve with conductor Np and split multiplicative reduction at p . In this section, we show that Theorem 3.3 implies the Mazur–Tate–Teitelbaum conjecture for E . The conjecture, stated below in Theorem 5.5, was proven by Greenberg and Stevens in [16].

Let \mathcal{I}_E^+ denote the ideal of the Hecke algebra of \overline{H} corresponding to E and the “plus” modular symbol (that is, the ideal generated by $T_\ell - a_\ell$ for $\ell \nmid Np$, $W_p - 1$, and $W_\infty - 1$, where $a_\ell = \ell + 1 - \#E(\mathbf{F}_\ell)$). The quotient $\overline{H}/\mathcal{I}_E^+$ has rank 1 over \mathbf{Z} ; the projection

$$\Psi_E^+ : \overline{H} \rightarrow H_E^+ := (\overline{H}/\mathcal{I}_E^+)_T \cong \mathbf{Z}$$

is the *plus modular symbol* attached to E . We retain the notation of [32] and write

$$\lambda_E(a, M) := \Psi_E^+ \left(\left[-\frac{a}{M} \right] - [\infty] \right).$$

THEOREM 5.5 (Greenberg and Stevens [16], conjectured by Mazur–Tate–Teitelbaum in Conjecture II.13.1 of [32]). – *Let ψ be a Dirichlet character of conductor c prime to p such that $\psi(p) = 1$. Then*

$$\lim_{n \rightarrow \infty} \sum_{a \bmod p^n c} \psi(a) \log_p(a) \lambda_E(a, p^n c) = \frac{\log_p(q_E)}{\text{ord}_p(q_E)} \sum_{a \bmod c} \psi(a) \lambda_E(a, c),$$

where $q_E \in \mathbf{Q}_p^\times$ is the Tate period of E .

After tensoring with \mathbf{G}_m , the projection Ψ_E^+ yields a map $\varphi: \overline{T} \rightarrow \mathbf{G}_m$. According to Theorem 3.3, the quotient $\mathbf{G}_m/\varphi(L)$ is an analytic space isogenous to the elliptic curve E . This implies that every element of $\varphi(L)$ is commensurable with the Tate period q_E of E . By evaluating a particular element of $\varphi(L)$, we will deduce the MTT conjecture. In what follows, we denote

$$\varphi \left(\int_{\tau_1 x}^{\tau_2 y} \int \omega_{\overline{T}} \right) \quad \text{by} \quad \int_{\tau_1 x}^{\tau_2 y} \omega_E^+ \in \mathbf{C}_p^\times.$$

Consider the class $c \in H_1(\Gamma, \mathcal{M})$ represented by the 1-cycle $([0] - [\infty])[(\frac{1/p}{0} \ 0)]$. The element c is in the image of the boundary map from $H_2(\Gamma, \mathbf{Z})$, since a simple calculation shows that the image of c in the next term of the exact sequence

$$(45) \quad H_2(\Gamma, \mathbf{Z}) \rightarrow H_1(\Gamma, \mathcal{M}) \rightarrow H_1(\Gamma, \text{Div } \mathbf{P}^1(\mathbf{Q})) = \Gamma_\infty^{\text{ab}}$$

vanishes (this is true for any class represented by $([x] - [y])[\gamma]$, for γ stabilizing x and y). Here Γ_∞ denotes the stabilizer of ∞ in Γ , and the equality of (45) follows from Shapiro’s Lemma. Thus the double integral

$$q' := \int_{\tau}^{\tau} \int_0^{\infty} \omega_E^+ \in \mathbf{Q}_p^\times$$

lies in $\varphi(L)$, and in particular does not depend on the choice of τ . In fact, since $W_p = W_\infty = 1$ on H_E^+ , it follows (see [6, Proposition 5.13]) that the multiplicative double integral is invariant under the full group $\tilde{\Gamma}$ (defined in (37)). In particular, one finds that

$$q := \int_{\tau/p}^{\tau} \int_0^{\infty} \omega_E^+ \in \mathbf{Q}_p^\times$$

is independent of τ and that $q' = q^2$. Thus q is commensurable with q_E as well, so

$$(46) \quad \frac{\log_p(q)}{\text{ord}_p(q)} = \frac{\log_p(q_E)}{\text{ord}_p(q_E)}.$$

To evaluate q , choose τ to reduce to the standard vertex v^* of the tree \mathcal{T} . Since the matrix P^{-1} sends v^* to w^* , Lemma 4.2 implies that

$$(47) \quad \text{ord}_p(q) = \Psi_E^+([0] - [\infty]) = \lambda_E(0, 1).$$

Let $n \geq 1$; for $a = 0, \dots, p^n - 1$ define $U_a := a + p^n \mathbf{Z}_p$. To evaluate $\log_p q \in \mathbf{Z}_p$ modulo p^n , it suffices to take a cover of $\mathbf{P}^1(\mathbf{Q})$ by the sets

$$(48) \quad U_\infty := \{t \in \mathbf{P}^1(\mathbf{Q}_p) : \text{ord}_p(t) < -n\},$$

$$(49) \quad \frac{1}{p^n} U_a, \frac{1}{p^{n-1}} U_a, \dots, \frac{1}{p} U_a \quad \text{for } a \not\equiv 0 \pmod{p},$$

and U_a for all $a = 0, \dots, p^n - 1$. The contributions to the integral defining $\log_p q$ from each of these terms are as follows:

$$(50) \quad U_\infty : 0,$$

$$\frac{1}{p^k} U_a : \log_p \left(\frac{a/p^k - \tau}{a/p^k - \tau/p} \right) \lambda_E(a, p^n) = \log_p \left(\frac{a - p^k \tau}{a - p^{k-1} \tau} \right) \lambda_E(a, p^n),$$

$$(51) \quad U_a : \log_p \left(\frac{a - \tau}{a - \tau/p} \right) \lambda_E(a, p^n) = \log_p \left(\frac{a - \tau}{pa - \tau} \right) \lambda_E(a, p^n).$$

Summing these values (the terms of (50) for $k = 1, \dots, n$ telescope, and the distribution relation

$$\lambda_E(a', p^{n-1}) = \sum_{\substack{a \pmod{p^n} \\ a \equiv a' \pmod{p^{n-1}}} } \lambda_E(a, p^n)$$

allows one to cancel terms in the denominator of (51) for all a with the terms in the numerator for $p|a$ one obtains

$$(52) \quad \log_p(q) \equiv \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n-1} \log_p(a) \lambda_E(a, p^n) \pmod{p^n}.$$

Eqs. (46), (47), and (52) yield Theorem 5.5 for the trivial character. The more general statement for a character of conductor $c > 1$ may be obtained by repeating our analysis above for each $(v, c) = 1$ with the 1-cycle

$$([v/c] - [\infty])[\gamma],$$

with $\gamma \in \Gamma$ stabilizing v/c and ∞ . We omit the details (see [6, §2.3]).

5.2. Hida families and the definition of \mathcal{L}_p

In this section we define the element $\mathcal{L}_p \in \mathcal{T} \otimes \mathbf{Z}_p$. Let $X_0 = X_0(Np)$, and define a tower of curves X_r above X_0 corresponding to the congruence subgroups $\Gamma_r := \Gamma_0(N) \cap \Gamma_1(p^r)$, for $r \geq 1$:

$$X_r(\mathbf{C}) = \Gamma_r \backslash \mathcal{H}^*.$$

The points of X_r classify triples (E, C, P) , where E is an elliptic curve, C a cyclic subgroup of size N , and P a point of order p^r . The natural maps $X_{r+1} \rightarrow X_r$ send $(E, C, P) \mapsto (E, C, pP)$ for $r \geq 1$, and the map $X_1 \rightarrow X_0$ sends $(E, C, P) \mapsto (E, \langle C, P \rangle)$. Composing $X_r \rightarrow X_0$ with the two maps $X_0 \rightarrow X_0(N)$ from (13), we obtain two degeneracy maps $X_r \rightarrow X_0(N)$ for each $r \geq 0$ (there are actually $r + 1$ natural degeneracy maps for each $r \geq 1$, but we will be interested in only these two). Let f_r^* denote the pullback on homology from the two copies of $X_0(N)$ to X_r , and define

$$H_r = [H_1(X_r, \mathbf{Z}_p) / f_r^*(H_1(X_0(N), \mathbf{Z}_p)^2)]_T,$$

so that $H_0 = H \otimes \mathbf{Z}_p$. Let \mathcal{T}_r denote the Hecke algebra of H_r , generated over \mathbf{Z}_p by T_ℓ for $\ell \nmid M$, U_ℓ for $\ell \mid M$, and the diamond operators $\langle d \rangle$ for $d \in (\mathbf{Z}/p^r\mathbf{Z})^\times$. Here $\mathcal{T}_0 = \mathcal{T} \otimes \mathbf{Z}_p$. Define the Hida Hecke algebra

$$\mathbf{T} := \varprojlim \mathcal{T}_r,$$

which has the structure of $\Lambda := \mathbf{Z}_p[[\mathbf{Z}_p^\times]]$ -module, where the group elements of \mathbf{Z}_p^\times act via the diamond operators. Let I denote the augmentation ideal of Λ . If \mathbf{T}° denotes the image of \mathbf{T} under Hida’s ordinary projector, Hida has shown:

THEOREM 5.6 (Hida [22, Corollary 3.2]). – *The Λ -module \mathbf{T}° is free of finite rank and*

$$\mathbf{T}^\circ / I\mathbf{T}^\circ \cong \mathcal{T}_0.$$

Remark 5.7. – The map $\mathbf{T}^\circ \rightarrow \mathcal{T}_0$ of Theorem 5.6 is the natural projection. It is clear that $I\mathbf{T}^\circ$ lies in the kernel; Hida’s “control theorem” 5.6 is that $I\mathbf{T}^\circ$ is the entire kernel.

