ON THE MAZUR–TATE CONJECTURE FOR PRIME CONDUCTOR AND MAZUR'S EISENSTEIN IDEAL

EMMANUEL LECOUTURIER

Yau Mathematical Sciences Center, Jing Zhai, Tsinghua University, Hai Dian District, Beijing China 100084

ABSTRACT. In 1995, Ehud de Shalit proved an analogue of a conjecture of Mazur–Tate for the modular Jacobian $J_0(p)$. His main result was valid away from the Eisenstein primes. We complete the work of de Shalit by including the Eisenstein primes, and give some applications such as an elementary combinatorial identity involving discrete logarithms of difference of supersingular j-invariants. An important tool is our recent work on the so called "generalized cuspidal 1-motive".

1. INTRODUCTION

Let p, $\ell \geq 5$ be primes such that ℓ divides $p - 1$. Let $r = \ell^t$ be the largest power of ℓ dividing $p - 1$ and $R = \mathbf{Z}/r\mathbf{Z}$. Barry Mazur and John Tate formulated in [13] an exceptional zero conjecture modulo r for elliptic curves of conductor p. This was proved under certain technical assumptions by Ehud de Shalit in [4] and [2]. de Shalit in fact proved an analogue of the Mazur–Tate conjecture for the (generalized) Jacobian of the modular curve $X_0(p)$. However, his result was not complete when localizing at the Eisenstein ideal. In this paper we resolve this issue and give various applications using the theory of the Eisenstein ideal, as we now explain in details.

1.1. **Some notation.** We first introduce some notation. We try to follow as much as possible the notation of de Shalit, since we will frequently refer to his papers. Let $\mathscr{D} = \mathbf{Z}[\mathbf{P}^1(\mathbf{Q})]$ and $\mathscr{D}_0$ be the augmentation subgroup of $\mathscr{D}$. The group $\mathrm{GL}_2(\mathbf{Q})$ acts on $\mathbf{P}^1(\mathbf{Q})$ via $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x = \frac{ax+b}{cx+d}$; this induces an action on $\mathscr{D}$ and $\mathscr{D}_0$. We denote by Γ, Γ_0 and Γ_1 the groups $\mathrm{SL}_2(\mathbf{Z})$, $\Gamma_0(p)$ and $\Gamma_1(p)$ respectively. If $G \subset \Gamma$ is a congruence subgroup and V is a left G-module, we denote by $\mathrm{Symb}_G(V)$ the group $\mathrm{Hom}_G(\mathscr{D}_0, V)$ of G-equivariant group homomorphisms $\mathscr{D}_0 \to V$; this is called the space of modular symbols of G in V.

Let $\mathbb{T} = \mathbf{Z}[T_n, n \geq 1]$ be the Hecke algebra over $\mathbf{Z}$ acting on the space of modular forms of weight 2 and level Γ_0, and by $\mathbb{T}^0$ its quotient acting on

---

the cusp forms. There is an action of $\mathbb{T}$ on $\mathrm{Symb}_{\Gamma_0}(R)$ (*cf.* [4, §2.5] for the precise definition).

Let $\log : (\mathbf{Z}/p\mathbf{Z})^\times \to R$ be a fixed surjective group homomorphism. The various equalities stated in this paper will be independent of the choice of $\log$ since both sides will depend on it in the same way. There is a group isomorphism $\mathbf{Q}_p^\times \otimes_{\mathbf{Z}} R \simeq R^2$ given by $\alpha \mapsto (v_R(\alpha), \lambda_R(\alpha))$, where $v_R(\alpha)$ is the reduction modulo r of the p-adic valuation $\mathrm{ord}_p(\alpha)$ of α and $\lambda_R(\alpha)$ is $\log$ of the reduction modulo p of $\alpha \cdot p^{-\mathrm{ord}_p(\alpha)} \in \mathbf{Z}_p^\times$.

1.2. **The Mazur–Tate conjecture for elliptic curves.** Let E is an elliptic curve over $\mathbf{Q}$ of conductor p with split multiplicative reduction at p (*i.e.* $a_p = 1$, where $\sum_{n \geq 1} a_n q^n \in S_2(\Gamma_0(p))$ is the eigenform associated to E). We know that there exists $q_E \in \mathbf{Q}_p^\times$, called the p-adic period of E, such that $E(\overline{\mathbf{Q}}_p) \simeq \overline{\mathbf{Q}}_p^\times / q_E^{\mathbf{Z}}$ as rigid analytic spaces. The Mazur–Tate conjecture may be stated as follows.

Conjecture 1.1 (Mazur–Tate). *For any $\psi \in \mathrm{Symb}_{\Gamma_0}(R)$ such that $T_q \psi = a_q \cdot \psi$ for all primes q, we have in R:*

$$(1) \qquad \lambda_R(q_E) \cdot \psi((0) - (\infty)) = v_R(q_E) \cdot \sum_{a=1}^{p-1} \lambda_R(a) \cdot \psi((a/p) - (\infty)) \ .$$

de Shalit proved the following result.

Theorem 1.2. [4, Theorem 0.3] *Conjecture 1.1 holds if the following conditions are satisfied.*

(i) *$E(\mathbf{Q})$ has no ℓ-torsion.*
(ii) *The degree of a modular parametrization $X_0(p) \to E$ is prime to ℓ.*

Remarks 1.1. (i) As de Shalit notes in [4, §6.3], condition (i) holds except if $E = X_0(11)$, in which case we may check conjecture 1.1 by hand. Thus, although this condition is *a posteriori* not necessary, we emphasize it because our results will allow to remove it *a priori*.
(ii) The necessity of condition (ii) follows from the fact that de Shalit actually works at the level of the Jacobian of $X_0(p)$. Under this condition, we have $v_R(q_E) \in R^\times$ so we may rewrite (1) as

$$(2) \qquad \mathscr{L}_E \cdot \psi((0) - (\infty)) = \sum_{a=1}^{p-1} \lambda_R(a) \cdot \psi((a/p) - (\infty))$$

where $\mathscr{L}_E := v_R(q_E)^{-1} \cdot \lambda_R(q_E) \in R$ is the so-called *refined $\mathscr{L}$-invariant of E*.
(iii) The original conjecture of Mazur and Tate was equality (1) for a specific and canonical modular symbol ψ_E attached to E (*cf.* [4, §6.1]). As de Shalit notices [4, §6.2], this is in fact not necessary and only the Hecke property $T_q \psi = a_q \cdot \psi$ is relevant.

1.3. The Mazur–Tate conjecture for the generalized Jacobian of $X_0(p)$.

We now describe the analogue of the Mazur–Tate conjecture for (the split part of) the Jacobian J_0 of $X_0(p)$ (defined over $\mathbf{Q}$, although most of the time we will consider it over $\mathbf{Q}_p$). The curve $X_0(p)$ has a model over $\mathbf{Z}_p$ whose special fiber is a union of two projective lines intersecting transversally at the supersingular points [5]. We denote by S these supersingular points, *i.e.* the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbf{F}}_p$. It is well-known that the elements of S are defined over $\mathbf{F}_{p^2}$. Let $\mathbf{Q}_{p^2}$ be the unramified quadratic extension of $\mathbf{Q}_p$ and $\mathbf{Z}_{p^2}$ be its valuation ring. By the general theory of Mumford curves, $J_0 \times_{\mathbf{Q}_p} \mathbf{Q}_{p^2}$ has a rigid analytic uniformization by a torus, which we now recall following [3].

We let $N = \mathbf{Z}[S]$ and N_0 the augmentation subgroup of N; there is a canonical action of $\mathbb{T}$ (resp. $\mathbb{T}^0$) on N (resp. N_0). There also is a natural action of $\mathrm{Gal}(\mathbf{F}_{p^2}/\mathbf{F}_p)$, and thus of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, on N and N_0.

There is a canonical symmetric bilinear pairing $Q_0 : N_0 \times N_0 \to \mathbf{Q}_{p^2}^\times$ inducing an isomorphism of rigid analytic spaces over $\mathbf{Q}_{p^2}$ (hence of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_{p^2})$-modules)

$$J_0(p)(\overline{\mathbf{Q}}_p) \simeq \mathrm{Hom}(N_0, \overline{\mathbf{Q}}_p^\times)/q_0(N_0)$$

where $q_0 : N_0 \to \mathrm{Hom}(N_0, \mathbf{Q}_{p^2}^\times)$ is induced by Q (note that q_0 is the analogue of the p-adic period q_E). In [3], de Shalit extended Q_0 to a bilinear pairing $Q : N \times N \to \mathbf{Q}_{p^2}^\times$. We denote by $q : N \to \mathrm{Hom}(N, \mathbf{Q}_{p^2}^\times)$ the induced linear map and by $q_R : N \otimes_{\mathbf{Z}} R \to \mathrm{Hom}(N \otimes_{\mathbf{Z}} R, \mathbf{Q}_{p^2}^\times \otimes_{\mathbf{Z}} R)$ the induced morphism modulo r.

We now state some of the properties of Q. The modular curve $X_0(p)$ has two cusps, namely the classes of 0 and ∞, which are defined over $\mathbf{Q}$. We denote by $J_0^\sharp$ the generalized Jacobian of $X_0(p)$ with respect to the modulus $(0) + (\infty)$. We have an exact sequence of group schemes over $\mathbf{Q}$:

$$1 \to \mathbf{G}_m \to J_0^\sharp \to J_0 \to 1 \ .$$

Proposition 1.3. (i) *The pairing $v_R \circ Q : N \times N \to R$ sends $([E], [E'])$ to $\delta_{E=E'} \cdot w_E$ where $E, E' \in S$ and $w_E \in \{1, 2, 3\}$ is $\frac{\mathrm{Card}(\mathrm{Aut}(E))}{2}$ ($\mathrm{Aut}(E)$ is the automorphism group of E over $\overline{\mathbf{F}}_p$). In particular, as $\ell \geq 5$, $v_R \circ q_R : N \otimes_{\mathbf{Z}} R \to \mathrm{Hom}(N \otimes_{\mathbf{Z}} R, R)$ is an isomorphism.*

(ii) *The pairing Q is symmetric and $\mathbb{T}$-equivariant, i.e. for all x, y in N and $T \in \mathbb{T}$, we have $Q(Tx, y) = Q(Ty, x)$.*

(iii) *The restriction of Q to $N_0 \times N$ takes values in $\mathbf{Q}_p^\times$ and is $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-equivariant, i.e. for all $x \in N_0$, $y \in N$ and $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, we have $Q(\sigma x, \sigma y) = \sigma Q(x, y) = Q(x, y)$. The same is true for Q (without restricting to $N_0 \times N$) modulo principal units of $\mathbf{Q}_{p^2}^\times$.*

(iv) *There is a $\mathbb{T}$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-equivariant group isomorphism*

(3) $$J_0^\sharp(\overline{\mathbf{Q}}_p) \simeq \mathrm{Hom}(N, \overline{\mathbf{Q}}_p^\times)/q(N_0) \ .$$

Proof. Assertion (i) follows from [3, §1.6 (9)]. Assertions (ii) and (iii) follow from [10, Propositions 3.14 and 3.15]. Assertion (iv) follows from [2, §2.3]. $\square$

Definition 1.4. *The* refined $\mathscr{L}$-invariant *of weight* 2 *and level* $\Gamma_0(p)$ *modulo* r *is*

$$\mathscr{L}_R := (v_R \circ q_R)^{-1} \circ (\lambda_R \circ q_R) \in \mathrm{End}(N \otimes_{\mathbf{Z}} R) \ .$$

Proposition 1.3 (iv) combined with a result of Emerton [7] allows us to prove the following result.

