©2013 The Mathematical Society of Japan
J. Math. Soc. Japan
Vol. 65, No. 3 (2013) pp. 733–772
doi: 10.2969/jmsj/06530733

Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties

By Masami Ohta

(Received Nov. 6, 2011)

Abstract. Let $N \geq 5$ be a prime number. Conrad, Edixhoven and Stein have conjectured that the rational torsion subgroup of the modular Jacobian variety $J_1(N)$ coincides with the 0-cuspidal class group. We prove this conjecture up to 2-torsion. To do this, we study certain ideals of the Hecke algebras, called the Eisenstein ideals, related to modular forms of weight 2 with respect to $\Gamma_1(N)$ that vanish at the 0-cusps.

Introduction.

In this paper, we fix a *prime number* $N \geq 5$.

Let $X_0(N)$ be the canonical model over $\mathbb{Q}$ of the modular curve attached to the congruence subgroup $\Gamma_0(N) = \left\{ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right] \in SL_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \pmod{N} \right\}$. It has two cusps, usually called ∞ and 0, both of which are rational over $\mathbb{Q}$. Let $J_0(N)$ be the Jacobian variety of $X_0(N)$ defined over $\mathbb{Q}$. Ogg has shown that the divisor class $\mathrm{cl}((0)-(\infty))$ of $(0)-(\infty)$ in $J_0(N)(\mathbb{Q})$ generates a group of order $n :=$ (the numerator of $(N-1)/12$) in [**Og1**], and conjectured that this is the full rational torsion subgroup $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ in [**Og2**]:

$$J_0(N)(\mathbb{Q})_{\mathrm{tors}} = \langle \mathrm{cl}((0)-(\infty)) \rangle \cong \mathbb{Z}/n\mathbb{Z}.$$

Mazur then proved, among others, that this is indeed the case, in his celebrated paper [**Ma**].

On the other hand, we have the modular curve attached to another congruence subgroup $\Gamma_1(N) = \left\{ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right] \in \Gamma_0(N) \,\middle|\, a \equiv d \equiv 1 \pmod{N} \right\}$. There are two natural choices of its model over $\mathbb{Q}$. We denote by $X_1(N)$ the one of which the 0-cusps (i.e. the cusps lying over $0 \in X_0(N)(\mathbb{Q})$) are rational over $\mathbb{Q}$, and by $J_1(N)$ its Jacobian variety defined over $\mathbb{Q}$. Let $\mathcal{C}_0$ be the subgroup of $J_1(N)(\mathbb{Q})_{\mathrm{tors}}$ consisting of the classes of divisors of degree zero supported at the 0-cusps. Klimek has computed the order of this group, which is given by

2010 *Mathematics Subject Classification.* Primary 11G18, 14G35; Secondary 11F11, 14G05.
Key Words and Phrases. modular Jacobian variety, rational torsion subgroup, Eisenstein ideal.

$$N\prod_{\chi}\frac{B_{2,\chi}}{4}=:c(N)$$

where the product ranges over all nontrivial even Dirichlet characters modulo N, and $B_{2,\chi}$ is the second generalized Bernoulli number (cf. Kubert and Lang [**KL**]). As for the rational torsion subgroup of $J_1(N)$, Conrad, Edixhoven and Stein have presented the following conjecture, together with numerical evidence:

CONJECTURE ([**CES**, Conjecture 6.2.2]). The rational torsion subgroup $J_1(N)(\mathbb{Q})_{\mathrm{tors}}$ coincides with the 0-cuspidal class group $\mathcal{C}_0$:

$$J_1(N)(\mathbb{Q})_{\mathrm{tors}}=\mathcal{C}_0.$$

In this direction, Kamienny [**Kam3**] proved that, if a prime $p\geq 5$ divides the order of $A(\mathbb{Q})_{\mathrm{tors}}$, where A is the quotient variety of $J_1(N)$ by the image of $J_0(N)$, then p is a divisor of $c(N)$. One of our main results of this paper is the following

THEOREM I. *The above conjecture of Conrad, Edixhoven and Stein is valid up to 2-torsion. Namely, for any odd prime p,*

$$J_1(N)(\mathbb{Q})[p^\infty]=\mathcal{C}_0[p^\infty]$$

where the symbol "$[p^\infty]$" indicates the p-torsion subgroup.