The standard identification $\langle d \rangle - 1 \mapsto d$ yields an isomorphism

$$I/I^2 \cong \varprojlim \mathbf{Z}_p^\times / (\mathbf{Z}_p^\times)^{p^n},$$

since the group \mathbf{Z}_p^\times is Abelian. Composing with $\log_p : \mathbf{Z}_p^\times \rightarrow \mathbf{Z}_p$, we obtain a map also denoted $\log_p : I/I^2 \rightarrow \mathbf{Z}_p$.

Let t be an element of \mathbf{T} whose image in \mathcal{T}_0 vanishes. By Hida’s Theorem 5.6, t° lies in $I\mathbf{T}^\circ$ (where t° is the image of t under the ordinary projector). Consider the image of t° in

$$I\mathbf{T}^\circ / I^2\mathbf{T}^\circ = I/I^2 \otimes_\Lambda \mathbf{T}^\circ.$$

Using the map

$$\log_p \otimes \text{Id} : I/I^2 \otimes_\Lambda \mathbf{T}^\circ \rightarrow \mathbf{Z}_p \otimes_\Lambda \mathbf{T}^\circ$$

we further map our element t to

$$\mathbf{Z}_p \otimes_\Lambda \mathbf{T}^\circ = \Lambda/I \otimes_\Lambda \mathbf{T}^\circ = \mathbf{T}^\circ / I\mathbf{T}^\circ = \mathcal{T}_0.$$

The image of t under this series of maps is denoted $t' \in \mathcal{T}_0$, to reflect the intuition that it represents the derivative of t in the direction of the level (i.e., the fact that $t^\circ \in I\mathbf{T}^\circ$ means that the “value” of the “function” t is 0 at the base of the tower, so its image in $I\mathbf{T}^\circ / I^2\mathbf{T}^\circ$ is its “derivative”).

Since $U_p = -W_p$ on H , and W_p is an involution, the element $1 - U_p^2$ vanishes in \mathcal{T} .

DEFINITION 5.2. – We define the element

$$\mathcal{L}_p := (1 - U_p^2)' \in \mathcal{T}_0.$$

5.3. Proof of Proposition 5.1

Let $\tau \in \mathcal{H}_p$ lie in the quadratic unramified extension K_p of \mathbf{Q}_p , and assume further that τ reduces to the central vertex v^* of the tree \mathcal{T} . Consider the map

$$\beta_{\mathcal{L}_p} : K_p^\times \otimes H \rightarrow K_p \otimes H, \quad k \otimes h \mapsto \log_p(k) \otimes h - \mathcal{L}_p(\text{ord}_p(k) \otimes h).$$

Composing the 2-cocycle $d_{\tau,x} \in Z^2(\Gamma, T(K_p))$ from Section 3.3 with $\beta_{\mathcal{L}_p}$ yields

$$d_{\tau,x}^{\mathcal{L}_p} \in Z^2(\Gamma, K_p \otimes H), \quad d_{\tau,x}^{\mathcal{L}_p}(\gamma_1, \gamma_2) := \beta_{\mathcal{L}_p} \left(\int_{\tau}^{\gamma_1 \tau} \int_{\gamma_1 x}^{\gamma_1 \gamma_2 x} \omega_{\mu} \right).$$

As in Section 3.3, the lattice $\beta_{\mathcal{L}_p}(L)$ is the smallest subgroup of $K_p \otimes H$ such that the cocycle $d_{\tau,x}^{\mathcal{L}_p}$ splits in the quotient; thus to prove equation Proposition 5.1, it suffices to prove that $d_{\tau,x}^{\mathcal{L}_p}$ splits.

We will in fact show a stronger result. Define a 1-cocycle

$$c_{\tau} \in Z^1(\Gamma, \text{Hom}(\mathcal{M}, T(K_p)))$$

by the rule

$$c_{\tau}(\gamma)(m) := \int_{\tau}^{\gamma \tau} \int_m \omega_{\mu}.$$

Composing c_{τ} with $\beta_{\mathcal{L}_p}$, we obtain a 1-cocycle

$$c_{\tau}^{\mathcal{L}_p} \in Z^1(\Gamma, \text{Hom}(\mathcal{M}, K_p \otimes H)).$$

It is a basic calculation⁶ that the splitting of $c_{\tau}^{\mathcal{L}_p}$ implies the splitting of $d_{\tau,x}^{\mathcal{L}_p}$; the splitting of $c_{\tau}^{\mathcal{L}_p}$ is in fact what we will show.

The main idea for splitting the cocycle $c_{\tau}^{\mathcal{L}_p}$ is to lift the modular symbol μ of measures on $\mathbf{P}^1(\mathbf{Q}_p)$ to a modular symbol of measures $\tilde{\mu}$ on a \mathbf{Z}_p^{\times} -bundle \mathbf{X} over $\mathbf{P}^1(\mathbf{Q}_p)$. The space $\mathbf{X} := (\mathbf{Z}_p \times \mathbf{Z}_p)'$ is defined to be the set of pairs $(a, b) \in \mathbf{Z}_p \times \mathbf{Z}_p$ such that a and b are not both divisible by p ; this set of “primitive vectors” makes an appearance in the earlier work of Greenberg and Stevens [17]. The space \mathbf{X} admits a map

$$\begin{aligned} \pi: \mathbf{X} &\rightarrow \mathbf{P}^1(\mathbf{Q}_p), \\ (a, b) &\mapsto a/b. \end{aligned}$$

The fibers of π are principal homogeneous spaces for \mathbf{Z}_p^{\times} . If we consider the elements of \mathbf{X} as column vectors and let $\mathbf{GL}_2(\mathbf{Z}_p)$ act on the left, the map π is $\mathbf{GL}_2(\mathbf{Z}_p)$ -equivariant. In this section, we will consider the groups $\Gamma_0(N), \Gamma_r, \Gamma$, etc. as subgroups of \mathbf{GL}_2 (rather than \mathbf{PGL}_2 as in previous sections).

Remark 5.8. – If the function $f(t) = t - \tau$ were integrable on $\mathbf{P}^1(\mathbf{Q}_p)$, a formal calculation would show that

$$\rho_{\tau}(m) = \int_{\mathbf{P}^1(\mathbf{Q}_p)} \log_p(t - \tau) d\mu_m(t)$$

is an explicit splitting of the cocycle $\log_p c_{\tau}$, i.e. that $d\rho_{\tau} = \log_p c_{\tau}$. However, this is not the case since $f(t)$ has a pole at $t = \infty$. This explains the role of the space \mathbf{X} : the function $f(a, b) = a - b\tau$ is integrable on \mathbf{X} , has a zero along the fiber over τ , and no poles.

⁶ If the 0-chain ρ_{τ} splits $c_{\tau}^{\mathcal{L}_p}$, then the 1-chain $\eta_{\tau,x}$ defined by $\eta_{\tau,x}(\gamma) = \rho_{\tau}([x] - [\gamma x])$ splits $d_{\tau,x}^{\mathcal{L}_p}$.

PROPOSITION 5.9. – *There exists a $\Gamma_0(N)$ -invariant $\text{Meas}(\mathbf{X}, H \otimes \mathbf{Z}_p)$ -valued modular symbol $\tilde{\mu}$ such that*

$$(53) \quad \tilde{\mu}_m(\mathbf{Z}_p^\times \times p\mathbf{Z}_p) = \mu_m(\mathbf{P}^1(\mathbf{Q}_p) - \mathbf{Z}_p) = -\psi(m)$$

for all $m \in \mathcal{M}$.

(Recall that the map ψ was defined in Section 3.2 to create a modular symbol valued in H rather than \overline{H} .)

Remark 5.10. – Since the $\Gamma_0(N)$ -translates of $\mathbf{P}^1(\mathbf{Q}_p) - \mathbf{Z}_p$ form a disjoint open cover of $\mathbf{P}^1(\mathbf{Q}_p)$, the $\Gamma_0(N)$ -invariance of $\tilde{\mu}$ combined with (53) implies that $\tilde{\mu}$ has the same total measure as μ , namely 0:

$$\tilde{\mu}_m(\mathbf{X}) = 0 \quad \text{for all } m \in \mathcal{M}.$$

Proof. – Our methods follow those of Greenberg and Stevens [17, p. 203]. Let A denote a free \mathbf{Z}_p -module of finite rank, viewed as a trivial $\Gamma_0(N)$ -module. A $\Gamma_0(N)$ -invariant $\text{Meas}(\mathbf{X}, A)$ -valued modular symbol is an element of

$$(54) \quad \mathbf{M}(A) := H^0(\Gamma_0(N), \text{Hom}(\mathcal{M}, \text{Meas}(\mathbf{X}, A))).$$