Proposition 1.5. *We have* $\mathscr{L}_R \in \mathbb{T} \otimes_{\mathbf{Z}} R$. *Thus,* $\mathscr{L}_R$ *acts naturally on* $\mathrm{Symb}_{\Gamma_0}(R)$.

We warn the reader that what de Shalit denotes by $\mathscr{L}_R$ in [4] is in fact the image of our $\mathscr{L}_R$ in $\mathbb{T}^0 \otimes_{\mathbf{Z}} R$, which we denote by $\mathscr{L}_R^0$.

Recall that in $\mathbb{T}$ we have $U_p^2 = 1$, where U_p is the Hecke operator of index p. If M is a $\mathbb{T} \otimes_{\mathbf{Z}} R$-module and $\epsilon \in \{1, -1\}$, we denote by $M^{U_p = \epsilon}$ the largest subspace of M on which U_p acts by multiplication by ϵ. Note that we have $M = M^{U_p=1} \oplus M^{U_p=-1}$ since ℓ is odd. We prove the following result, which is an extension of [3, Theorem 0.5].

Theorem 1.6 (Main theorem). *For all* $\psi \in \mathrm{Symb}_{\Gamma_0}(R)^{U_p=1}$, *we have*

$$(4) \qquad (\mathscr{L}_R \cdot \psi)((0) - (\infty)) = \sum_{a=1}^{p-1} \lambda_R(a) \cdot \psi((a/p) - (\infty)) \ .$$

Notice the similarity between (2) and (4). de Shalit in fact deduces Theorem 1.2 from [4, Theorem 0.5]. Theorem 1.6 allows us to remove assumption (i) in Theorem 1.2. In [4, Theorem 0.5], de Shalit only proved (4) for modular symbols ψ in a certain subspace of $\mathrm{Symb}_{\Gamma_0}(R)^{U_p=1}$, which is a proper subspace precisely when localizing at the Eisenstein ideal. In other words, we remove the condition "non-Eisenstein" in [4, Theorem 5.6].

1.4. **Strategy of the proof.** We give a rough overview of the proof of Theorem 1.6. The strategy is similar to the one of de Shalit, which is itself inspired by the proof by Ralph Greenberg and Glenn Stevens of the Mazur–Tate–Teitelbaum conjecture [8]. The key player is the Shimura covering $X_1(p) \to X_0(p)$. There are two main steps.

The first step is to prove (4) where $\mathscr{L}_R$ is replaced by a certain Hecke operator which is a "tame" derivative (with respect to the diamond operators) of the operator $U_p^2 - 1$ of level $\Gamma_1(p)$. The analogous statement for $\mathscr{L}_R^0$ was tackled by de Shalit in [4, §3] using 2-variables theta elements ("tame" analogues of 2-variable p-adic L functions).

The second step is to relate $\mathscr{L}_R$ to the above operator. We begin by briefly recalling de Shalit's strategy. By Proposition 1.3 (iv), there is a filtration of $R[\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)]$-modules

$$(5) \qquad 0 \to \mathrm{Hom}(N, \mu_r) \to J_0^{\sharp}[r] \to N_0 \otimes_{\mathbf{Z}} R \to 0 \ ,$$

where μ_r is the module of rth root of unity and $J_0^{\sharp}[r]$ is the r torsion in $J_0^{\sharp}(\overline{\mathbf{Q}}_p)$. de Shalit constructed a deformation of this filtration by considering the r-torsion of the generalized Jacobian $J_1^{\sharp}$ of $X_1(p)$ with respect to the reduced cuspidal modulus. This filtered deformation enabled de Shalit to relate $\mathscr{L}_R^0$ to the tame derivative of $U_p^2 - 1$.

4

Proposition 1.3 (iv) only gives a modular interpretation of the restriction of Q to $N_0 \times N$. To get information on $\mathscr{L}_R$ and not only on $\mathscr{L}_R^0$, we need to consider the full pairing Q. This pairing yields a 1-motive $\mathbf{Z} = N/N_0 \to J_0^\sharp$. One can in fact describe algebraically this 1-motive, and prove that it takes values in $J_0^\sharp(\mathbf{Q})$ [10, Theorem 1.6]. This 1-motive provides a Galois-equivariant extension of $N \otimes_\mathbf{Z} R$ by $\mathrm{Hom}(N, \mu_r)$, which is characterized by $\mathscr{L}_R$. The main point in the two steps above is then to construct a deformation of this extension. This is done in Theorem 2.1 by using the results of [10, Theorem 1.6], where we construct a 1-motive $\mathbf{Z}[\mathrm{cusps}]_0 \to J_1^\sharp$.

1.5. **Applications using Mazur's Eisenstein ideal.** Let $I \subset \mathbb{T}$ be the Eisenstein ideal, *i.e.* the ideal generated by the elements $T_q - q - 1$ for primes $q \neq p$ and $U_p - 1$.

Question 1.7. *Let s be an integer such that $1 \leq s \leq t = \mathrm{ord}_\ell(p-1)$. Can we determine*

$$\alpha(p, \ell, s) := \sup\{n \in \mathbf{Z}_{\geq 0}, \ \mathscr{L}_R \cdot (\mathbb{T} \otimes_\mathbf{Z} \mathbf{Z}/\ell^s\mathbf{Z}) \subset I^n \cdot (\mathbb{T} \otimes_\mathbf{Z} \mathbf{Z}/\ell^s\mathbf{Z})\} \ ?$$

Obviously, $\alpha(p, \ell, s)$ is a decreasing function of s. The first result we prove toward this question is the following.

Theorem 1.8. *We have $\alpha(p, \ell, t) \geq 2$.*

The proof is a simple combination of Theorem 1.6 and basic facts due to Mazur concerning the Eisenstein ideal. Combining Theorem 1.8 and [3, §1.6 Main thm], one can prove the following elementary identity, for which we do not have an elementary proof.

Theorem 1.9. *Assume $p \equiv 1$ (modulo 12), i.e. that for all $E \in S$ we have $w_E = 1$. Let $\mathcal{T}(S)$ be the set of spanning trees of the complete graph with vertices in S. If $T \in \mathcal{T}(S)$, let $\mathcal{E}(T)$ be the set of edges of T. If $E \neq E'$ are in S, let $[E, E']$ be the edge between E and E. We have:*

$$(6) \qquad \sum_{T \in \mathcal{T}(S)} \prod_{[E,E'] \in \mathcal{E}(T)} \log((j(E') - j(E))^{p+1}) = 0 \ .$$

We next give a criterion for $\alpha(p, \ell, s) \geq 3$. Let K be the unique extension of $\mathbf{Q}$ of degree ℓ^t inside $\mathbf{Q}(\zeta_p)$ and $\mathcal{O}_K$ be the ring of integers of K. Let $\mathcal{K}_s = K_2(\mathcal{O}_K[\frac{1}{\ell p}]) \otimes_\mathbf{Z} \mathbf{Z}/\ell^s\mathbf{Z}$, where if A is a ring we denote by $K_2(A)$ the second Quillen K-group of A. There is a canonical action of $\mathbf{Z}[\mathrm{Gal}(K/\mathbf{Q})]$ on $\mathcal{K}_s$. If $x, y \in \mathbf{Z}[\zeta_p, \frac{1}{\ell p}]^\times$, we denote by $\{x, y\} \in K_2(\mathbf{Z}[\zeta_p, \frac{1}{\ell p}])$ the corresponding Steinberg symbol and by (x, y) the image of $\{x, y\}$ under the norm map $K_2(\mathbf{Z}[\zeta_p, \frac{1}{\ell p}]) \to \mathcal{K}_s$.

Theorem 1.10. *We have $\alpha(p, \ell, s) \geq 3$ if and only if the element*

$$(7) \qquad \sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \log(a) \cdot (1 - \zeta_p^a, 1 - \zeta_p) \in J \cdot \mathcal{K}_s$$

belongs to $J^2 \cdot \mathcal{K}_s$, where J is the augmentation ideal of $\mathbf{Z}[\mathrm{Gal}(K/\mathbf{Q})]$.

Remarks 1.2. (i) The classical tame symbol in K-theory yields a group isomorphism $\mathcal{K}_s/J \cdot \mathcal{K}_s \xrightarrow{\sim} \mathbf{Z}/\ell^s\mathbf{Z}$ given by

$$(x,y) \mapsto \log(\overline{x^{v(y)}/y^{v(x)}}) \ ,$$

where $v(x)$ is the $(1-\zeta_p)$-adic valuation of x and the bar means the reduction modulo $(1-\zeta_p)$.

(ii) The proof is a consequence of Theorem 1.6 and our work (with Jun Wang) on a conjecture of Sharifi [11].

(iii) One can show that $\sum_{a\in(\mathbf{Z}/p\mathbf{Z})^\times} \log(a)\cdot(1-\zeta_p^a, 1-\zeta_p)$ always belongs to $J \cdot \mathcal{K}_s$. Furthermore, the group $J \cdot \mathcal{K}_s/J^2 \cdot \mathcal{K}_s$ is isomorphic to $I^2 \cdot (\mathbb{T}\otimes_{\mathbf{Z}}\mathbf{Z}/\ell^s\mathbf{Z})/I^3 \cdot (\mathbb{T}\otimes_{\mathbf{Z}}\mathbf{Z}/\ell^s\mathbf{Z})$. The class of (7) in $J \cdot \mathcal{K}_s/J^2 \cdot \mathcal{K}_s$ corresponds to the class of $\mathscr{L}_R$ in $I^2 \cdot (\mathbb{T}\otimes_{\mathbf{Z}}\mathbf{Z}/\ell^s\mathbf{Z})/I^3 \cdot (\mathbb{T}\otimes_{\mathbf{Z}}\mathbf{Z}/\ell^s\mathbf{Z})$.

(iv) The condition $\alpha(p,\ell,s) \geq 3$ is not always satisfied, *e.g.* if $(p,\ell,s) = (181,5,1)$. It is however satisfied if $I^2 \cdot (\mathbb{T} \otimes_{\mathbf{Z}} \mathbf{Z}/\ell^s\mathbf{Z}) = I^3 \cdot (\mathbb{T} \otimes_{\mathbf{Z}} \mathbf{Z}/\ell^s\mathbf{Z})$, which is the case if and only if $\sum_{k=1}^{\frac{p-1}{2}} k\cdot\log(k) \not\equiv 0$ (modulo ℓ) as a consequence of a result of Merel [14, Théorème 1].

2. Proof of the main theorem

In this section, we prove Theorem 1.6.

2.1. **Notation and conventions.** Keep the notation of section 1. We introduce some more notation. Fix an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$ together with embeddings $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$ and $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$.