Let $h_2(\Gamma_1(N);\mathbb{Z})$ be the Hecke algebra generated over $\mathbb{Z}$ by the diamond operators $\langle a\rangle$ and the Hecke operators $T(n)$ acting on the space $S_2(\Gamma_1(N);\mathbb{C})$ of cusp forms of weight 2 with respect to $\Gamma_1(N)$. It can be considered as a subalgebra of $\mathrm{End}_{\mathbb{Q}}(J_1(N))$ in a natural way. To study the rational torsion subgroup of $J_1(N)$, we are led, by [**Ma**], to seek an ideal, called the *Eisenstein ideal* $I_{\infty,\mathbb{Z}}$ of $h_2(\Gamma_1(N);\mathbb{Z})$ which enjoys the properties stated in the following Theorem II. To define "correct" $I_{\infty,\mathbb{Z}}$ and study it, we are then led to consider the space, denoted $M_2^\infty(\Gamma_1(N);R)$, of modular forms over a ring R which vanish at the 0-cusps (equivalently, whose corresponding differentials have poles only at the ∞-cusps, the cusps lying over $\infty\in X_0(N)(\mathbb{Q})$). Let $H_2^\infty(\Gamma_1(N);\mathbb{Z})$ be the Hecke algebra associated with $M_2^\infty(\Gamma_1(N);\mathbb{C})$ in the same sense as above. We define $\mathcal{I}_{\infty,\mathbb{Z}}$ (resp. $I_{\infty,\mathbb{Z}}$) as the ideal of $H_2^\infty(\Gamma_1(N);\mathbb{Z})$ (resp. $h_2(\Gamma_1(N);\mathbb{Z})$) generated by $T(l)-(1+l\langle l\rangle)$ with prime numbers $l\neq N$, $T(N)-1$ *together with* $\tau=\sum\langle a\rangle$ (the sum being over $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$). The (not necessarily proper) ideal $I_{\infty,\mathbb{Z}}$ is the image of $\mathcal{I}_{\infty,\mathbb{Z}}$ under the canonical surjective homomorphism $H_2^\infty(\Gamma_1(N);\mathbb{Z})\to h_2(\Gamma_1(N);\mathbb{Z})$, and $\mathcal{I}_{\infty,\mathbb{Z}}$ turns out to be the annihilator ideal of the space of Eisenstein series in $M_2^\infty(\Gamma_1(N);\mathbb{C})$, which, hopefully, justifies our terminology. Set

$$\begin{cases} h_2(\Gamma_1(N);\mathbb{Z}_p) := h_2(\Gamma_1(N);\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p, \\ I_{\infty,\mathbb{Z}_p} := I_{\infty,\mathbb{Z}} \cdot h_2(\Gamma_1(N);\mathbb{Z}_p) \end{cases}$$

for a prime number p.

THEOREM II. *Let p be an odd prime.*

(1) *We have the equality of indices*:

$$|h_2(\Gamma_1(N);\mathbb{Z}_p) : I_{\infty,\mathbb{Z}_p}| = |\mathbb{Z}_p : c(N)\mathbb{Z}_p|.$$

(2) *$I_{\infty,\mathbb{Z}_p}$ annihilates $J_1(N)(\mathbb{Q})[p^\infty]$.*

This Theorem II is the key to the proof of Theorem I. But for the prime N, we need some finer arguments, decomposing the above objects with respect to the action of $(\mathbb{Z}/N\mathbb{Z})^\times$. In this case, the situation is different from the other cases in that $J_0(N)$ does not have good reduction at N (but A above attains everywhere good reduction over $\mathbb{Q}(\zeta_N)$), and there is an extra factor N in the definition of $c(N)$, etc. However, there is no N-torsion in $J_0(N)(\mathbb{Q})$ by [**Ma**], and the N-division points of A have been studied rather extensively, mainly in connection with the theory of cyclotomic fields, by Ribet [**Ri**], Wiles [**Wi**], Mazur and Wiles [**MW1**], [**MW2**], Kamienny [**Kam2**], [**Oh1**], [**Oh2**] and others. We give the proofs of Theorems I and II for the prime N separately in the subsection 3.3, employing some of these works. We note that these works also guided us in studying the other p-torsion parts.

In the rest of this introduction, we thus explain our plan mainly in the case where $p \neq 2, N$ in mind.