For each $r \geq 1$, let $\Gamma_r = \Gamma_0(N) \cap \Gamma_1(p^r)$ as in Section 5.2. The $\Gamma_0(N)$ -module $\text{Meas}(\mathbf{X}, A)$ is isomorphic to an inverse limit of induced modules from the groups Γ_r as follows. Let $\mathbf{X}_r := (\mathbf{Z}/p^r\mathbf{Z} \times \mathbf{Z}/p^r\mathbf{Z})'$, the set of primitive vectors in $(\mathbf{Z}/p^r\mathbf{Z})^2$. Then we have

$$\text{Meas}(\mathbf{X}, A) = \varprojlim \text{Meas}(\mathbf{X}_r, A),$$

where the maps $\text{Meas}(\mathbf{X}_{r+1}, A) \rightarrow \text{Meas}(\mathbf{X}_r, A)$ are given by $\mu_{r+1} \mapsto \mu_r$, where

$$\mu_r(x) = \sum_{y \equiv x \pmod{p^r}} \mu_{r+1}(y).$$

The map $\Gamma_0(N)/\Gamma_r \rightarrow \mathbf{X}_r$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a \\ c \end{pmatrix}$$

is a bijection and hence induces an isomorphism

$$\text{Meas}(\mathbf{X}_r, A) \cong \text{Ind}_{\Gamma_r}^{\Gamma_0(N)}(A).$$

Thus by Shapiro’s Lemma and the universal coefficient theorem, (54) can be identified with

$$(55) \quad \varprojlim \text{Hom}(H_0(\Gamma_r, \mathcal{M}), A).$$

Concretely, an element of (55) is a sequence of maps $\varphi_r : H_0(\Gamma_r, \mathcal{M}) \rightarrow A$, compatible in the sense that

$$\varphi_r(m) = \sum_i \varphi_{r+1}(\gamma_i^{-1}m) \in A,$$

for all $m \in \mathcal{M}$, where the γ_i range over a set of coset representatives for Γ_r/Γ_{r+1} . The sequence $\{\varphi_r\}$ defines a $\Gamma_0(N)$ -invariant $\text{Meas}(\mathbf{X}, A)$ -valued modular symbol by the rule:

$$\tilde{\mu}_m \left(\left\{ x \in \mathbf{X} : x \equiv \begin{pmatrix} a \\ c \end{pmatrix} \pmod{p^r} \right\} \right) = \varphi_r(\gamma^{-1}m)$$

where γ is a matrix in $\Gamma_0(N)$ that is equivalent to $\begin{pmatrix} a & * \\ c & * \end{pmatrix}$ modulo p^r .

For an element $\tilde{\mu}$ of (55) representing an element of $\mathbf{M}(A)$, the measure of the compact open set $\mathbf{Z}_p^\times \times p\mathbf{Z}_p$ (the inverse image under π of $\mathbf{P}^1(\mathbf{Q}_p) - \mathbf{Z}_p$) is given by the image of $\tilde{\mu}$ in $\text{Hom}(H_0(\Gamma_0(Np), \mathcal{M}), A)$.

Extending our maps via \mathbf{Z}_p -linearity, and identifying $H_0(\Gamma_r, \mathcal{M})_T$ geometrically with $H_1(X_r, \text{cusps}, \mathbf{Z})$, we may write

$$\mathbf{M}(A) = \varprojlim \text{Hom}_{\mathbf{Z}_p}(H_1(X_r, \text{cusps}, \mathbf{Z}_p), A).$$

In relating the module $\mathbf{M}(A)$ to the work of Hida, it will be convenient to dualize the description above. Denote by \check{A} the \mathbf{Z}_p -dual $\text{Hom}_{\mathbf{Z}_p}(A, \mathbf{Z}_p)$; then for two finite free \mathbf{Z}_p -modules A and B , it is clear that $\text{Hom}_{\mathbf{Z}_p}(A, B) = \text{Hom}_{\mathbf{Z}_p}(\check{B}, \check{A})$; we write the map corresponding to $f \in \text{Hom}_{\mathbf{Z}_p}(A, B)$ as $\check{f} \in \text{Hom}_{\mathbf{Z}_p}(\check{B}, \check{A})$, so $\check{f}(g)(a) := g \circ f(a)$. Identifying the dual of $H_1(X_r, \text{cusps}, \mathbf{Z}_p)$ with $H_1(Y_r, \mathbf{Z}_p)$ (where $Y_r = X_r - \text{cusps}$) via Poincaré duality, we then have

$$\mathbf{M}(A) = \varprojlim \text{Hom}_{\mathbf{Z}_p}(\check{A}, H_1(Y_r, \mathbf{Z}_p)).$$

The statement of the proposition is that there exists an element of $\mathbf{M}(H \otimes \mathbf{Z}_p)$ such that its image in $\text{Hom}_{\mathbf{Z}_p}(\check{H}, H_1(Y_0, \mathbf{Z}_p))$ is precisely $\check{\psi}$. Such an element exists since the maps $H_1(Y_r, \mathbf{Z}_p) \rightarrow H_1(Y_{r-1}, \mathbf{Z}_p)$ are surjective. \square

In the course of the above proof, we showed $\mathbf{M}(A) = \text{Hom}_{\mathbf{Z}_p}(\mathbf{M}, A)$, where

$$\mathbf{M} = \varinjlim H_1(X_r, \text{cusps}, \mathbf{Z}_p).$$

As usual \mathbf{M} has a Hecke algebra generated over \mathbf{Z}_p by the diamond operators and the operators T_ℓ , etc.

Remark 5.11. – A point of caution is in order: since the tower defining \mathbf{M} is (essentially) dual to the tower of Section 5.2, one must correspondingly take the dual Hecke operators. In other words, T_ℓ is given by $T \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}$ in the notation of Section 4.2, since these are the operators that are compatible with the maps in the *direct* limit defining \mathbf{M} . In particular, the action of U_p is given by $T \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$, for which the α_i in (35) can be chosen to be

$$\left\{ \begin{pmatrix} 1 & 0 \\ Np^r i & p \end{pmatrix} \right\}_{i=0}^{p-1}$$

for the group $\Delta = \Gamma_r$.

Define the ordinary part $\mathbf{M}(A)^\circ \subset \mathbf{M}(A)$ to be the set of homomorphisms that factor through the ordinary projector $\mathbf{M} \rightarrow \mathbf{M}^\circ \subset \mathbf{M}$. In order to have U_p invertible, we will always assume that the modular symbol $\tilde{\mu}$ arises from \mathbf{M}° .

Let the modular symbol $\tilde{\mu}$ correspond to a \mathbf{Z}_p -module homomorphism $f : \mathbf{M}^o \rightarrow A$. For each element $t \in \text{End}(\mathbf{M}^o)$ of the Hecke algebra of \mathbf{M}^o , the map $f \circ t : \mathbf{M}^o \rightarrow A$ yields another measure-valued modular symbol, which we denote by $\tilde{\mu}^t$.

We also extend all measures on \mathbf{X} to the larger space $\mathbf{Y} := \mathbf{Q}_p^2 - 0$ by imposing invariance under multiplication by p :

$$\tilde{\mu}_m(pU) = \tilde{\mu}_m(U)$$

for all compact opens $U \subset \mathbf{Y}$; this extension is well defined because \mathbf{X} forms a fundamental domain for the action of multiplication by p on \mathbf{Y} . The purpose of this extension is that \mathbf{Y} (considered as column vectors) has a natural action of Γ by left multiplication, whereas \mathbf{X} does not. Recall that P denotes the matrix $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$.

PROPOSITION 5.12. – *Let U be a compact open subset of \mathbf{X} and let $\tilde{\mu}$ be as above. We have*

$$\tilde{\mu}_{Pm}(PU) = \begin{cases} \tilde{\mu}_m^{U_p}(U) & \text{if } U \subset \mathbf{Z}_p^\times \times p\mathbf{Z}_p, \\ \tilde{\mu}_m^{U_p^{-1}}(U) & \text{if } U \subset \mathbf{Z}_p \times \mathbf{Z}_p^\times. \end{cases}$$

Proof. – Let $U(a, c; r, s)$ denote the basic compact open set

$$U(a, c; r, s) = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbf{X} : x \equiv a \pmod{p^r}, y \equiv c \pmod{p^s} \right\}.$$

We will demonstrate the first case of the proposition by considering $U = U(a, c; r, r)$ with $Np|c$ and $(a, p) = 1$. Then

$$\begin{aligned} \tilde{\mu}_{Pm}(PU) &= \tilde{\mu}_{Pm}\left(U\left(a, \frac{c}{p}; r, r-1\right)\right) \\ &= \sum_{i=0}^{p-1} \tilde{\mu}_{Pm}\left(U\left(a, \frac{c}{p} + Np^{r-1}i; r, r\right)\right) \\ &= \varphi_r\left(\sum_{i=0}^{p-1} \begin{pmatrix} a & * \\ \frac{c}{p} + Np^{r-1}i & * \end{pmatrix}^{-1} Pm\right) \\ &= \varphi_r\left(\sum_{i=0}^{p-1} \begin{pmatrix} 1 & 0 \\ Np^r i & p \end{pmatrix}^{-1} \begin{pmatrix} a & * \\ c & * \end{pmatrix}^{-1} m\right) \\ &= \tilde{\mu}_m^{U_p}(U), \end{aligned}$$

where the *’s are chosen so that the resulting matrices lie in $\Gamma_0(N)$. This proves the first case of the proposition. Similarly, one shows that

$$\tilde{\mu}_{P^{-1}m}(P^{-1}V) = \tilde{\mu}_m^{U_p}(V)$$

for $V \subset p\mathbf{Z}_p \times \mathbf{Z}_p^\times$; letting $U = P^{-1}V$ proves the second case of the proposition. \square

COROLLARY 5.13. – *The push forward under π of the modular symbol $\tilde{\mu}$ is precisely μ , i.e.,*

$$\tilde{\mu}_m(\pi^{-1}(U)) = \mu_m(U)$$

for all $m \in \mathcal{M}$ and all compact open $U \subset \mathbf{P}^1(\mathbf{Q}_p)$.