Let $\boldsymbol{\Lambda} = R[\mathbf{F}_p^\times]$, $\mathbf{J}$ be the augmentation ideal of $\boldsymbol{\Lambda}$, $\Lambda = R[\mu_r(\mathbf{F}_p^\times)]$, J be the augmentation ideal of Λ, $\Lambda' = R[\mu_{(p-1)/r}(\mathbf{F}_p^\times)]$ and J' be the augmentation ideal of Λ'. Here, for any integer $n \geq 1$ we have denoted by $\mu_n(\mathbf{F}_p^\times)$ the elements of order dividing n in $\mathbf{F}_p^\times$. Note that Λ is a local ring and a direct factor of $\boldsymbol{\Lambda}$. The R-algebra Λ' is étale. We warn the reader that de Shalit uses the notation $\mathbf{I}$, I and I' for $\mathbf{J}$, J and J' respectively (we want to avoid confusion with the Eisenstein ideal). If M is a Λ-module, we denote by $M[J]$ the elements of M annihilated by J (a similar notation applies to $\mathbf{J}$ and J'). We let $\langle . \rangle : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \Lambda^\times$ be the character sending g to $[\chi_p(g)^{(p-1)/r}]$ where $\chi_p : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathbf{F}_p^\times$ is the cyclotomic character modulo p.

Concerning Hecke operators (of level Γ_0 or Γ_1), we will consider the dual ones (induced by Picard functoriality), *i.e.* those considered in [2, §1.1]. We warn the reader that de Shalit uses the *standard* Hecke operators in [4] (*i.e.* those induced by Albanese functoriality). We will only use the Hecke operator U_p in what follows (it is usually denoted by U_p^* in the litterature, *e.g.* in [6, §5.5]). We shall use bold letters for Hecke operators of level Γ_1,

to distinguish them from those of level Γ_0 (*e.g.* $\mathbf{U}_p$ versus U_p). We denote by $\mathbb{T}_1$ the Hecke algebra of weight 2 and level Γ_1 over $\mathbf{Z}$. There is a ring morphism $\Lambda \to \mathbb{T}_1 \otimes_{\mathbf{Z}} R$ sending $[a]$ to $\langle a \rangle$ (the ath dual diamond operator, corresponding to a matrix in Γ_0 whose *upper-left* corner is congruent to a modulo p).

We denote by $\mathcal{C}_0$ and $\mathcal{C}_1$ the cusps of X_0 and X_1 respectively. We have $\mathcal{C}_1 = \mathcal{C}_1^{\mathrm{et}} \sqcup \mathcal{C}_1^{\mu}$ where $\mathcal{C}_1^{\mathrm{et}}$ (resp. $\mathcal{C}_1^{\mu}$) is the set of cusps of X_1 above the cusp 0 (resp. ∞) of X_0.

We choose the standard canonical model for the modular curve X_1 over $\mathbf{Q}$, *i.e.* the moduli space of pairs $(E, \mathbf{Z}/p\mathbf{Z} \hookrightarrow E[p])$. In this model, the cusps of X_1, the cusps in $\mathcal{C}_1^{\mu}$ (resp. $\mathcal{C}_1^{\mathrm{et}}$) are defined over $\mathbf{Q}(\zeta_p)^+$ (resp. $\mathbf{Q}$).

2.2. Construction of a filtered deformation.

Let $\bar{q} : N \to J_0^{\sharp}(\overline{\mathbf{Q}}_p)$ be the composite of $q : N \to \mathrm{Hom}(N, \mathbf{Q}_{p^2}^{\times})$ with the uniformization map $\mathrm{Hom}(N, \overline{\mathbf{Q}}_p^{\times}) \to J_0^{\sharp}(\overline{\mathbf{Q}}_p)$. Since $\bar{q}(N_0) = 0$, $\bar{q}(N)$ is a cyclic group. We let

$$W_0 := (J_0^{\sharp}(\overline{\mathbf{Q}}_p)/\bar{q}(N))[r] \ .$$

By Proposition 1.3, we have a $\mathbb{T}$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-equivariant short exact sequence

$$(8) \qquad\qquad 0 \to W_0^0 \to W_0 \to W_0^1 \to 0 \ .$$

where $W_0^0 = \mathrm{Hom}(N, \mu_r)$ and $W_0^1 = N \otimes_{\mathbf{Z}} R$.

Our key input is the following result, whose proof relies on the ideas developed by the author in [10] and the techniques of de Shalit.

Theorem 2.1. *There exists a R-module W_1 with a commuting action of $\mathbb{T}_1$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ satisfying the following properties.*

(i) W_1 is a free Λ-module of rank $2m + 2$ where m is the genus of X_0.

(ii) There is a group isomorphism $\tau : W_0 \xrightarrow{\sim} W_1[J]$ which is $\mathbb{T}_1$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-equivariant.

(iii) There is a short exact sequence of $\mathbb{T}_1$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ modules

$$(9) \qquad\qquad 0 \to W_1^0 \to W_1 \to W_1^1 \to 0 \ ,$$

where W_1^0 and W_1^1 are free Λ-modules of rank $m + 1$. Furthermore, the analogous exact sequence

$$(10) \qquad\qquad 0 \to W_1^0[J] \to W_1[J] \to W_1^1[J] \to 0 \ .$$

remains exact and is identified with (8) under τ.

(iv) Let $\phi : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{Aut}(W_1)$ be the unramified representation sending Frob_p to $\mathbf{U}_p$ (note that $\mathbf{U}_p$ acts invertibly on W_1 since it does so on $W_1[J]$ by (ii)). The action of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ on W_1^0 is given by ϕ^{-1}. The action of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ on W_1^1 is given by $\phi\langle\cdot\rangle^{-1}$.

Remarks 2.1. (i) Theorem 2.1 is analogous to [4, Theorem 4.3], where de Shalit deforms the filtration (5) (notice that our character $\langle\cdot\rangle$ is inverse to the one of de Shalit in this theorem). The main difference

here is that we have replaced (5) by (8). Another important difference is that the Λ-module W_1 is free, while the analogous statement is false in de Shalit's situation.

(ii) Theorem 2.1 (iv) is similar to [4, Proposition 4.6].

(iii) There is in fact an action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on W_0 and W_1, but the exact sequences (8) and (9) are presumably not $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-stable.

Proof. Following de Shalit, we begin by recalling some facts about the geometry of X_1. Let $K = \mathbf{Q}_p(\zeta_p)$ and $\mathcal{O}_K$ be its ring of integer, where $\zeta_p \in \overline{\mathbf{Q}}_p$ is a primitive pth root of unity. Let $\mathscr{X}_1$ be the model of X_1 over $\mathcal{O}_K$ considered by de Shalit in [2, §2.4]. The special fiber over $\mathbf{F}_p$ of $\mathscr{X}_1$ is the union of two irreducible components Σ^{et} and Σ^{μ}, both isomorphic to the Igusa curve $\mathrm{Ig}(p)$, intersecting at the supersingular points S. The cusps in $\mathcal{C}_1^{\mathrm{et}}$ (resp. $\mathcal{C}_1^{\mu}$) define $\mathcal{O}_K$ points of $\mathscr{X}_1$ whose special fibers lie in Σ^{et} (resp. Σ^{μ}).

We denote by $\mathscr{J}_1^{\sharp}$ the Néron model of $J_1^{\sharp} \times_{\mathbf{Q}} K$ over $\mathcal{O}_K$ and by $(\mathscr{J}_{1/\mathbf{F}_p}^{\sharp})^0$ the connected component of the special fiber of $\mathscr{J}_1^{\sharp}$. We have an exact sequence of abelian group schemes over $\mathbf{F}_p$:

$$(11) \qquad 0 \to \mathrm{Hom}(\mathbf{Z}[S], \mathbf{G}_{m/\mathbf{F}_p}) \to (\mathscr{J}_{1/\mathbf{F}_p}^{\sharp})^0 \to J^{\mathrm{et},\sharp} \times J^{\mu,\sharp} \to 0$$

where $J^{\mathrm{et},\sharp}$ is the generalized Jacobian of Σ^{et} with respect to the reduced cuspidal modulus and similarly for $J^{\mu,\sharp}$. We denote by $(\mathscr{J}_1^{\sharp})^0$ the preimage of $(\mathscr{J}_{1/\mathbf{F}_p}^{\sharp})^0(\overline{\mathbf{F}}_p)$ by the reduction map $\mathscr{J}_1^{\sharp}(\mathcal{O}_K^{\mathrm{unr}}) \to \mathscr{J}_1^{\sharp}(\overline{\mathbf{F}}_p)$ (where $\mathcal{O}_K^{\mathrm{unr}}$ is the valuation ring of the maximal unramified extension K^{unr} of K). Note that $(\mathscr{J}_1^{\sharp})^0$ is a subgroup of $J_1^{\sharp}(K^{\mathrm{unr}})$ by the Néron mapping property. We denote by $\mathscr{J}_1^{\sharp,\mathrm{sub}}$ the kernel of the projection $(\mathscr{J}_1^{\sharp})^0 \to J^{\mu,\sharp}(\overline{\mathbf{F}}_p)$. In the notation of de Shalit [2, §2.7 Definition], we have $\mathscr{J}_1^{\sharp,\mathrm{sub}}[r] = J_1^{\sharp}[r]^{\mathrm{sub}}$ (this follows from the facts that the kernel of the reduction map is a pro-p group and $\gcd(\ell, p) = 1$).

We denote by $\mathscr{J}_1^{',\sharp}$ the Néron model of $J_1^{\sharp}$ over $\mathbf{Z}_p$. If $L \subset \overline{\mathbf{Q}}_p$ is an extension of $\mathbf{Q}_p$ (possibly ramified or infinite) with residue field κ_L and valuation ring $\mathcal{O}_L$, we denote by $(\mathscr{J}_1^{',\sharp})^0(\mathcal{O}_L)$ the preimage of $(\mathscr{J}_{1/\mathbf{F}_p}^{',\sharp})^0(\kappa_L)$ under the reduction map $\mathscr{J}_1^{',\sharp}(\mathcal{O}_L) \to \mathscr{J}_{1/\mathbf{F}_p}^{',\sharp}(\kappa_L)$, where $(\mathscr{J}_{1/\mathbf{F}_p}^{',\sharp})^0$ is the connected component of $\mathscr{J}_{1/\mathbf{F}_p}^{',\sharp}$. By the Néron mapping property, there is a canonical map of $\mathcal{O}_K$-schemes $\mathscr{J}_1^{',\sharp} \times_{\mathbf{Z}_p} \mathcal{O}_K \to \mathscr{J}_1^{\sharp}$. We denote by $\mathcal{G}_1$ the image of $(\mathscr{J}_1^{',\sharp})^0(\mathcal{O}_K^{\mathrm{unr}})$ in $(\mathscr{J}_1^{\sharp})^0$ via the latter map. The argument of [2, Proof of Proposition 2.5] shows that $\mathcal{G}_1$ is contained in $\mathscr{J}_1^{\sharp,\mathrm{sub}}$ and that $\mathcal{G}_1[r] = \mathscr{J}_1^{\sharp,\mathrm{sub}}[r]$.

Lemma 2.2. *For $i \in \{0,1\}$, let $\mathcal{C}_i$ be the set of cusps of the modular curve X_i and $\mathbf{Z}[\mathcal{C}_i]_0$ be the augmentation subgroup of $\mathbf{Z}[\mathcal{C}_i]$. There exists a group homomorphism*

$$\varphi_i : \mathbf{Z}[\mathcal{C}_i]_0 \to J_i^{\sharp}(\overline{\mathbf{Q}})$$

satisfying the following properties.

8

(i) The map φ_i is injective. Furthermore φ_i is $\mathbb{T}_1$ and $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-equivariant.