Proof. – The fact that $\tilde{\mu}$ is $\Gamma_0(N)$ -invariant means that

$$(56) \quad \tilde{\mu}_{\gamma m}(\gamma U) = \tilde{\mu}_m(U)$$

for all $\gamma \in \Gamma_0(N)$. Furthermore, we showed in Proposition 5.12 that we can choose a Γ -stable basis of compact opens U of \mathbf{X} satisfying

$$(57) \quad \tilde{\mu}_{Pm}(PU) = \tilde{\mu}_m^{U^{\pm 1}}(U).$$

Combining (56) and (57) we find

$$(58) \quad \tilde{\mu}_{P^{-1}\gamma Pm}(P^{-1}\gamma PU) = \tilde{\mu}_m^{U^e}(U)$$

for $\gamma \in \Gamma_0(N)$, where e denotes some even power depending on γ . Since Γ is generated by its subgroups $\Gamma_0(N)$ and $P^{-1}\Gamma_0(N)P$ (our description of the action of Γ on the tree \mathcal{T} in Section 3.1 shows that Γ is the amalgam of these two subgroups with respect to their intersection $\Gamma_0(M)$, cf. [38, §II.1.4]), Eqs. (56) and (58) imply that

$$(59) \quad \tilde{\mu}_{\gamma m}(\gamma U) = \tilde{\mu}_m^{U^e}(U)$$

for all $\gamma \in \Gamma$. Let us apply this rule with $U = \mathbf{Z}_p^\times \times p\mathbf{Z}_p$:

$$(60) \quad \begin{aligned} \tilde{\mu}_m(\gamma U) &= \tilde{\mu}_{\gamma^{-1}m}^{U^e}(U) \\ &= -U_p^e(\psi(\gamma^{-1}m)) \end{aligned}$$

$$(61) \quad = \mu_m(\gamma(\mathbf{P}^1(\mathbf{Q}_p) - \mathbf{Z}_p)).$$

Here (60) follows from property (53) defining $\tilde{\mu}$; (61) uses the fact that $U_p^2 = 1$ on H , and the definition of μ . Since the Γ translates of $\mathbf{P}^1(\mathbf{Q}_p) - \mathbf{Z}_p$ and its complement form a basis of compact opens for $\mathbf{P}^1(\mathbf{Q}_p)$, the result follows. \square

The modular symbol $\tilde{\mu}$ can be used to split the cocycle $c_\tau^{\mathcal{L}_p}$ explicitly. Define a 0-chain $\rho_\tau \in C^0(\Gamma, \text{Hom}(\mathcal{M}, K_p \otimes H))$ by the rule

$$\begin{aligned} \rho_\tau(m) &:= \int_{\mathbf{X}} \log_p(a - b\tau) d\tilde{\mu}_m(a, b) \\ &:= \lim_{\|\mathcal{U}\| \rightarrow 0} \sum_{U \in \mathcal{U}} \log_p(a_U - b_U\tau) \otimes \tilde{\mu}_m(U), \end{aligned}$$

where the limit is over uniformly finer covers \mathcal{U} of \mathbf{X} by disjoint compact opens U , and (a_U, b_U) is an arbitrary point of U . We will show in stages that $d\rho_\tau = c_\tau^{\mathcal{L}_p}$.

PROPOSITION 5.14. – *If $\gamma \in \Gamma_0(N)$, then*

$$\begin{aligned} \rho_\tau(\gamma^{-1}m) - \rho_\tau(m) &= \log_p \left(\int_{\tau}^{\gamma\tau} \int_m \omega_\mu \right) \\ &= c_\tau^{\mathcal{L}_p}(\gamma)(m). \end{aligned}$$

Proof. – Recall our assumption that τ reduces to the distinguished vertex v^* of the Bruhat–Tits tree of $\mathbf{PGL}_2(\mathbf{Q}_p)$. Since $\Gamma_0(N)$ preserves this vertex, Lemma 4.2 shows that

$$\mathrm{ord}_p \left(\int_{\tau}^{\gamma\tau} \int_m \omega_\mu \right) = 0,$$

and hence the first equality of the proposition implies the second. Write $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Using the $\Gamma_0(N)$ invariance of $\tilde{\mu}$ we calculate $\rho_\tau(\gamma^{-1}m) - \rho_\tau(m)$:

$$\begin{aligned} & \int_{\mathbf{X}} \log_p(x - y\tau) \, d\tilde{\mu}_m(\gamma(x, y)) - \int_{\mathbf{X}} \log_p(x - y\tau) \, d\tilde{\mu}_m(x, y) \\ &= \int_{\mathbf{X}} \left[\log_p((dx - by) - (-cx + ay)\tau) - \log_p(x - y\tau) \right] d\tilde{\mu}_m(x, y) \\ &= \int_{\mathbf{X}} \log_p \left(\frac{(dx - by) - (-cx + ay)\tau}{x - y\tau} \right) d\tilde{\mu}_m(x, y). \end{aligned}$$

Since the integrand depends only on $t = x/y$ and the push forward of $\tilde{\mu}$ is μ , the above expression equals

$$\begin{aligned} & \int_{\mathbf{P}^1(\mathbf{Q}_p)} \log_p \left(\frac{(dt - b) - (-t + a)\tau}{t - \tau} \right) d\mu_m(t) \\ &= \int_{\mathbf{P}^1(\mathbf{Q}_p)} \log_p \left(\frac{t(d + c\tau) - (a\tau + b)}{t - \tau} \right) d\mu_m(t) \\ &= \int_{\mathbf{P}^1(\mathbf{Q}_p)} \log_p \left(\frac{t - \gamma\tau}{t - \tau} \right) d\mu_m(t) + \int_{\mathbf{P}^1(\mathbf{Q}_p)} \log_p(d + c\tau) \, d\mu_m(t) \\ &= \log_p \left(\int_{\tau}^{\gamma\tau} \int_m \omega_\mu \right), \end{aligned}$$

where the last equality follows since μ has total measure zero. \square

For the matrix $P \notin \Gamma_0(N)$, the situation is somewhat different.

PROPOSITION 5.15. –

$$(62) \quad \begin{aligned} & \int_{\mathbf{X}} \log_p(x - y\tau) \, d\tilde{\mu}_{Pm}^U(x, y) - \int_{\mathbf{X}} \log_p(x - y\tau) \, d\tilde{\mu}_m(x, y) \\ &= (\log_p - \mathcal{L}_p \mathrm{ord}_p) \left(\int_{\tau}^{P^{-1}\tau} \int_m \omega_\mu \right). \end{aligned}$$

Proof. – We use the change of variables $(x, y) \mapsto (px, y)$ and the decomposition

$$P^{-1}\mathbf{X} = (\mathbf{Z}_p \times \mathbf{Z}_p^\times) \sqcup \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}^{-1} (\mathbf{Z}_p^\times \times p\mathbf{Z}_p)$$

to break up the first integral (note also $\log_p(px - y\tau) = \log_p(x - \frac{y\tau}{p})$):

$$\begin{aligned} & \int_{\mathbf{X}} \log_p(x - y\tau) d\tilde{\mu}_{P^m}^{U_p}(x, y) \\ &= \int_{\mathbf{Z}_p \times \mathbf{Z}_p^\times} \log_p\left(x - \frac{y\tau}{p}\right) d\tilde{\mu}_{P^m}^{U_p}(px, y) + \int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} \log_p\left(x - \frac{y\tau}{p}\right) d\tilde{\mu}_{P^m}^{U_p}(x, y/p) \\ &= \int_{\mathbf{Z}_p \times \mathbf{Z}_p^\times} \log_p\left(x - \frac{y\tau}{p}\right) d\tilde{\mu}_m(x, y) + \int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} \log_p\left(x - \frac{y\tau}{p}\right) d\tilde{\mu}_m^{U_p^2}(x, y), \end{aligned}$$

by Proposition 5.12. Thus the left-hand side of (62) becomes

$$(63) \quad \int_{\mathbf{X}} \log_p\left(\frac{x - \frac{y\tau}{p}}{x - y\tau}\right) d\tilde{\mu}_m(x, y) - \int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} \log_p\left(x - \frac{y\tau}{p}\right) d\tilde{\mu}_m^{1-U_p^2}(x, y).$$

The first integral of (63) can be pushed forward to $\mathbf{P}^1(\mathbf{Q}_p)$ as in the proof of Proposition 5.14 and equals

$$\log_p\left(\int_{\tau}^{P^{-1}\tau} \int_m \omega_\mu\right).$$

The second integral of (63) may be further decomposed:

$$(64) \quad \begin{aligned} & \int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} \log_p\left(x - \frac{y\tau}{p}\right) d\tilde{\mu}_m^{1-U_p^2}(x, y) \\ &= \int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} \log_p(x) d\tilde{\mu}_m^{1-U_p^2}(x, y) + \int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} \log_p\left(1 - \frac{y\tau}{px}\right) d\tilde{\mu}_m^{1-U_p^2}(x, y). \end{aligned}$$

The second integral of (64) is again a push forward to $\mathbf{P}^1(\mathbf{Q}_p) - \mathbf{Z}_p$; since the push forward of $\tilde{\mu}_m^{1-U_p^2}$ is evidently the zero measure, this integral vanishes. Thus the proposition results from the lemma below (and Lemma 4.2). \square

Recall the notation of Section 5.2.