(ii) We have a commutative diagram

$$
\begin{array}{ccc}
\mathbf{Z}[\mathcal{C}_0]_0 & \xrightarrow{\;\varphi_0\;} & J_0^\sharp(\overline{\mathbf{Q}}) \\
\downarrow & & \downarrow \\
\mathbf{Z}[\mathcal{C}_1]_0 & \xrightarrow{\;\varphi_1\;} & J_1^\sharp(\overline{\mathbf{Q}})
\end{array}
$$

where the vertical maps are the natural maps.

(iii) The following two maps $\mathbf{Z} \to J_0^\sharp(\overline{\mathbf{Q}}_p)$ coincide:

- The map $\mathbf{Z} \to J_0^\sharp(\overline{\mathbf{Q}}_p)$ obtained from φ_0 after identifying $\mathbf{Z}[\mathcal{C}_0]_0$ with $\mathbf{Z}$ (via the choice of $(\infty) - (0)$ as a generator) and embedding $J_0^\sharp(\overline{\mathbf{Q}})$ into $J_0^\sharp(\overline{\mathbf{Q}}_p)$.
- The map $\mathbf{Z} \to J_0^\sharp(\overline{\mathbf{Q}}_p)$ obtained from $\overline{q} : \mathbf{Z} = N/N_0 \to J_0^\sharp(\overline{\mathbf{Q}}_p)$.

(iv) The group $\varphi_1(\mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0)$ is contained in $r \cdot \mathcal{G}_1$ (and thus in $\mathscr{J}_1^{\sharp,\mathrm{sub}}$).

(v) The $\mathbf{J}$-coinvariants of $(J_1^\sharp(\overline{\mathbf{Q}})/\varphi_1(\mathbf{Z}[\mathcal{C}_1]_0))[r]$ is a free R-module of rank $2m + 2$ (where $m = \mathrm{genus}(X_0)$).

Remark 2.1. Actually, the group $\mathcal{G}_1$ is r-divisible so $r \cdot \mathcal{G}_1 = \mathcal{G}_1$.

Proof. We will use the results of [10]. For the convenience of the reader, we recall some of the notation of that paper. Let X be a proper smooth curve over a field k, F be any field extension of k, $F(X)$ be the function field of $X \times_k F$, $\mathcal{C}$ be a subset of $X(F)$, $Y = X \backslash \mathcal{C}$ and $J^\sharp$ be the generalized Jacobian (over k) of X relative to the reduced modulus with support in $\mathcal{C}$. If P is a closed point in $X \times_k F$, let $F(X)_P$ be the completion of $F(X)$ at P and $U_P \subset F(X)_P^\times$ be the group of principal units. Let

$$
\mathrm{Div}(X, \mathcal{C})(F) := \mathrm{Div}(Y)(F) \oplus \bigoplus_{c \in \mathcal{C}} F(X)_c^\times / U_c^\times \ ,
$$

where $\mathrm{Div}(Y)(F)$ is the group of divisors of Y defined over F. We denote by $\mathrm{Div}^0(X, \mathcal{C})(F)$ the kernel of the degree map $\mathrm{Div}(X, \mathcal{C})(F) \to \mathbf{Z}$ given by

$$
D \oplus (f_c \text{ modulo } U_c)_{c \in \mathcal{C}} \mapsto \deg(D) + \sum_{c \in \mathcal{C}} \mathrm{ord}_c(f_c) \ .
$$

There is a canonical map $F(X)^\times \to \mathrm{Div}^0(X, \mathcal{C})(F)$, given by

$$
f \mapsto \mathrm{div}_Y(f) \oplus (f \text{ modulo } U_c)_{c \in \mathcal{C}}
$$

where $\mathrm{div}_Y(f)$ is the divisor of the restriction of f to Y. Then there is a canonical $\mathrm{Gal}(F/k)$-equivariant group isomorphism

(12) $$ J^\#(F) \xrightarrow{\sim} \mathrm{Div}^0(X, \mathcal{C})(F)/F(X)^\times $$

sending the class of a divisor D supported on Y to the image of $(D \oplus 0)$ in $\mathrm{Div}^0(X, \mathcal{C})(F)/F(X)^\times$.

We can now give the definition of φ_0 and φ_1. We start with φ_0. Note that j^{-1} (resp. $(j \circ w_p)^{-1}$, where w_p is the Atkin–Lehner involution) is a uniformizer at the cusp ∞ (resp. 0) of X_0. Then φ_0 sends $(\infty) - (0)$ to the class of $j^{-1} \oplus j \circ w_p$ in $\mathrm{Div}^0(X_0, \mathcal{C}_0)(\mathbf{Q})/\mathbf{Q}(X_0)^\times$ (the latter group being

identified with $J_0^{\#}(\mathbf{Q})$ by (12)). Property (i) for $i = 0$ follows from [10, Theorem 1.6 (ii)]. Property (iii) follows from [10, Theorem 1.7].

We now define φ_1. Note that j^{-1} (resp. $(j \circ w_p)^{-1}$) is a uniformizer at any cusp in $\mathcal{C}_1^{\mu}$ (resp. $\mathcal{C}_1^{\mathrm{et}}$). We then define $\varphi_1(\sum_{c \in \mathcal{C}_1^{\mu}} n_{\mu,c} \cdot [c] + \sum_{c \in \mathcal{C}_1^{\mathrm{et}}} n_{\mathrm{et},c} \cdot [c])$ as the class of $(j^{-n_{\mu,c}})_{c \in \mathcal{C}_1^{\mu}} \oplus ((j \circ w_p)^{-n_{\mathrm{et},c}})_{c \in \mathcal{C}_1^{\mathrm{et}}}$ in

$$\mathrm{Div}^0(X_1, \mathcal{C}_1)(\mathbf{Q}(\zeta_p))/\mathbf{Q}(\zeta_p)(X_1)^{\times} \simeq J_1^{\#}(\mathbf{Q}(\zeta_p))$$

(the isomorphism coming from (12)).

We prove property (i) for $i = 1$. The injectivity of φ_1 follows from [10, Theorem 1.5 (ii), Theorem 1.1, Remark 3.1 (i)]. Let us prove that φ_1 is $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-equivariant. The action of $g \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $\mathrm{Div}^0(X_1, \mathcal{C}_1)(\overline{\mathbf{Q}})$ is given by the usual action on $\mathrm{Div}(Y_1)(\overline{\mathbf{Q}})$ and the following action on $\bigoplus_{c \in \mathcal{C}_1} F(X)_c^{\times}/U_c^{\times}$:

$$g \cdot (f_c)_{c \in \mathcal{C}_1} = (g \cdot f_c)_{g(c), c \in \mathcal{C}_1} \ .$$

Since j and $j \circ w_p$ are defined over $\mathbf{Q}$ and $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ stabilizes $\mathcal{C}_1^{\mathrm{et}}$ and $\mathcal{C}_1^{\mu}$, we see that φ_1 is indeed $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-equivariant.

It remains to prove that φ_1 is $\mathbb{T}_1$-equivariant (recall that we have chosen the dual Hecke operators). Let $D = D^{\mu} + D^{\mathrm{et}} \in \mathbf{Z}[\mathcal{C}_1]_0$, where $D^{\mu} = \sum_{c \in \mathcal{C}_1^{\mu}} m_c \cdot c \in \mathbf{Z}[\mathcal{C}_1^{\mu}]$ and $D^{\mathrm{et}} = \sum_{c \in \mathcal{C}_1^{\mathrm{et}}} e_c \cdot c \in \mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]$. We want to prove that $\varphi_1(T \cdot D) = T \cdot \varphi_1(D)$ where T is the Hecke operator $\langle a \rangle$, $\mathbf{T}_{\ell}$ or $\mathbf{U}_p$ ($a \in (\mathbf{Z}/p\mathbf{Z})^{\times}$, $\ell \neq p$ prime).

We easily check that $\langle a \rangle \cdot \varphi_1(D)$ is the class of

$$(j^{-m_{\langle a \rangle^{-1} \cdot c}} \circ \langle a \rangle^{-1})_{c \in \mathcal{C}_1^{\mu}} \oplus (j^{-e_{\langle a \rangle^{-1} \cdot c}} \circ w_p \circ \langle a \rangle^{-1})_{c \in \mathcal{C}_1^{\mathrm{et}}}$$

in $J_1^{\sharp}$, which is the equal to the class of

$$(j^{-m_{\langle a \rangle^{-1} \cdot c}})_{c \in \mathcal{C}_1^{\mu}} \oplus (j^{-e_{\langle a \rangle^{-1} \cdot c}} \circ w_p)_{c \in \mathcal{C}_1^{\mathrm{et}}}$$

$$= (j^{-m_c})_{\langle a \rangle \cdot c, c \in \mathcal{C}_1^{\mu}} \oplus (j^{-e_c} \circ w_p)_{\langle a \rangle \cdot c, c \in \mathcal{C}_1^{\mathrm{et}}}$$

$$= \varphi_1(\langle a \rangle \cdot D) \ .$$

This proves that $\langle a \rangle \cdot \varphi_1(D) = \varphi_1(\langle a \rangle \cdot D)$.

We now consider the Hecke operator $\mathbf{T}_{\ell}$. If $c \in \mathcal{C}_1^{\mu}$, we have $\mathbf{T}_{\ell}(c) = (\ell \cdot \langle \ell \rangle + 1)(c)$. Similarly, if $c \in \mathcal{C}_1^{\mathrm{et}}$, we have $\mathbf{T}_{\ell}(c) = (\langle \ell \rangle + \ell)(c)$. If $i \in \{0, 1, ..., \ell-1\}$, let $g_i = \begin{pmatrix} 1 & i \\ 0 & \ell \end{pmatrix}$. Let $g_{\infty} = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(p)$ be such that $d \equiv \ell$ (modulo p). We easily check that $\mathbf{T}_{\ell} \cdot \varphi_1(D)$ is the class in $J_1^{\sharp}$ of $(f_c)_{c \in \mathcal{C}_1^{\mu}} \oplus (h_c)_{c \in \mathcal{C}_1^{\mathrm{et}}}$ where f_c and h_c are functions on the upper-half plane $\mathfrak{h}$ given by

$$f_c = (j^{-m_{\langle \ell \rangle^{-1} \cdot c}} \circ g g_{\infty}) \cdot \prod_{i=0}^{\ell-1} j^{-m_c} \circ g_i$$

and

$$h_c = (j^{-e_{\langle \ell \rangle^{-1} \cdot c}} \circ w_p \circ g g_{\infty}) \cdot (j^{-e_c} \circ w_p \circ g_0) \cdot \prod_{i=1}^{\ell-1} j^{-e_{\langle \ell \rangle^{-1} \cdot c}} \circ w_p \circ g_i \ .$$

10

Note that $j(z)^{-1} \equiv e^{2i\pi z}$ (modulo U_∞) where $z \in \mathfrak{h}$ is near $i\infty$. Thus, we have

$$f_\infty(z) \equiv (e^{2i\pi \cdot \ell z})^{m_{\langle \ell \rangle - 1}\infty} \cdot \prod_{i=0}^{\ell-1} (e^{2i\pi \cdot \frac{z+i}{\ell}})^{m_\infty} \text{ (modulo } U_\infty) \ .$$

We get

$$f_\infty \equiv (-1)^{\ell-1} \cdot j^{-\ell \cdot m_{\langle \ell \rangle - 1} \cdot \infty - m_\infty} \text{ (modulo } U_\infty) \ .$$

More generally, for any $c \in \mathcal{C}_1^\mu$ we have

$$f_c \equiv (-1)^{\ell-1} j^{-\ell \cdot m_{\langle \ell \rangle - 1} \cdot c - m_c} \text{ (modulo } U_c) \ .$$

Similarly, for any $c \in \mathcal{C}_1^{\mathrm{et}}$ we have

$$h_c \equiv (-1)^{\ell-1} \cdot j^{-\ell \cdot e_c - e_{\langle \ell \rangle - 1} \cdot c} \circ w_p \text{ (modulo } U_c) \ .$$

This proves that $\mathbf{T}_\ell \cdot \varphi_1(D) = \varphi_1(\mathbf{T}_\ell \cdot D)$. The proof for $\mathbf{U}_p$ is similar and left to the reader.

Property (ii) follows from the functoriality of our construction of φ_0 and φ_1. We prove property (iv). By construction, the restriction of φ_1 to $\mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0$ takes values in $J_1^\sharp(\mathbf{Q})$ (we use the fact that $j \circ w_p : X_1(p) \to \mathbf{P}^1$ and $\mathcal{C}_1^{\mathrm{et}}$ are defined over $\mathbf{Q}$). By the Néron mapping property, φ_1 induces group homomorphisms $\varphi_1' : \mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0 \to \mathscr{J}_1^{',\sharp}(\mathbf{Z}_p) \hookrightarrow \mathscr{J}_1^{',\sharp}(\mathcal{O}_K) = (\mathscr{J}_1^{',\sharp} \times_{\mathbf{Z}_p} \mathcal{O}_K)(\mathcal{O}_K)$ and $\varphi_1'' : \mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0 \to \mathscr{J}_1^\sharp(\mathcal{O}_K)$ satisfying a commutative diagram:

$$\mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0 \xrightarrow{\varphi_1'} (\mathscr{J}_1^{',\sharp} \times_{\mathbf{Z}_p} \mathcal{O}_K)(\mathcal{O}_K)$$
$$\searrow^{\varphi_1''} \qquad \downarrow \qquad \qquad .$$
$$\mathscr{J}_1^\sharp(\mathcal{O}_K)$$

It remains to show that φ_1' takes values in $r \cdot (\mathscr{J}_1^{',\sharp})^0(\mathcal{O}_K^{\mathrm{unr}})$. Since the group $(\mathscr{J}_1^{',\sharp})^0(\mathbf{Z}_p^{\mathrm{unr}})$ is r-divisible, it suffices to prove that φ_1' takes values in $(\mathscr{J}_1^{',\sharp})^0(\mathbf{Z}_p)$. Let $\mathscr{J}_1'$ the Néron model of the (usual as opposed to generalized) Jacobian of X_1 over $\mathbf{Z}_p$. Define $(\mathscr{J}_1')^0(\mathbf{Z}_p) \subset \mathscr{J}_1'(\mathbf{Z}_p)$ similarly. There is a canonical map $\pi : \mathscr{J}_1^{',\sharp}(\mathbf{Z}_p) \to \mathscr{J}_1'(\mathbf{Z}_p)$ and the preimage of $(\mathscr{J}_1')^0(\mathbf{Z}_p)$ by this map is $(\mathscr{J}_1^{',\sharp})^0(\mathbf{Z}_p)$. Thus it suffices to prove that $\pi \circ \varphi_1'$ takes values in $(\mathscr{J}_1')^0(\mathbf{Z}_p)$. By construction, $\pi \circ \varphi_1'$ is the canonical map sending a divisor to its class in the Jacobian. Since all the cusps in $\mathcal{C}_1^{\mathrm{et}}$ lie in the same irreducible component in the special fiber, $\pi \circ \varphi_1'$ takes values in $(\mathscr{J}_1')^0(\mathbf{Z}_p)$ (the connected component of the special fiber corresponds to divisors which have degree 0 in each irreducible component).

We finally prove property (v). Since $\gcd(r, 2p) = 1$, [10, Theorem 1.5 (ii) and Theorem 2.10 (vii)] shows that we have an isomorphism of $\mathbb{T}_1$-modules

$$(J_1^\sharp(\overline{\mathbf{Q}})/\varphi_1(\mathbf{Z}[\mathcal{C}_1]_0))[r] \simeq H_1(X_1, \mathcal{C}_1, R)_+ \oplus H_1(Y_1, R)_- \ .$$

Here, $H_1(X_1, \mathcal{C}_1, R)$ is the first singular homology group of X_1 relative the cusps with coefficients in R, and similarly for $H_1(Y_1, R)$. These two groups have a natural action of the complex conjugation. The '+' (resp. '−') in the subscript means the subspace on which the complex conjugation acts

11

by multiplication by 1 (resp. -1). The R-modules $H_1(X_0, \mathcal{C}_0, R)_+$ and $H_1(Y_0, R)_-$, set in duality by the intersection pairing, are each free of rank $m + 1$ over R. In order to prove property (v), it thus suffices to prove that the natural maps

(13) $$H_1(X_1, \mathcal{C}_1, R)/\mathbf{J} \cdot H_1(X_1, \mathcal{C}_1, R) \to H_1(X_0, \mathcal{C}_0, R)$$

and

$$H_1(Y_1, R)/\mathbf{J} \cdot H_1(Y_1, R) \to H_1(Y_0, R)$$

are isomorphisms. The former map is shown to be an isomorphism in [2, Proposition 1.3] (where we use the fact that $H_1(X_1, \mathcal{C}_1, R) \simeq H^1(\Gamma_1, R)$). As for the latter map, notice it is a surjective map so it suffices to prove that $H_1(Y_1, R)/\mathbf{J} \cdot H_1(Y_1, R)$ is a free R-module of rank $2m + 1$. There is a perfect and $\mathbf{\Lambda}$-equivariant pairing $H_1(X_1, \mathcal{C}_1, R) \times H_1(Y_1, R) \to R$ (namely the intersection pairing twisted by the Atkin–Lehner involution). In [2, Step 1, Proof of Proposition 2.8], it is shown that as a $\mathbf{\Lambda}$-module, $H_1(X_1, \mathcal{C}_1, R)$ is isomorphic to $\mathbf{\Lambda}^{2m} \oplus \mathbf{\Lambda}/\mathbf{J}$. Thus, we have a $\mathbf{\Lambda}$-equivariant group isomorphism $H_1(Y_1, R) \simeq \mathbf{\Lambda}^{2m} \oplus \mathbf{\Lambda}/\mathbf{J}$. This proves that $H_1(Y_1, R)/\mathbf{J} \cdot H_1(Y_1, R)$ has rank $2m + 1$ over R. This concludes the proof of property (v), and thus the proof of Lemma 2.2. $\qquad\square$

We define

$$\mathbf{W}_1 = (J_1^\sharp(\overline{\mathbf{Q}}_p)/\varphi_1(\mathbf{Z}[\mathcal{C}_1]_0))[r],$$
$$\mathbf{W}_1^0 = (\mathscr{J}_1^{\sharp,\mathrm{sub}}/\varphi_1(\mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0))[r]$$

and $\mathbf{W}_1^1 = \mathbf{W}_1/\mathbf{W}_1^0$. By Lemma 2.2 (i), $\mathbf{W}_1$ is a $\mathbb{T}_1$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-module. Furthermore, $\mathbf{W}_1^0$ is a sub- $\mathbb{T}_1$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/K)$-module.

Lemma 2.3. *The inclusion $\mathcal{G}_1 \subset \mathscr{J}_1^{\sharp,\mathrm{sub}}$ induces an isomorphism*

$$(\mathcal{G}_1/\varphi_1(\mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0))[r] \xrightarrow{\sim} W_1^0 \ .$$

In particular, $\mathbf{W}_1^0$ is stable by $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$.

Proof. We first note that by Lemma 2.2 (iv), $\mathcal{G}_1/\varphi_1(\mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0)$ is well-defined. Let $x \in \mathscr{J}_1^{\sharp,\mathrm{sub}}$ such that $r \cdot x \in \varphi_1(\mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0)$. By Lemma 2.2 (iv), there exists $y \in \mathcal{G}_1$ such that $r \cdot x = r \cdot y$. Thus, we have $r \cdot (x - y) = 0$, so $x - y \in \mathscr{J}_1^{\sharp,\mathrm{sub}}[r] = \mathcal{G}_1[r]$. This proves that $x \in \mathcal{G}_1$. The second statement of the lemma follows from the fact that $\mathscr{J}_1^{',\sharp}$ is defined over $\mathbf{Z}_p$. $\qquad\square$

We define $W_1 = \mathbf{W}_1[J']$, $W_1^0 = \mathbf{W}_1^0[J']$ and $W_1^1 = \mathbf{W}_1^1[J']$. Since taking the kernel by J' is exact, we have an exact sequence of Λ-modules

$$0 \to W_1^0 \to W_1 \to W_1^1 \to 0 \ .$$

Furthermore, this exact sequence is $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ and $\mathbb{T}_1$ equivariant.

We prove Theorem 2.1 (i). By Lemma 2.2 (v), the R-module $W_1/J \cdot W_1$ is free of rank $2m + 2$. By Nakayama's lemma, there is a surjection of Λ-modules $\Lambda^{2m+2} \to W_1$. To prove that this surjection is an isomorphism, it suffices to prove that the rank of W_1 over R is $r \cdot (2m + 2)$. By Lemma 2.2 (i), the snake lemma provides an exact sequence of Λ-modules

(14) $$0 \to J_1^\sharp(\overline{\mathbf{Q}}_p)[r, J'] \to W_1 \to (\Lambda \oplus \Lambda)_0 \to 0$$

12

where $(\Lambda \oplus \Lambda)_0$ is the kernel of the composite $\Lambda \oplus \Lambda \xrightarrow{(x,y) \mapsto x+y} \Lambda \to \Lambda/J = R$ (we identify $(\Lambda \oplus \Lambda)_0$ with $R[\mathcal{C}_1]_0[J']$). The R-module $J_1^\sharp(\overline{\mathbf{Q}})[r, J']$ is free of rank $2rm+1$ (this follows from the Riemann-Hurwitz formula, alternatively this follows from [2, Theorem 1]). The R-module $(\Lambda \oplus \Lambda)_0$ is free of rank $2r - 1$. This proves that the R-module W_1 is free of rank $r \cdot (2m + 2)$, so this concludes the proof of Theorem 2.1 (i).

We prove Theorem 2.1 (ii). By Lemma 2.2 (ii) and (iii), (14) fits into a commutative diagram of R-modules whose rows are exact:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & J_1^\sharp(\overline{\mathbf{Q}}_p)[r, J'] & \longrightarrow & W_1 & \longrightarrow & (\Lambda \oplus \Lambda)_0 & \longrightarrow & 0 \\
& & \uparrow & & {\scriptstyle \tau}\uparrow & & \uparrow & & \\
0 & \longrightarrow & J_0^\sharp(\overline{\mathbf{Q}}_p)[r] & \longrightarrow & W_0 & \longrightarrow & R & \longrightarrow & 0
\end{array} \quad .
$$

By [4, Proposition 4.2], the vertical map $J_0^\sharp(\overline{\mathbf{Q}})[r] \to J_1^\sharp(\overline{\mathbf{Q}})[r, J']$ is injective and its image is $J_1^\sharp(\overline{\mathbf{Q}})[r, \mathbf{J}]$. The vertical map $R \to (\Lambda \oplus \Lambda)_0$ sends 1 to $\sum_{\zeta \in \mu_r(\mathbf{F}_p)}[\zeta] \oplus -\sum_{\zeta' \in \mu_r(\mathbf{F}_p)}[\zeta']$, so it is injective. It follows that τ is injective. Since the image of τ is clearly contained in $W_1[J]$, it remains to show the equality. It suffices to prove that $W_1[J]$ is a free R-module of the same rank as the one of W_0, namely $2m + 2$. This follows from Theorem 2.1 (i). The map τ is $\mathbb{T}_1$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-equivariant by construction, so this proves Theorem 2.1 (ii).