LEMMA 5.16. – *Let t be an element of \mathbf{T} whose image in \mathcal{T}_0 vanishes. We have*

$$\int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} \log_p(x) d\tilde{\mu}_m^t(x, y) = -t' \cdot \psi(m).$$

Proof. – By Hida’s Theorem 5.6, we need only consider elements of the form $t = (\langle d \rangle - 1)h$, with $h \in \mathbf{T}$. Modulo p^r ,

$$(65) \quad \int_{\mathbf{Z}_p^\times \times p\mathbf{Z}_p} \log_p(x) d\tilde{\mu}_m^t(x, y) \equiv \sum_{\gamma \in \Gamma_0(Np)/\Gamma_r} \log_p(a) \varphi_r(h(\langle d \rangle - 1)\gamma^{-1}m),$$

where a represents the upper left entry of the matrix γ . The action of $\langle d \rangle$ is given by a matrix $\gamma_d \in \Gamma_0(N)$ such that

$$\gamma_d \equiv \begin{pmatrix} d^{-1} & * \\ 0 & d \end{pmatrix} \pmod{p^r},$$

so (65) becomes

$$(66) \quad \sum_{\gamma \in \Gamma_0(Np)/\Gamma_r} \log(a)\varphi_r(h\gamma_d^{-1}\gamma^{-1}m) - \sum_{\gamma \in \Gamma_0(Np)/\Gamma_r} \log(a)\varphi_r(h\gamma^{-1}m).$$

As γ ranges through coset representatives for $\Gamma_0(Np)/\Gamma_r$, the matrices $\gamma\gamma_d$ do as well; the change of variables $\gamma \mapsto \gamma\gamma_d$ in the first sum of (66) simplifies the entire expression to

$$\begin{aligned} \sum_{\gamma \in \Gamma_0(Np)/\Gamma_r} (\log_p(ad) - \log_p(a))\varphi_r(h\gamma^{-1}m) &= \log_p(d) \sum_{\gamma \in \Gamma_0(Np)/\Gamma_r} \varphi_r(h\gamma^{-1}m) \\ &= \log_p(d)\tilde{\mu}_m^h(\mathbf{Z}_p^\times \times p\mathbf{Z}_p) \\ &= -\log_p(d) \cdot h \cdot \psi(m). \end{aligned}$$

This proves the desired result. \square

Propositions 5.14 and 5.15 together imply that for $\gamma \in \Gamma_0(N)$, we have

$$(67) \quad \rho_\tau(P^{-1}\gamma Pm) - \rho_\tau(m) = c_\tau^{\mathcal{L}_p}(P^{-1}\gamma P)(m).$$

Since the groups $\Gamma_0(N)$ and $P^{-1}\Gamma_0(N)P$ generate Γ , Propositions 5.14 and Eq. (67) yield the following proposition, which implies Proposition 5.1:

PROPOSITION 5.17. – *The chain ρ_τ splits the 1-cocycle $c_\tau^{\mathcal{L}_p}$ for the group Γ , i.e., $d\rho_\tau = c_\tau^{\mathcal{L}_p}$.*

5.4. Proof of Proposition 5.4

The methods of this section follow very closely those of [16], but we include the argument for completeness. The map Q yields an exact sequence of $\mathcal{S}[G_p]$ -modules:

$$(68) \quad 0 \rightarrow X \rightarrow \text{Hom}(X, \overline{\mathbf{Q}}_p^\times) \rightarrow J(\overline{\mathbf{Q}}_p) \rightarrow 0.$$

The image of the first nontrivial map above lies in $\text{Hom}(X, \mathbf{Q}_p^\times)$.

DEFINITION 5.3. – The \mathcal{L} -invariant of J is the element of $\text{End}(X \otimes \mathbf{Q}_p)$ such that

$$\log_p Q(x) = \text{ord}_p Q(\mathcal{L}x) \quad \text{for all } x \in X,$$

where $\log_p Q$ and $\text{ord}_p Q$ have been extended via \mathbf{Q}_p -linearity.

Following Greenberg and Stevens, we will interpret the \mathcal{L} -invariant of J as arising from the deformation theory of the Galois action on its Tate module $\text{Ta}_p J$. Let $\text{rec}: \mathbf{Q}_p^\times \rightarrow G_p^{\text{ab}}$ be the Artin reciprocity map. Write Frob_p for $\text{rec}(p)^{-1}$; this is a lifting to G_p^{ab} of the Frobenius map on the maximal unramified extension of \mathbf{Q}_p .

From (68) one finds (by connecting (68) with itself via the multiplication by p^r map, employing the snake lemma, and taking the inverse limit over all r):

$$0 \rightarrow \text{Hom}(X, \text{Ta}_p \overline{\mathbf{Q}}_p^\times) \rightarrow \text{Ta}_p J \rightarrow X \otimes \mathbf{Z}_p \rightarrow 0.$$

Twist the above sequence by the unramified character $\varphi: G_p \rightarrow \mathcal{T}^\times$ that sends Frob_p to U_p (so the module $X(\varphi)$ has trivial G_p -action), and tensor with \mathbf{Q}_p . We then have

$$(69) \quad 0 \rightarrow \text{Hom}(X(\varphi), V_p \overline{\mathbf{Q}}_p^\times) \rightarrow V_p J(\varphi) \rightarrow X(\varphi) \otimes \mathbf{Q}_p \rightarrow 0,$$

where V_p denotes $\mathbf{Q}_p \otimes \text{Ta}_p$. We will denote the three terms in this sequence by A, B , and C , respectively. As noted by Greenberg and Stevens, the \mathcal{L} -invariant of J can be deduced from knowledge about deformations of the sequence (69). A deformation of the module A is a $\mathbf{T}^\circ[G_p]$ -module \mathbf{A} such that $\mathbf{A}/I\mathbf{A} \cong A$ as $(\mathbf{T}^\circ/I\mathbf{T}^\circ)[G_p] = \mathcal{T}_0[G_p]$ -modules, where I is the augmentation ideal of Λ as in Section 5.2. Suppose we have a deformation of the sequence (69), that is, a commutative diagram

$$(70) \quad \begin{array}{ccccccc} 0 & \longrightarrow & I\mathbf{A} & \longrightarrow & I\mathbf{B} & \longrightarrow & I\mathbf{C} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathbf{A} & \longrightarrow & \mathbf{B} & \longrightarrow & \mathbf{C} \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C \longrightarrow 0 \end{array}$$

where we have omitted the 0 terms on both ends of the vertical short exact sequences. Suppose further that \mathbf{A} is a trivial deformation, in the sense that the action of G_p on \mathbf{A} is given by the cyclotomic character (as it is on A). Let $\Psi: G_p \rightarrow \text{End}(\mathbf{C})$ define the Galois action on \mathbf{C} . Since G_p acts trivially on C , for each $\mathbf{c} \in \mathbf{C}$ we have $\sigma(\mathbf{c}) - \mathbf{c} \in I\mathbf{C}$. Consider the image of $\sigma(\mathbf{c}) - \mathbf{c}$ in

$$(71) \quad IC/I^2\mathbf{C} = I/I^2 \otimes_\Lambda \mathbf{C}.$$

As in Section 5.2, we map this via $\log_p \otimes \text{Id}$ to

$$(72) \quad \mathbf{Z}_p \otimes_\Lambda \mathbf{C} = \Lambda/I \otimes_\Lambda \mathbf{C} = \mathbf{C}/I\mathbf{C} = C.$$

Thus to each $\sigma \in G_p$ and $\mathbf{c} \in \mathbf{C}$, we have associated an element denoted $\Psi'(\sigma)(\mathbf{c})$. Furthermore $\Psi'(\sigma)(I\mathbf{C}) = 0$, so $\Psi'(\sigma)$ factors through the quotient $\mathbf{C}/I\mathbf{C} = C$, and may thus be viewed as an element of $\text{End}(C)$. It is trivial to check that $\Psi'(\sigma)$ depends only on the image of $\sigma \in G_p^{\text{ab}}$. We now relate the \mathcal{L} -invariant of J to Ψ' .

PROPOSITION 5.18. – *Let $u \in 1 + p\mathbf{Z}_p$ be a nontrivial unit. Then we have*

$$(73) \quad \Psi'(\text{Frob}_p) = \mathcal{L} \circ \frac{1}{\log_p u} \Psi'(\text{rec}(u))$$

as elements of $\text{End}(C) = \text{End}(X \otimes \mathbf{Q}_p)$.

Proof. – Denote by $\Delta_C: IC \rightarrow C$ the composition of the maps in (71) and (72). Define Δ_A similarly, and use the same notation for the induced maps on cohomology. A basic calculation

verifies the commutativity of the following diagram of G_p -cohomology groups:

$$(74) \quad \begin{array}{ccccc} H^0(C) & \xrightarrow{\delta_C} & H^1(IC) & \xrightarrow{\Delta_C} & H^1(C) \\ -\delta_1 \downarrow & & \delta_2 \downarrow & & \delta_3 \downarrow \\ H^1(A) & \xrightarrow{\delta_A} & H^2(IA) & \xrightarrow{\Delta_A} & H^2(A) \end{array}$$

All of the maps labelled δ arise from coboundary maps in (70). Now G_p acts trivially on C , so $H^0(C) = C$ and $H^1(C) = \text{Hom}_{\text{cont}}(G_p^{\text{ab}}, C)$. Furthermore, for each nontrivial unit $u \in 1 + p\mathbf{Z}_p$, the map $H^1(C) \rightarrow C \oplus C$ given by

$$(75) \quad \pi : \xi \mapsto \left(\xi(\text{Frob}_p), \frac{1}{\log_p u} \xi(\text{rec}(u)) \right)$$

is an isomorphism independent of u .

By definition, $\Psi'(\sigma)(c) = \Delta_C \circ \delta_C(c)(\sigma)$. Also, since \mathbf{A} is a trivial deformation, $\delta_A = 0$. Thus from the commutativity of (74), we have

$$(76) \quad \delta_3 \left(\Psi'(\text{Frob}_p)(c), \frac{1}{\log_p u} \Psi'(\text{rec}(u))(c) \right) = 0$$

for all $c \in C$. We will determine the kernel of δ_3 via the perfect pairings of Tate duality (see [40, §3] for a general reference and [16, p. 422 of §3] for the present application):

$$H^i(C) \times H^{2-i}(A) \rightarrow H^2(\mathbf{Q}_p(1)) = \mathbf{Q}_p, \quad i = 0, 1, 2.$$

This pairing may be described explicitly for $i = 1$ as follows. For each element $\hat{c} \in \text{Hom}(X, \mathbf{Q}_p^\times)$, we define an element $\gamma_{\hat{c}} \in H^1(A)$; choose a p^n th root \hat{c}^{1/p^n} of \hat{c} in $\text{Hom}(X, \overline{\mathbf{Q}}_p^\times)$ for each n , compatible in the sense that $(\hat{c}^{1/p^{n+1}})^p = \hat{c}^{1/p^n}$. The assignment

$$\sigma \mapsto (\sigma - 1)(\hat{c}^{1/p^n}) \in \text{Hom}(X, \text{Ta}_p \overline{\mathbf{Q}}_p^\times)$$

is a cocycle representing a class denoted $\gamma_{\hat{c}} \in H^1(A)$. The definition of $\gamma_{\hat{c}}$ is independent of the choice of p^n th roots of \hat{c} . If

$$\hat{c} = \sum f \otimes q \in X^* \otimes \mathbf{Q}_p^\times = \text{Hom}(X, \mathbf{Q}_p^\times)$$

and $\xi \in H^1(C)$, the Tate duality pairing is given by

$$\langle \xi, \gamma_{\hat{c}} \rangle = \sum f(\xi(\text{rec}(q))) \in \mathbf{Q}_p.$$

From this description, it one verifies that the dual π^* of the isomorphism π from (75) satisfies

$$(77) \quad \begin{aligned} (\pi^*)^{-1} : H^1(A) &\rightarrow C^* \oplus C^*, \\ \gamma_{\hat{c}} &\mapsto (-\text{ord}_p(\hat{c}), \log_p(\hat{c})). \end{aligned}$$

By the self-duality of (69), the kernel of δ_3 is dual to the image of δ_1 . Yet δ_1 is the map $c \mapsto \gamma_{Q(c)}$. Thus (77) implies that the kernel of δ_3 consists of elements of the form $(\mathcal{L}a, a)$; hence (76) yields the result. \square

The following theorem of Mazur and Wiles is the main arithmetic ingredient towards proving $\mathcal{L} = \mathcal{L}_p$.

THEOREM 5.19 (Mazur and Wiles [34]). – *There exists a deformation sequence as in (70) with the Galois action on \mathbf{C} given by $\Psi : G_p \rightarrow \mathbf{T}^\circ \rightarrow \text{End}(\mathbf{C})$ satisfying*

$$\Psi(\text{Frob}_p) = U_p^2 \in \mathbf{T}^\circ \quad \text{and} \quad \Psi(\text{rec}(u)) = \langle u \rangle$$

for $u \in 1 + p\mathbf{Z}_p$.

Proof. – This is Proposition 2 of Chapter 8 in [34]; see the comments at the end of that chapter for a description of the Galois action. Although [34] deals only with $N = 1$, the constructions of [33] from which the result is derived are carried out for higher level N as well. \square

We may now verify Proposition 5.4:

PROPOSITION 5.20. – *The \mathcal{L} -invariant of J is equal to \mathcal{L}_p .*

Proof. – With Ψ as in Theorem 5.19, it is clear that $\Psi'(\text{Frob}_p) = \mathcal{L}_p$ and $\Psi'(\text{rec}(u)) = \log_p u$. Thus the proposition follows from Proposition 5.18. \square

6. Computational examples

Definition 3.1 of the multiplicative double integral is explicitly calculable on a computer. For fixed p , this definition allows one to calculate a given double integral to an accuracy of M p -adic digits in time exponential in M . Darmon and Pollack [9] have devised an algorithm to calculate these double integrals in time polynomial in M , but we use only the naive definition in the present article. The computations of this section were done in PARI/GP to 3 significant p -adic digits.

In this section we restrict to the case $N = 1$. As noted by Manin [28], the group $\overline{H} = H_0(\Gamma_0(p), \mathcal{M})$ has a presentation with generators \tilde{i} for $i \in \mathbf{P}^1(\mathbf{F}_p)$ subject to the relations $\tilde{i} + \tilde{S}i = 0$ and $\tilde{i} + \tilde{T}i + \tilde{T}^2i = 0$, where the matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ act on $\mathbf{P}^1(\mathbf{F}_p)$ by linear fractional transformations. Here the generator \tilde{i} corresponds to the element $[1/i] - [0]$ for an arbitrary lift of i in \mathbf{Z} , and the generator $\tilde{\infty}$ corresponds to $[0] - [\infty]$.

For simplicity, we will only consider the minus quotient H_- , and take ψ_- to be the natural projection $\overline{H} \rightarrow H_-$.

Recall sequence (45):

$$(78) \quad H_2(\Gamma, \mathbf{Z}) \rightarrow H_1(\Gamma, \mathcal{M}) \rightarrow H_1(\Gamma, \text{Div } \mathbf{P}^1(\mathbf{Q})) = \Gamma_\infty^{\text{ab}}.$$

There is an explicit isomorphism $\Gamma_\infty^{\text{ab}} \cong \mathbf{Z} \times \mathbf{Z}/(p^2 - 1)\mathbf{Z}$ given by $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mapsto (\text{ord}_p(a), ab)$. We identify the image of $H_2(\Gamma, \mathbf{Z})$ in $H_1(\Gamma, \mathcal{M})$ as those elements whose images in $\Gamma_\infty^{\text{ab}}$ vanish.

As discussed in the proof of Proposition 4.9, the group $H_2(\Gamma, \mathbf{Z})$ is isomorphic to $H_1(Y_0(p), \mathbf{Z})$ (perhaps modulo some 2- and 3-torsion, which we will ignore). The kernel of $H_1(Y_0(p), \mathbf{Z}) \rightarrow H_1(X_0(p), \text{cusps}, \mathbf{Z})$ is generated by a small loop ℓ around one of the cusps. By sequence (33), the image of ℓ in $H_1(\Gamma, \mathcal{M})$ lies in the image of $H_1(\mathbf{PSL}_2(\mathbf{Z}), \mathcal{M})^2$. But an explicit calculation shows that a generator g of $H_1(\mathbf{PSL}_2(\mathbf{Z}), \mathcal{M})$ maps to $(0, 6)$ in $\Gamma_\infty^{\text{ab}}$; thus the image of ℓ in $H_1(\Gamma, \mathcal{M})$ is precisely $((p^2 - 1)/6)g$. But this multiple of g vanishes under the integration map Φ_1 (we saw already that $\Phi_1(g)$ is torsion, and hence of order dividing $p - 1$; in fact by Mazur's work on the Eisenstein ideal it follows that g has order dividing the numerator of $(p - 1)/12$).

Thus, we may calculate $\Phi_2(y)$ for an element $y \in H_2(\Gamma, \mathbf{Z})$ as follows. We find the image of y in \overline{H} , calculate a pre-image in $H_1(\Gamma, \mathcal{M})$, and modify this pre-image by a multiple of g so that its image in $\Gamma_\infty^{\text{ab}}$ vanishes; this defines an element $y' \in H_1(\Gamma, \mathcal{M})$, and we have

$$\Phi_2(y) = \Phi_1(y') = \int_{\tau}^{\gamma^{-1}\tau} \int_{m_\gamma} \omega_\mu \in \mathbf{Q}_p^\times \otimes H_-,$$

where $\sum m_\gamma[\gamma]$ is a 1-cycle representing y' .

6.1. Genus one

Consider the case $p = 11$. The group \overline{H} is generated by $\tilde{0}$, $\tilde{2}$, and $\tilde{4}$. The subgroup H^+ on which complex conjugation acts as $+1$ is generated by $\tilde{0}$ and $\tilde{2}$, so the quotient $H_- \cong \mathbf{Z}$ is generated by the image of $\tilde{4}$. We calculate a lift of $\tilde{4}$ from \overline{H} to $H_1(\Gamma, \mathcal{M})$ whose image in $\Gamma_\infty^{\text{ab}}$ vanishes, and find that its image under the integration map is

$$q \otimes \tilde{4}, \quad \text{where } q = 10 \cdot 11 + 4 \cdot 11^2 + 9 \cdot 11^3 + O(11^4).$$

This q is the Tate period of the elliptic curve labelled 11A2 in Cremona’s tables, with minimal Weierstrass equation

$$E_{11A2}: y^2 + y = x^3 - x^2 - 7820x - 263580.$$

This elliptic curve is 5-isogenous to $E_{11A1} = X_0(11) = J_0(11)$. The Tate period of E_{11A1} is q^5 , and an explicit isogeny $E_{11A2} = \mathbf{G}_m/q \rightarrow E_{11A1} = \mathbf{G}_m/q^5$ is given by $x \mapsto x^5$. Thus the conjecture that the Stark–Heegner points we define on E_{11A2} are global implies that the Stark–Heegner points which Darmon defines on $X_0(11)$ should be images of global points from E_{11A2} . Computationally, Darmon and Green [8] found even more to be true: their results suggest that the Stark–Heegner points on $X_0(11)$ constructed from the minus modular symbol are all globally multiples of 5.