We prove Theorem 2.1 (iii). de Shalit constructed an exact sequence (*cf.* [2, §2.7]) of $\mathbb{T}_1$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-modules:

$$
0 \to J_1^\sharp[r]^{\mathrm{sub}} \to J_1^\sharp[r] \to J_1^\sharp[r]^{\mathrm{quot}} \to 0 \ .
$$

Furthermore, de Shalit proved (*cf.* [4, Theorem 4.3]) that we have isomorphisms of Λ-modules $J_1^\sharp[r]^{\mathrm{sub}} \simeq R \oplus \Lambda^m$ and $J_1^\sharp[r]^{\mathrm{quot}} \simeq \Lambda^m$. By construction, we have $J_1^\sharp[r]^{\mathrm{sub}} = \mathscr{J}_1^{\sharp,\mathrm{sub}}[r]$. Thus, we have a commutative diagram whose rows and columns are exact, $\mathbb{T}_1$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ equivariant:

$$
\begin{array}{ccccccccc}
& & 0 & & 0 & & 0 & & \\
& & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & R[\mathcal{C}_1^{\mathrm{et}}]_0[J'] & \longrightarrow & R[\mathcal{C}_1]_0[J'] & \longrightarrow & R[\mathcal{C}_1^\mu][J'] & \longrightarrow & 0 \\
& & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & W_1^0 & \longrightarrow & W_1 & \longrightarrow & W_1^1 & \longrightarrow & 0 \\
& & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & J_1^\sharp[r]^{\mathrm{sub}}[J'] & \longrightarrow & J_1^\sharp[r][J'] & \longrightarrow & J_1^\sharp[r]^{\mathrm{quot}}[J'] & \longrightarrow & 0 \\
& & \uparrow & & \uparrow & & \uparrow & & \\
& & 0 & & 0 & & 0 & &
\end{array} \quad .
$$

Note that the middle column is isomorphic to (14). Note also that as we have isomorphisms of Λ-modules $R[\mathcal{C}_1^\mu][J'] \simeq \Lambda$ and $R[\mathcal{C}_1^{\mathrm{et}}]_0[J'] \simeq J$. Using

13

the above diagram and the fact that W_1 is free over Λ, we conclude that W_1^0 and W_1^1 are free Λ-modules of rank $m+1$. We also conclude that $W_1^0[J] = J_1^\sharp[r]^{\mathrm{sub}}[J', J] = J_1^\sharp[r]^{\mathrm{sub}}[\mathbf{J}]$ and that $W_1^1[J]$ is an extension of R by $J_1^\sharp[r]^{\mathrm{quot}}[\mathbf{J}]$. We know that via the isomorphism $J_0^\sharp[r] \xrightarrow{\sim} J_1^\sharp[r, \mathbf{J}]$, the submodule $\mathrm{Hom}(N, R)$ of $J_0^\sharp[r]$ is identified with $J_1^\sharp[r]^{\mathrm{sub}}[\mathbf{J}]$ (this follows again from [4, Theorem 4.3]). Thus, the submodule $\mathrm{Hom}(N, R)$ of W_0 is identified with $W_1^0[J]$ via τ. This concludes the proof of Theorem 2.1 (iii).

We finally prove Theorem 2.1 (iv). We first consider the Galois action on W_1^0. We begin by proving that W_1^0 is unramified. Let $x \in W_1^0$ and let $\tilde{x}$ be a lift of x to $\mathscr{J}_1^{\sharp, \mathrm{sub}}$, so that $r \cdot \tilde{x} \in \varphi_1(\mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0)$. Let g in the inertia group of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. By Lemma 2.3, $y := g \cdot \tilde{x} - \tilde{x}$ belongs to the the kernel of the reduction map $\rho : (\mathscr{J}_1^\sharp)^0 \to (\mathscr{J}_{1/\mathbf{F}_p}^\sharp)^0(\overline{\mathbf{F}}_p)$. Furthermore, we have $r \cdot y = 0$ since $r \cdot \tilde{x}$ is in $\varphi_1(\mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0) \subset J_1^\sharp(\mathbf{Q})$. Since $\gcd(r, p) = 1$ we get $y = 0$, so W_1^0 is unramified. The proof of [2, Proposition §3.2] shows that $\rho(U_p \cdot \tilde{x} - p \cdot \mathrm{Frob}_p^{-1} \cdot \tilde{x}) = 0$ where $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ is any arithmetic Frobenius. Thus, we have $U_p \cdot \tilde{x} - p \cdot \mathrm{Frob}_p^{-1} \cdot \tilde{x} \in \mathrm{Ker}(\rho)$. Furthermore, we have $r \cdot (U_p \cdot \tilde{x} - p \cdot \mathrm{Frob}_p^{-1} \cdot \tilde{x}) = 0$ since $r \cdot \tilde{x} \in \varphi_1(\mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0)$, U_p acts on $\mathcal{C}_1^{\mathrm{et}}$ by multiplication by p and Frob_p acts trivially on $\varphi_1(\mathbf{Z}[\mathcal{C}_1^{\mathrm{et}}]_0)$. This proves that $U_p \cdot \tilde{x} - p \cdot \mathrm{Frob}_p^{-1} \cdot \tilde{x} \in \mathrm{Ker}(\rho)[r] = 0$, so $U_p \cdot x = p \cdot \mathrm{Frob}_p^{-1} \cdot x = \mathrm{Frob}_p^{-1} \cdot x$ (since $p \equiv 1 \pmod{r}$). We have thus proved that the action of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ on W_1^0 is given by ϕ^{-1}. The fact that the action of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ on W_1^1 is given by $\phi\langle.\rangle^{-1}$ follows from the proof of [2, §3.7 Proposition]. $\qquad \square$

2.3. Conclusion of the proof of Theorem 1.6.

The rest of the proof is now close to the one of de Shalit. We thus sketch the main steps and refer to his papers for further details.

Recall that in $\mathbb{T}$, we have $U_p^2 - 1 = 0$. Since $W_1[J] = W_0$ and W_1 is free over Λ by Theorem 2.1, the endomorphism $\mathbf{U}_p^2 - 1$ of $W_1[J^2]$ induces an element in $\mathrm{Hom}_R(W_1[J^2]/W_1[J], W_1[J])$. The choice of $\log : (\mathbf{Z}/p\mathbf{Z})^\times \to R$ yields a generator $[d] - 1$ of J over Λ, where $d \in \mathbf{F}_p^\times$ is such that $\log(d) = 1$. The multiplication by $[d] - 1$ induces an identification $W_1[J^2]/W_1[J] = W_1[J] = W_0$ since W_1 is free over Λ. Thus $\mathbf{U}_p^2 - 1$ induces an endomorphism of W_0, which we denote by U_p' (thought as the "tame derivative" of $\mathbf{U}_p^2 - 1$). By construction, U_p' commutes with the action of $\mathbb{T}$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. Furthermore, U_p' stabilises W_0^0 and W_0^1 since $\mathbf{U}_p$ stabilises W_1^0 and W_1^1.

The following result (and its proof) is similar to [4, §4.11 Theorem].

Theorem 2.4. *We have $U_p' = \mathscr{L}_R$ in $\mathrm{End}_R(W_0)$.*

14

Proof. Let $M_1 = W_1[J^2]$, $M_1^0 = W_1^0[J^2]$, $M_1^1 = W_1^1[J^2]$ and $\mathbb{T}_1' = (\mathbb{T}_1 \otimes_{\mathbf{Z}} R)/\mathbf{J}^2 \cdot (\mathbb{T}_1 \otimes_{\mathbf{Z}} R)$. We have a commutative diagram of $\mathbb{T}_1'$ and $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-modules

(15)

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & W_0^0 & \longrightarrow & W_0 & \longrightarrow & W_0^1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_1^0 & \longrightarrow & M_1 & \longrightarrow & M_1^1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & W_0^0 & \longrightarrow & W_0 & \longrightarrow & W_0^1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
,
$$

where the first line (resp. the third line) corresponds to the J-invariants (resp. J-coinvariants).

Lemma 2.5. *The natural map* $(\mathbb{T}_1 \otimes_{\mathbf{Z}} R)/\mathbf{J} \cdot (\mathbb{T}_1 \otimes_{\mathbf{Z}} R) \to \mathbb{T} \otimes_{\mathbf{Z}} R$ *is an isomorphism.*

Proof. Note that there is indeed a natural map $\mathbb{T}_1 \to \mathbb{T}$, whose kernel contains the augmentation ideal, given by restriction to $M_2(\Gamma_0) \subset M_2(\Gamma_1)$ (where $M_2(\Gamma_i)$ is the space of modular forms over $\mathbf{Z}$ of weight 2 and level Γ_i). Recall (*cf.* (13)) that we have an isomorphism

(16) $\qquad H_1(X_1, \mathcal{C}_1, R)_+/\mathbf{J} \cdot H_1(X_1, \mathcal{C}_1, R)_+ \xrightarrow{\sim} H_1(X_0, \mathcal{C}_0, R)_+ \, ,$

where the '+' sign means the invariant for the action of the complex conjugation (we use the fact that ℓ is odd).

We claim that $H_1(X_0, \mathcal{C}_0, R)_+$ is free of rank 1 over $\mathbb{T} \otimes_{\mathbf{Z}} R$. Since $\mathbb{T} \otimes_{\mathbf{Z}} R$ is an Artinian ring, it suffices to prove it after localizing at maximal ideals. For non maximal Eisenstein ideals, this is a consequence of [12, Proposition 18.3] since ℓ is odd. For the Eisenstein maximal ideal, this is deduced from Mazur's result in [9, Proposition 4.1].