The cases $p = 17$ and $p = 19$ are similar.

6.2. Genus two

For the cases where $J_0(p)$ has genus two and is simple ($p = 23, 29, 31$), Teitelbaum [39] has provided an explicit power series expression for theta series which can be used to compute the p -adic expansions of the periods. We now compare our results to those which he obtains.

For $p = 23$, the group H is generated by $\tilde{0}$, $\tilde{2}$, $\tilde{5}$, $\tilde{7}$, and $\tilde{16}$. The subgroup H^+ is generated by $\tilde{0}$, $\tilde{2}$, and $\tilde{7} + \tilde{16}$. The quotient H_- is generated by the images of $\tilde{5}$ and $\tilde{7}$. Lifting the elements $\tilde{5}$ and $\tilde{7}$ to elements of $H_1(\Gamma, \mathcal{M})$ in the image of $H_2(\Gamma, \mathbf{Z})$, we find the following periods in $\mathbf{Q}_p^\times \otimes H_-$:

$$\begin{aligned} q_{\tilde{5}} &= 23(5 + 13 \cdot 23 + 19 \cdot 23^2 + O(23^3)) \otimes \tilde{5} + (1 + 18 \cdot 23 + 12 \cdot 23^2 + O(23^3)) \otimes \tilde{7}, \\ q_{\tilde{7}} &= (18 + 0 \cdot 23 + 8 \cdot 23^2 + O(23^3)) \otimes \tilde{5} + 23(19 + 22 \cdot 23 + 19 \cdot 23^2 + O(23^3)) \otimes \tilde{7}. \end{aligned}$$

The supersingular j -invariants in characteristic 23 are -4 , 1728, and 0; the corresponding elliptic curves have automorphism groups of size 2, 4, and 6, respectively. The elements $\gamma_1 = e_{1728} - e_0$ and $\gamma_2 = e_0 - e_{-4}$ form a basis for X . There is an isomorphism of Hecke

modules $\xi'_- : H_- \rightarrow X$ given by $\xi'_-(\tilde{5}) = \gamma_1$ and $\xi'_-(\tilde{7}) = \gamma_1 + \gamma_2$. Letting ξ_- be the composition

$$H_- \xrightarrow{\xi'_-} X \xrightarrow{\text{ord}_p Q} X^*,$$

the commutativity of (44) implies that the pairing $Q : X \times X \rightarrow \mathbf{Q}_p^\times$ is given by the matrix

$$Q(\gamma_i, \gamma_j) = \begin{bmatrix} 23^5(20 + 11 \cdot 23 + 13 \cdot 23^2 + O(23^3)) & 23^{-3}(7 + 17 \cdot 23 + 20 \cdot 23^2 + O(23^3)) \\ 23^{-3}(7 + 17 \cdot 23 + 20 \cdot 23^2 + O(23^3)) & 23^4(4 + 3 \cdot 23 + 5 \cdot 23^2 + O(23^3)) \end{bmatrix}.$$

This agrees with Teitelbaum’s matrix for the periods of $J_0(23)$ with respect to this basis; the cases $p = 29$ and $p = 31$ are similar.

6.3. Genus three

For $p = 41$, the group \overline{H} is generated by $\tilde{0}, \tilde{2}, \tilde{3}, \tilde{4}, \tilde{14}$, and $\tilde{16}$. The subgroup H^+ is generated by $\tilde{0}, \tilde{2}, \tilde{3} - \tilde{14}$, and $\tilde{4}$; the quotient H_- is generated by $\tilde{3}, \tilde{6}$, and $\tilde{16}$. To an accuracy of three 41-adic digits, we calculate the periods:

$$\begin{aligned} q_{\tilde{3}} &= 41(23782 + O(41^3)) \otimes \tilde{3} + (59512 + O(41^3)) \otimes \tilde{6} + (25675 + O(41^3)) \otimes \tilde{16}, \\ q_{\tilde{6}} &= (12226 + O(41^3)) \otimes \tilde{3} + 41(32593 + O(41^3)) \otimes \tilde{6} + (23174 + O(41^3)) \otimes \tilde{16}, \\ q_{\tilde{16}} &= (62438 + O(41^3)) \otimes \tilde{3} + (25675 + O(41^3)) \otimes \tilde{6} + 41(4828 + O(41^3)) \otimes \tilde{16}. \end{aligned}$$

The supersingular j -invariants in characteristic 41 are 0, 3, 28, and 32. The group X has a basis given by $\gamma_1 = e_0 - e_3$, $\gamma_2 = e_3 - e_{28}$, and $\gamma_3 = e_{28} - e_{32}$, and there is a Hecke-equivariant isomorphism $H_- \rightarrow X$ given by $\tilde{3} \mapsto \gamma_2$, $\tilde{6} \mapsto \gamma_1 + 3\gamma_2 - \gamma_3$ and $\tilde{16} \mapsto -\gamma_1 - 2\gamma_2$. We then find the following period matrix for $J_0(41)$:

$$Q(\gamma_i, \gamma_j) = \begin{bmatrix} 41^4(44694 + O(41^3)) & 41^{-1}(584 + O(41^3)) & 44659 + O(41^3) \\ 41^{-1}(584 + O(41^3)) & 41^2(33290 + O(41^3)) & 41^{-1}(61525 + O(41^3)) \\ 44659 + O(41^3) & 41^{-1}(61525 + O(41^3)) & 41^2(37136 + O(41^3)) \end{bmatrix}.$$

Appendix A. Hecke equivariance of the integration map

In Section 3.2 we defined an integration map:

$$(A.1) \quad \int \omega_{\overline{\mu}} : ((\text{Div}_0 \mathcal{H}_p) \otimes M)_\Gamma \rightarrow \overline{T} = \mathbf{G}_m \otimes \overline{H}.$$

In Section 4.2 we defined a Hecke action on $((\text{Div}_0 \mathcal{H}_p) \otimes M)_\Gamma$ and also on \overline{T} .

PROPOSITION A.1. – *The integration map (A.1) is equivariant for T_ℓ, U_ℓ for $\ell \neq p$, and W_∞ .*

Proof. – The first observation is that since $\ell \neq p$, we may take the same set of α_i in defining the Hecke operators for Γ and \overline{H} . Also, we have $\alpha_i e^* = e^*$ for the distinguished edge e^* . We now show that this implies

$$(A.2) \quad \sum_{i=0}^{\ell} \overline{\mu}_{\alpha_i^{-1} m}(\alpha_i^{-1} U) = T_\ell(\overline{\mu}_m(U)).$$

For $\gamma \in \Gamma$, write $\gamma^{-1}\alpha_i = \alpha_{\gamma(i)}\gamma_i^{-1}$ for some index $\gamma(i)$ and $\gamma_i \in \Gamma$. Then

$$\sum_{i=0}^{\ell} \bar{\mu}_{\alpha_i^{-1}m}(\alpha_i^{-1}U_{\gamma e^*}) = \sum_{i=0}^{\ell} \bar{\mu}_{\alpha_i^{-1}m}(\gamma_i U_e^*) = \sum_{i=0}^{\ell} \gamma_i^{-1}\alpha_i^{-1}m = \sum_{j=0}^{\ell} \alpha_j^{-1}\gamma^{-1}m.$$

This proves Eq. (A.2).