We thus have a (non-canonical) commutative diagram

$$
\begin{array}{ccc}
\mathbb{T}_1 \otimes_{\mathbf{Z}} R & \xrightarrow{\ f\ } & H_1(X_1, \mathcal{C}_1, R)_+ \\
\downarrow & & \downarrow \\
\mathbb{T} \otimes_{\mathbf{Z}} R & \longrightarrow & H_1(X_0, \mathcal{C}_0, R)_+
\end{array}
$$

where the bottom arrow is an isomorphism and the vertical maps are the natural ones. The map f is surjective modulo $\mathbf{J} \cdot H_1(X_1, \mathcal{C}_1, R)_+$, and hence surjective. Since $\mathbb{T}_1 \otimes_{\mathbf{Z}} R$ and $H_1(X_1, \mathcal{C}_1, R)_+$ are finite groups of the same cardinality, f is an isomorphism. By (16), the kernel of $\mathbb{T}_1 \otimes_{\mathbf{Z}} R \to \mathbb{T}_0 \otimes_{\mathbf{Z}} R$ is $\mathbf{J} \cdot (\mathbb{T}_1 \otimes_{\mathbf{Z}} R)$. $\qquad\square$

Lemma 2.6. *The $\mathbb{T}_1'$-modules M_1^0 and M_1^1 are free of rank 1.*

Proof. By [7, Theorems 0.5 and 1.14], the $\mathbb{T} \otimes_{\mathbf{Z}} R$-modules W_0^0 and W_0^1 are free of rank 1. By Nakayama's lemma, the modules M_1^0 and M_1^1 are cyclic over $\mathbb{T}_1'$. We know by Theorem 2.1 (iii) that M_1^0 and M_1^1 are free Λ/J^2-modules of rank $m + 1$. By Lemma 2.5 and Nakayama's Lemma, $\mathbb{T}_1'$ has $m + 1$ generators as a Λ/J^2. By comparison of cardinalities, M_1^0 and M_1^1 are in fact free over $\mathbb{T}_1'$. $\qquad\square$

Both U_p' and $\mathscr{L}_R$ stabilise $W_0^0 = \mathrm{Hom}(N, R)$ and $W_0^1 = N \otimes_{\mathbf{Z}} R$.

Lemma 2.7. *We have $U_p' = \mathscr{L}_R$ in $\mathrm{End}(W_0^0)$ and $\mathrm{End}(W_0^1)$.*

Proof. The proof is a standard Galois cohomological computation using (15) and Theorem 2.1 (iv). We refer to the proofs of [4, §4.11 and §5.3 Theorem] for the structure of the proof, which is easily adaptable to our situation. In the notation of de Shalit, U_p' corresponds to $-B_p$ (resp. $-C_p$) in $\mathrm{End}(W_0^0)$ (resp. $\mathrm{End}(W_0^1)$). The sign difference corresponds to the fact that de Shalit considers in [4] diamond operators which are dual (equivalently inverse) to our diamond operators (the latter corresponding to the ones of [2]), *cf.* Remarks 2.1 (i). $\qquad\square$

We now conclude the proof of Theorem 2.4. The $\mathbb{T} \otimes_{\mathbf{Z}} R$-modules W_0^0 and W_0^1 are free of rank 1. We can thus find a splitting (as Hecke modules) of (8) and write $W_0 \simeq W_0^0 \oplus W_0^1$. The Hecke operator $\mathscr{L}_R$ preserves this decomposition. By Lemma 2.7, it suffices to show that we can choose this splitting so that it is stable by U_p'. This follows from Lemma 2.6 and the fact that $\mathbf{U}_p^2 - 1$ is in $\mathbb{T}_1'$. $\qquad\square$

By definition of W_0 and by Lemma 2.2, there is a canonical Hecke and Galois equivariant embedding $J_0^\sharp(\overline{\mathbf{Q}}_p)[r] \hookrightarrow W_0$. Since we have fixed embeddings $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$ and $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$, we have canonical identifications of $\mathbb{T}$-modules

$$J_0^\sharp(\overline{\mathbf{Q}}_p)[r] = J_0^\sharp(\overline{\mathbf{Q}})[r] = J_0^\sharp(\mathbf{C})[r] = \mathrm{Symb}_{\Gamma_0}(R) \ .$$

We refer to [4, §2.4 (9)] for the details of how these idenfications work and to [4, §2.5] for the precise definition of the action of $\mathbb{T}$ on $\mathrm{Symb}_{\Gamma_0}(R)$ (in this case, since Hecke operators are self-dual there are no possible confusions anyway). Note that U_p' stabilises $\mathrm{Symb}_{\Gamma_0}(R)$ by Theorem 2.4. To conclude the proof of Theorem 1.6 it suffices to prove the following result, which is in fact an easy consequence of [4, Proposition 3.14].

Theorem 2.8. *For all $\psi \in \mathrm{Symb}_{\Gamma_0}(R)^{U_p=1}$, we have*

$$(17) \qquad (U_p' \cdot \psi)((0) - (\infty)) = \sum_{a=1}^{p-1} \lambda_R(a) \cdot \psi((a/p) - (\infty)) \ .$$

Proof. Following [4, §3.12], let $s : \mathrm{Symb}_{\Gamma_1}(R) \to \mathrm{Symb}_{\Gamma_0}(R)$ be the trace map, corresponding to the projection map $H_1(Y_1, R) \to H_1(Y_0, R)$. We apply [4, Proposition 3.14] with $W^0 = J_1^\sharp(\overline{\mathbf{Q}}_p)[r]$ in the notation of [4, §3.9]. We get that for all $\psi \in s(\mathrm{Symb}_{\Gamma_1}(R))^{U_p=1}$, formula (17) holds. Note that

16

what de Shalit denotes by $-2 \cdot (A_p - 1)$ modulo I^2 is the (matrix of the) restriction of U_p' to $\mathrm{Symb}_{\Gamma_0}(R)^{U_p=1}$ (the minus sign is explained as in the proof of Lemma 2.7).

Note that (17) is trivially satisfied if ψ is fixed by the complex conjugation (*i.e.* for any $a, b \in \mathbf{P}^1(\mathbf{Q})$, we have $\psi((-a) - (-b)) = -\psi((a) - (b))$). Furthermore, we claim that s induces a surjection $\mathrm{Symb}_{\Gamma_1}(R)_- \to \mathrm{Symb}_{\Gamma_0}(R)_-$, where the '$-$' corresponds to the elements on which the complex conjugation acts by -1 *i.e.* to those ψ such that $\psi((a) - (b)) = \psi((-a) - (-b))$. To prove this claim, it suffices to prove that the map $H_1(Y_1, R)_- \to H_1(Y_0, R)_-$ is surjective. This follows from the facts that ℓ is odd, $H_1(Y_i, R) = \Gamma_i^{\mathrm{ab}} \otimes_{\mathbf{Z}} R$ ($i = 0, 1$) and the fact that for any $\gamma \in \Gamma_0$, we have $c(\gamma) \cdot \gamma^{-1} \in \Gamma_1$ where $c(\gamma) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \gamma \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ corresponds to the complex conjugation. This concludes the proof of Theorem 2.8. $\qquad\square$

3. Applications using Mazur's Eisenstein ideal

Keep the notation of §1.5. Fix an integer s such that $1 \leq s \leq t$. We denote by $\mathscr{L}_s$ the image of $\mathscr{L}_R$ in $\mathbb{T} \otimes_{\mathbf{Z}} \mathbf{Z}/\ell^s\mathbf{Z}$.

Let $H := H_1(X_0(p), \mathrm{cusps}, \mathbf{Z}/\ell^s\mathbf{Z})$ be the singular homology of $X_0(p)$ relative to the cusps, with coefficients in $\mathbf{Z}/\ell^s\mathbf{Z}$. Similarly, we denote by H^0 the absolute homology $H_1(X_0(p), \mathbf{Z}/\ell^s\mathbf{Z})$. We denote by H_+ (resp. $(H^0)_+$) the subspace of H (resp. H^0) fixed by the complex conjugation. If α, $\beta \in \mathbf{P}^1(\mathbf{Q})$, we denote by $\{\alpha, \beta\} \in H$ the class of the geodesic path between α and β in the Poincaré upper-half plane.

Recall that we defined a K-theoretic group $\mathcal{K}_s$ just above the statement of Theorem 1.10.

3.1. Some reminder about K-theory.
We briefly summarize the basic K-theory relevant to our work. If E is a field, then by Matsumoto's theorem we have a canonical isomorphism

$$ K_2(E) \simeq E^\times \otimes_{\mathbf{Z}} E^\times / \langle x \otimes y \text{ where } x, y \in E^\times \text{ satisfy } x + y = 1 \rangle . $$

The Steinberg symbol $\{x, y\} \in K_2(E)$ corresponds to the image of $x \otimes y$ in the right hand side of this isomorphism. If E is a number field and $\mathcal{O}_{E,S}$ denotes the ring of S-integers of E for some finite set of primes S, then we have the following localization exact sequence of Quillen:

$$ 0 \to K_2(\mathcal{O}_{E,S}) \to K_2(E) \to \bigoplus_{\mathfrak{p} \notin S} (\mathcal{O}_E/\mathfrak{p})^\times \to 0 $$

where the map $K_2(E) \to (\mathcal{O}_E/\mathfrak{p})^\times$ for a prime $\mathfrak{p} \notin S$ is the so-called *tame symbol*. It sends a Steinberg symbol $\{x, y\}$ to the residue class of $(-1)^{v_{\mathfrak{p}}(x) v_{\mathfrak{p}}(y)} \frac{x^{v_{\mathfrak{p}}(y)}}{y^{v_{\mathfrak{p}}(x)}}$ modulo $\mathfrak{p}$ (here, $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation). It is known that the group $K_2(\mathcal{O}_{E,S})$ is finite.

3.2. **Results concerning the Eisenstein ideal.** In this paragraph, we recall some results concerning the Eisenstein ideal that we will use to prove the theorems stated in §1.5.

By Manin, we have a surjective group homomorphism $\xi : \mathbf{Z}[\Gamma_0 \backslash \mathrm{SL}_2(\mathbf{Z})] \to H$ sending $\Gamma_0 \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $\{\frac{b}{d}, \frac{a}{c}\}$. We identify $\Gamma_0 \backslash \mathrm{SL}_2(\mathbf{Z})$ with $\mathbf{P}^1(\mathbf{Z}/p\mathbf{Z})$, via the map $\Gamma_0 \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto [c : d]$. The subgroup H^0 of H is spanned by the elements $\xi([a : 1])$ with $a \not\equiv 0$ (modulo p). Since $[a : 1]$ corresponds to the coset $\Gamma_0 \cdot \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, the group H^0 is spanned by the elements $\{0, \frac{1}{a}\}$ for $a \in \mathbf{Z}$ coprime to p (this only depends on a modulo p). Let $w_p \in \mathbb{T}$ be the Atkin–Lehner involution (which, in this case, is simply $-U_p$). We have $w_p\{0, \frac{1}{a}\} = \{\infty, -\frac{a}{p}\}$, so H^0 is also spanned by the elements $\{\infty, \frac{a}{p}\}$ for $a \in \mathbf{Z}$ coprime to p. In view of (4), it will be more convenient to work with the latter elements rather than the original Manin symbols.

Theorem 3.1.   (i) *We have $I \cdot H_+ = (H^0)_+$.*

(ii) *(Mazur) There is a group isomorphism $(H^0)_+/I \cdot (H^0)_+ \xrightarrow{\sim} \mathbf{Z}/\ell^s\mathbf{Z}$ sending $\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \lambda_a \cdot \{\infty, \frac{a}{p}\}$ to $\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \lambda_a \cdot \log(a)$ modulo ℓ^s.*

(iii) *(Wang–Lecouturier) There is a group isomorphism $I \cdot (H^0)_+/I^2 \cdot (H^0)_+ \xrightarrow{\sim} J \cdot \mathcal{K}_s/J^2 \cdot \mathcal{K}_s$ sending $\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \lambda_a \cdot \{\infty, \frac{a}{p}\}$ to*

$$\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \lambda_a \cdot \left((1 - \zeta_p^a, 1 - \zeta_p) - \frac{1}{2} \cdot ([\sigma_a] - 1) \cdot (1 - \zeta_p^a, 1 - \zeta_p) \right) ,$$

where $\sigma_a \in \mathrm{Gal}(K/\mathbf{Q})$ is the restriction of the automorphism of $\mathbf{Q}(\zeta_p)$ sending ζ_p to ζ_p^a.

Proof. Point (i) is well-known, but we give a proof for the convenience of the reader. We have an exact sequence of $\mathbb{T}$-modules

$$0 \to H^0 \to H \to (\mathbf{Z}/\ell^s\mathbf{Z})[\mathcal{C}_0]_0 \to 0$$

where $(\mathbf{Z}/\ell^s\mathbf{Z})[\mathcal{C}_0]_0$ is the group of degree zero divisors supported on the cusps $\mathcal{C}_0 = \{\Gamma_0 0, \Gamma_0 \infty\}$. Since I annihilates $(\mathbf{Z}/\ell^s\mathbf{Z})[\mathcal{C}_0]_0$, we have $I \cdot H_+ \subset (H^0)_+$. To prove the equality, it suffices to prove that $H_+/I \cdot H_+ \simeq \mathbf{Z}/\ell^s\mathbf{Z}$. This is a consequence of a result of Mazur, as explained in [9, Proposition 4.1]. Point (ii) follows from [12, Proposition II.18.8]. Point (iii) follows from [11, Theorem 1.12]. $\qquad\square$

The following result, due to Mazur, will be useful.

Proposition 3.2. *Let $U \in \mathbb{T} \otimes_{\mathbf{Z}} \mathbf{Z}/\ell^s\mathbf{Z}$ and $n \in \mathbf{Z}_{\geq 0}$. The following assertions are equivalent.*

(i) $U \in I^n \cdot (\mathbb{T} \otimes_{\mathbf{Z}} \mathbf{Z}/\ell^s\mathbf{Z})$.
(ii) $U \cdot H_+ \subset I^n \cdot H_+$.

Proof. This follows from the fact that H_+ is locally free of rank 1 as a Hecke module localized at the the maximal ideal $I + (\ell)$, a consequence of a result of Mazur (*cf.* [9, Proposition 4.1]). $\qquad\square$

3.3. Study of $\alpha(p, \ell, s)$. We first reformulate Theorem 1.6 using the language of §3.2. There is a perfect bilinear pairing $\bullet : \mathrm{Symb}_{\Gamma_0}(\mathbf{Z}/\ell^s\mathbf{Z}) \times H \to \mathbf{Z}/\ell^s\mathbf{Z}$ given by $\psi \bullet \{\alpha, \beta\} = \psi((\alpha) - (\beta))$. This pairing is $\mathbb{T}$-equivariant, meaning that for all $T \in \mathbb{T}$, $\psi \in \mathrm{Symb}_{\Gamma_0}(\mathbf{Z}/\ell^s\mathbf{Z})$ and $x \in H$ we have $(T \cdot \psi) \bullet x = \psi \bullet (T \cdot x)$ (in general the pairing exchanges T with its dual T^*, but in level Γ_0 we have $T = T^*$).

Theorem 1.6 modulo ℓ^s is equivalent to the single equality in H_+:

$$(18) \qquad \mathscr{L}_s \cdot \{0, \infty\} = \frac{1}{2} \cdot (U_p + 1) \cdot \sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \log(a) \cdot \{\frac{a}{p}, \infty\}$$

The factor $\frac{1}{2} \cdot (U_p + 1)$ is to take into account the fact that Theorem 1.6 is restricted to those ψ fixed by U_p (recall that $U_p = -w_p$ so $U_p\{0, \infty\} = -w_p\{0, \infty\} = -\{\infty, 0\} = \{0, \infty\}$).

We now prove Theorem 1.8. Notice that the right hand side of (18) lies in $(H^0)_+$. By Proposition 3.2 and Theorem 3.1 (i), we have $\mathscr{L}_s \in I \cdot (\mathbb{T} \otimes_{\mathbf{Z}} \mathbf{Z}/\ell^s\mathbf{Z})$. To prove that we have $\mathscr{L}_s \in I^2 \cdot (\mathbb{T} \otimes_{\mathbf{Z}} \mathbf{Z}/\ell^s\mathbf{Z})$, it suffices to prove that we have $\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \log(a) \cdot \{\frac{a}{p}, \infty\} \in I \cdot (H^0)_+$. This follows from Theorem 3.1 (ii) and the fact that $\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \log(a)^2 \equiv 0$ (modulo ℓ^s).

We now prove Theorem 1.10. By (18), Theorem 3.1 (i) and Proposition 3.2, we have $\alpha(p, \ell, s) \geq 3$ if and only if

$$\frac{1}{2} \cdot (U_p + 1) \cdot \sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \log(a) \cdot \{\frac{a}{p}, \infty\} \in I^2 \cdot (H^0)_+ \ .$$

Since ℓ is odd and $U_p - 1 \in \cap_{n \geq 0} I^n$, we have $\alpha(p, \ell, s) \geq 3$ if and only if

$$\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \log(a) \cdot \{\frac{a}{p}, \infty\} \in I^2 \cdot (H^0)_+ \ .$$

By Theorem 3.1 (iii), this is equivalent to saying that

$$\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \log(a) \cdot \left((1 - \zeta_p^a, 1 - \zeta_p) - \frac{1}{2} \cdot ([\sigma_a] - 1) \cdot (1 - \zeta_p^a, 1 - \zeta_p) \right)$$

$$\in J^2 \cdot \mathcal{K}_s \ .$$

To conclude the proof of Theorem 1.10, it suffices to prove that

$$\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \log(a) \cdot ([\sigma_a] - 1) \cdot (1 - \zeta_p^a, 1 - \zeta_p) \in J^2 \cdot \mathcal{K}_s \ ,$$

or equivalently, since $[\sigma_a] - 1 \equiv \log(a) \cdot ([\sigma_d] - 1)$ modulo J^2 (where $\log(d) = 1$), that

$$\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \log(a)^2 \cdot (1 - \zeta_p^a, 1 - \zeta_p) \in J \cdot \mathcal{K}_s \ .$$

By Remarks 1.2 (i), this is equivalent to $\sum_{a \in (\mathbf{Z}/p\mathbf{Z})^\times} \log(a)^3 \equiv 0$ (modulo ℓ^s), which is true since $\ell \geq 5$.

3.4. **The tree formula.** This this last paragraph, we prove Theorem 1.9. We recall the main result of [3], that are essential to our proof. Recall that by definition, $\mathscr{L}_R$ is an endomorphism of $N \otimes_{\mathbf{Z}} R$. Joseph Oesterlé conjectured an explicit formula for this endomorphism, and de Shalit proved this conjecture in [3] (up to a sign, which is unimportant here since ℓ is odd). The formula is as follows (*cf.* [3, §1.6 Main thm]).

For any $E \in S$, we have in $N \otimes_{\mathbf{Z}} R$:

$$(19) \qquad \mathscr{L}_R([E]) = \sum_{\substack{E' \in S \\ E' \neq E}} \frac{1}{w_{E'}} \cdot \log((j(E') - j(E))^{p+1}) \cdot ([E'] - [E]) \ ,$$

where $j(E)$ is the j-invariant of E. Recall that $j(E)$ is in $\mathbf{F}_{p^2}$, so $(j(E') - j(E))^{p+1}$ belongs to $\mathbf{F}_p^\times$ and we can apply log to it. The image of $\mathscr{L}_R$ is visibly contained in $N_0 \otimes_{\mathbf{Z}} R$, which is another way to prove that $\mathscr{L}_R \in I \cdot (\mathbb{T} \otimes_{\mathbf{Z}} R)$.

Using results of Mazur and Emerton, one can show that the fact that $\alpha(p, \ell, t) \geq 2$ implies that the kernel of $\mathscr{L}_R$ (in $N \otimes_{\mathbf{Z}} R$) contains a free R-module of rank 2. More precisely, $\mathrm{Ker}(\mathscr{L}_R)$ contains $R \cdot e_0 \oplus R \cdot e_1$ where e_0 and e_1 are the first two *higher Eisenstein elements* in $N \otimes_{\mathbf{Z}} R$ defined in [9, §3.1]. We have an explicit elementary formula for e_1 [9, Theorem 1.6], which gives $m + 1$ quadratic identities in log of difference of supersingular j-invariants, where $m = \mathrm{genus}(X_0)$. We leave to the interested reader the task to write down the formulas, since we focus instead on the single formula (6).

Fix an ordering $(E_0, ..., E_m)$ of S and denote by M the matrix of $\mathscr{L}_R$ in the R-basis $([E_0], ..., [E_m])$ of $N \otimes_{\mathbf{Z}} R$. Note that M is symmetric if $p \equiv 1$ (modulo 12), which we assume from now on. We have seen that $\mathrm{Ker}(M)$ contains a sub-R-module isomorphic to R^2. We can thus apply the following fact (whose proof is easy and left to the reader).

Lemma 3.3. *Let q be a prime power and M be a square matrix with coefficients in $\mathbf{Z}/q\mathbf{Z}$ whose kernel contains a submodule isomorphic to $(\mathbf{Z}/q\mathbf{Z})^2$. Then all the first minors of M are equal to 0.*

To conclude the proof of Theorem 1.9, it suffices to prove that the left-hand side of (6) is (up to sign) the determinant of a first minor of M. This is a direct consequence of the weighted matrix-tree theorem (*cf.* for instance [1, Theorem 1]) applied to the complete graph whose vertices are elements of S and whose weight on the edge linking E and E' is $\log((j(E') - j(E))^{p+1})$. Note that we have used the fact that M is symmetric and that the sum of each column is zero, which is why we assumed $p \equiv 1$ (modulo 12).

REFERENCES

[1] Yurii Burman and Boris Shapiro. Around matrix-tree theorem. *Math. Res. Lett.*, 13(5-6):761–774, 2006.

[2] Ehud de Shalit. On certain Galois representations related to the modular curve $X_1(p)$. *Compositio Math.*, 95(1):69–100, 1995.

[3] Ehud de Shalit. On the p-adic periods of $X_0(p)$. *Math. Ann.*, 303(3):457–472, 1995.

[4] Ehud de Shalit. p-adic periods and modular symbols of elliptic curves of prime conductor. *Invent. Math.*, 121(2):225–255, 1995.

[5] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349, 1973.

[6] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[7] Matthew Emerton. Supersingular elliptic curves, theta series and weight two modular forms. *J. Amer. Math. Soc.*, 15(3):671–714, 2002.

[8] Ralph Greenberg and Glenn Stevens. p-adic L-functions and p-adic periods of modular forms. *Invent. Math.*, 111(2):407–447, 1993.

[9] Emmanuel Lecouturier. Higher Eisenstein elements, higher Eichler formulas and rank of Hecke algebras. *Invent. Math.*, 223(2):485–595, 2021.

[10] Emmanuel Lecouturier. Mixed modular symbols and the generalized cuspidal 1-motive. *Trans. Amer. Math. Soc.*, 374(4):2823–2872, 2021.

[11] Emmanuel Lecouturier and Jun Wang. On a Conjecture of Sharifi and Mazur's Eisenstein Ideal. *International Mathematics Research Notices*, 06 2020. DOI:10.1093/imrn/rnaa115.

[12] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[13] B. Mazur and J. Tate. Refined conjectures of the "Birch and Swinnerton-Dyer type". *Duke Math. J.*, 54(2):711–750, 1987.

[14] Loïc Merel. L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$. *J. Reine Angew. Math.*, 477:71–115, 1996.