We now calculate, for $k = ([\tau_2] - [\tau_1]) \otimes m \in ((\text{Div}_0 \mathcal{H}_p) \otimes M)_{\Gamma}$,

$$\begin{aligned} \text{(A.3)} \quad \left(\int \int \omega_{\bar{\mu}} \right) (T_{\ell} k) &= \prod_i \int_{\alpha_i^{-1}\tau_1 m}^{\alpha_i^{-1}\tau_2} \omega_{\bar{\mu}} \\ &= \prod_i \lim_{\|\mathcal{U}\| \rightarrow 0} \prod_{U \in \mathcal{U}} \left(\frac{t_U - \alpha_i^{-1}\tau_2}{t_U - \alpha_i^{-1}\tau_1} \right) \otimes \bar{\mu}_{\alpha_i^{-1}m}(U) \\ &= \prod_i \lim_{\|\mathcal{U}\| \rightarrow 0} \prod_{U \in \mathcal{U}} \left(\frac{\alpha_i^{-1}t_U - \alpha_i^{-1}\tau_2}{\alpha_i^{-1}t_U - \alpha_i^{-1}\tau_1} \right) \otimes \bar{\mu}_{\alpha_i^{-1}m}(\alpha_i^{-1}U) \\ \text{(A.4)} \quad &= \prod_i \lim_{\|\mathcal{U}\| \rightarrow 0} \prod_{U \in \mathcal{U}} \left(\frac{t_U - \tau_2}{t_U - \tau_1} \right) \otimes \bar{\mu}_{\alpha_i^{-1}m}(\alpha_i^{-1}U) \\ \text{(A.5)} \quad &= \lim_{\|\mathcal{U}\| \rightarrow 0} \prod_{U \in \mathcal{U}} \left(\frac{t_U - \tau_2}{t_U - \tau_1} \right) \otimes T_{\ell}(\bar{\mu}_m(U)). \end{aligned}$$

Eq. (A.4) uses the fact that $\bar{\mu}_m(\mathbf{P}^1(\mathbf{Q}_p)) = 0$, and (A.5) uses (A.2). The right-hand side of (A.5) is

$$T_{\ell} \left(\left(\int \int \omega_{\bar{\mu}} \right) (k) \right),$$

as desired. \square

PROPOSITION A.2. – *The integration map (A.1) is W -equivariant.*

Proof. – The key to this proposition is that the matrix α_p defining W_p on H interchanges the vertices v^* and w^* , and hence sends the edge e^* to its opposite. The action of W on the Γ -coinvariants of a $\mathbf{PGL}_2(\mathbf{Q})$ -module is given by the action of a matrix in R of determinant p . Thus for each $\gamma \in \Gamma$, if we let $\beta = \alpha_p^{-1}\gamma\alpha_p \in \Gamma$, we find that

$$\begin{aligned} \bar{\mu}_{\alpha_p^{-1}m}(\alpha_p^{-1}U_{\gamma e^*}) &= \bar{\mu}_{\alpha_p^{-1}m}(\alpha_p^{-1}\gamma\mathbf{Z}_p) = \bar{\mu}_{\alpha_p^{-1}m}(\beta\alpha_p^{-1}\mathbf{Z}_p) \\ &= -\bar{\mu}_{\alpha_p^{-1}m}(\beta\mathbf{Z}_p) = -\beta^{-1}\alpha_p^{-1}m \\ &= -\alpha_p^{-1}\gamma^{-1}m = W(\bar{\mu}_m(U_{\gamma e^*})). \end{aligned}$$

The proof of the proposition now follows along the proof of Proposition A.1. \square

REFERENCES

[1] BERTOLINI M., DARMON H., Heegner points, p -adic L -functions and the Cerednik–Drinfeld uniformization, *Invent. Math.* **131** (1998) 453–491.
 [2] BERTOLINI M., DARMON H., The rationality of Stark–Heegner points over genus fields of real quadratic fields, in preparation.

- [3] BERTOLINI M., DARMON H., DASGUPTA S., Stark–Heegner points and special values of L -series, in preparation.
- [4] BOSCH S., LÜTKEBOHMERT W., Degenerating Abelian varieties, *Topology* **30** (4) (1991) 653–698.
- [5] BOSCH S., LÜTKEBOHMERT W., RAYNAUD M., Néron Models, *Ergeb. Math. Grenzgeb. (3) (Results in Mathematics and Related Areas (3))*, vol. **21**, Springer, Berlin, 1990.
- [6] DARMON H., Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications, *Ann. of Math. (2)* **154** (3) (2001) 589–639.
- [7] DARMON H., DASGUPTA S., Elliptic units for real quadratic fields, *Ann. of Math.*, submitted for publication.
- [8] DARMON H., GREEN P., Elliptic curves and class fields of real quadratic fields: Algorithms and verifications, *Experimental Math.* **11** (1) (2002) 37–55.
- [9] DARMON H., POLLACK R., The efficient calculation of Stark–Heegner points via overconvergent modular symbols, in preparation.
- [10] DASGUPTA S., Gross–Stark units, Stark–Heegner points, and class fields of real quadratic fields, PhD thesis, University of California–Berkeley, May 2004.
- [11] DASGUPTA S., Computations of elliptic units for real quadratic fields, *Canad. J. Math.*, in press.
- [12] DELIGNE P., RAPOPORT M., Les schémas de modules de courbes elliptiques, in: *Modular Functions of One Variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, in: *Lecture Notes in Math.*, vol. **349**, Springer, Berlin, 1973, pp. 143–316.
- [13] DE SHALIT E., p -adic periods and modular symbols of elliptic curves of prime conductor, *Invent. Math.* **121** (2) (1995) 225–255.
- [14] DE SHALIT E., On the p -adic periods of $X_0(p)$, *Math. Ann.* **303** (1995) 457–472.
- [15] GERRITZEN L., VAN DER PUT M., Schottky Groups and Mumford Curves, *Lecture Notes in Math.*, vol. **817**, Springer, Berlin, 1980.
- [16] GREENBERG R., STEVENS G., p -adic L -functions and p -adic periods of modular forms, *Invent. Math.* **111** (2) (1993) 407–447.
- [17] GREENBERG R., STEVENS G., On the conjecture of Mazur, Tate, and Teitelbaum, in: *p -Adic Monodromy and the Birch and Swinnerton-Dyer conjecture, Boston, MA, 1991*, in: *Contemp. Math.*, vol. **165**, American Mathematical Society, Providence, RI, 1994, pp. 123–211.
- [18] GRIFFITHS P., HARRIS J., Principles of Algebraic Geometry, Reprint of the 1978 original. Wiley Classics Library, Wiley, New York, 1994.
- [19] GROSS B.H., p -adic L -series at $s = 0$, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** (3) (1981) 979–994 (1982).
- [20] GROSS B.H., Kolyvagin’s work on modular elliptic curves, in: *L -Functions and Arithmetic, Durham, 1989*, in: *London Math. Soc. Lecture Note Ser.*, vol. **153**, Cambridge University Press, Cambridge, 1991, pp. 235–256.
- [21] GROSS B.H., ZAGIER D.B., Heegner points and derivatives of L -series, *Invent. Math.* **84** (2) (1986) 225–320.
- [22] HIDA H., Iwasawa modules attached to congruences of cusp forms, *Ann. Sci. École Norm. Sup. (4)* **19** (2) (1986) 231–273.
- [23] ICHIKAWA T., Schottky uniformization theory on Riemann surfaces Mumford curves of infinite genus, *J. reine Angew. Math.* **486** (1997) 45–68.
- [24] IHARA Y., On Congruence Monodromy Problems, vols. 1 and 2, *Lecture Notes*, vols. **1–2**, Department of Mathematics, University of Tokyo, Tokyo, 1968.
- [25] KOEBE P., Über die Uniformisierung der algebraischen Kurven IV, *Math. Ann.* **75** (1914) 42–129.
- [26] KOLYVAGIN V.A., Euler systems, in: *The Grothendieck Festschrift, vol. II*, in: *Progr. Math.*, vol. **87**, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.
- [27] KOLYVAGIN V.A., LOGACHÈV D.Y., Finiteness of the Shafarevich–Tate group and the group of rational points for some modular Abelian varieties, *Algebra i Analiz* **1** (5) (1989) 171–196 (in Russian); translation in: *Leningrad Math. J.* **1** (5) (1990) 1229–1253.
- [28] MANIN J.I., Parabolic points and zeta functions of modular curves, *Izv. Akad. Nauk SSSR Ser. Mat.* **36** (1) (1972) 19–66.
- [29] MANIN Y.I., DRINFELD V., Periods of p -adic Schottky groups, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, *J. reine Angew. Math.* **262/263** (1973) 239–247.

- [30] MAZUR B., Modular curves and the Eisenstein ideal, *Inst. Hautes Études Sci. Publ. Math.* **47** (1977) 33–186 (1978).
- [31] MAZUR B., On the arithmetic of special values of L functions, *Invent. Math.* **55** (3) (1979) 207–240.
- [32] MAZUR B., TATE J., TEITELBAUM J., On p -adic analogues of the conjectures of Birch–Swinnerton-Dyer, *Invent. Math.* **84** (1) (1986) 1–48.
- [33] MAZUR B., WILES A., Class fields of Abelian extensions of Q , *Invent. Math.* **76** (2) (1984) 179–330.
- [34] MAZUR B., WILES A., On p -adic analytic families of Galois representations, *Compositio Math.* **59** (2) (1986) 231–264.
- [35] MUMFORD D., An analytic construction of degenerating curves over complete local rings, *Compositio Math.* **24** (2) (1972) 129–174.
- [36] RIBET K., Congruence relations between modular forms, in: *Proceedings of the International Congress of Mathematicians, vols. 1 and 2, Warsaw, 1983*, PWN, Warsaw, 1984, pp. 503–514.
- [37] SCHOTTKY F., Über eine specielle Function, welche bei einer bestimmten linearen Transformation ihres Arguments unverändert bleibt, *J. reine Angew. Math.* **101** (1887) 227–272.
- [38] SERRE J.-P., Trees, Translated from the French original by John Stillwell. Corrected 2nd printing of the 1980 English translation, Springer Monographs in Mathematics, Springer, Berlin, 2003.
- [39] TEITELBAUM J., p -adic periods of genus two Mumford–Schottky curves, *J. reine Angew. Math.* **385** (1988) 117–151.
- [40] WASHINGTON L., Galois cohomology, in: *Modular Forms and Fermat’s Last Theorem, Boston, MA, 1995*, Springer, New York, 1997, pp. 101–120.

(Manuscrit reçu le 20 octobre 2004 ;
accepté le 22 mars 2005.)

Samit DASGUPTA
Department of Mathematics,
Harvard University,
Oxford Street,
Cambridge, MA 02138, USA
E-mail: dasgupta@post.harvard.edu