Section 1 is preliminary. In 1.1, we recall known facts on modular forms and cusp forms of weight 2 with respect to $\Gamma_1(N)$, introduce $M_2^\infty(\Gamma_1(N);R)$, and show that this latter space has the usual properties such as the base changing property and the q-expansion principle. (In Sections 1 and 2, we use another model $X_\mu(N)$ of the modular curve which is suited to consider the q-expansions.) In 1.2, we consider the Hecke algebras acting on these spaces, and recall some properties of $h_2(\Gamma_1(N);\mathbb{Z})$ viewed as an endomorphism subalgebra of the Jacobian variety $J_\mu(N)$ of $X_\mu(N)$. In 1.3, we prove the duality between $M_2^\infty(\Gamma_1(N);R)$ and its Hecke algebra $H_2^\infty(\Gamma_1(N);R)$ when N is invertible in R, which is an analogue of the well-known duality in the case of cusp forms. This duality plays an important role in the proof of Theorem II, (1).

In Section 2, we first recall Eisenstein series of weight 2 with respect to $\Gamma_1(N)$, and introduce our Eisenstein ideals in 2.1. We show that one can exclude $T(N)-1$ from the list of generators of $I_{\infty,\mathbb{Z}_p}$ when $p \neq N$, which helps us in proving Theorem

II, (2). The rest of Section 2 is devoted to the proof of Theorem II, (1) for $p \neq 2, N$. For this, we use the method of [**Oh1**] and [**Oh2**], in which ordinary Λ-adic situation was studied. In 2.2, we study the "residue mapping" for $M_2^{\infty}(\Gamma_1(N); R)$ for later use. In 2.3, we prove a result on the behavior of congruence modules under duality. These results, together with the duality proved in 1.3, allow us to interpret the index in question as the order of certain congruence module, which is much easier to compute. We then accomplish the actual computation in 2.4.

In Section 3, we at length start the study of $J_1(N)(\mathbb{Q})_{\mathrm{tors}}$. In 3.1, we prove Theorem II, (2) for $p \neq 2, N$. Among the generators of $I_{\infty,\mathbb{Z}_p}$, the annhilation of $J_1(N)(\mathbb{Q})[p^{\infty}]$ by $T(l)-(1+l\langle l\rangle)$ $(l \neq N)$ is a rather well-known consequence of the Eichler-Shimura congruence relation and a result of Raynaud [**Ra**]. The point here is the annihilation by τ for which we invoke results of [**CES**] and [**Ma**] (whereas for $J_1(N)(\mathbb{Q})[N^{\infty}]$, we need an effort to prove the annihilation by $T(N)-1$ in 3.3). We finish the proof of Theorem I for $p \neq 2, N$ using the method of [**Wi**] and [**MW1**] in 3.2. Finally in 3.4, we derive the results on $J_{\mu}(N)(\mathbb{Q})_{\mathrm{tors}}$ corresponding to Theorems I and II from them.

1. Modular forms and Hecke algebras.

1.1. Modular forms.

Throughout the paper, we fix a *prime number* $N \geq 5$.

In this section, we consider modular forms of weight 2 and level N. We are especially interested in the space $M_2^{\infty}(\Gamma_1(N); R)$ below, and the associated Hecke algebras. Our purpose here is to recall known facts and to see that these objects have usual good properties as in the case of cusp forms or modular forms. Basic references are Deligne and Rapoport [**DR**], Katz [**Kat1**], [**Kat2**], Katz and Mazur [**KM**] and Shimura [**Sh**]; cf. also Diamond and Im [**DI**] and Gross [**G**] which contain good summary of the algebraic theory of modular forms with respect to $\Gamma_1(N)$.

Let R be a $\mathbb{Z}[1/N]$-algebra. We denote by $X_{\mu}(N)_{/R}$ the (fine) moduli scheme classifying the pairs (E, α) consisting of

$$\begin{cases} \text{a generalized elliptic curve } E \text{ over an } R\text{-scheme } S, \text{ and} \\ \text{a closed immersion } \alpha : \boldsymbol{\mu}_N \hookrightarrow E^{\mathrm{reg}} \text{ of } S\text{-group schemes.} \end{cases} \tag{1.1.1}$$

Here, E^{reg} denotes the smooth locus of E/S, and we require that the image of α meets every geometric irreducible component of E/S. $X_{\mu}(N)_{/R}$ is a proper, smooth and geometrically irreducible curve over R.

There is the universal family

$$\pi : \mathcal{E} \to X_\mu(N)_{/R} \text{ together with } \boldsymbol{\mu}_N \hookrightarrow \mathcal{E}^{\mathrm{reg}} \tag{1.1.2}$$

of the pair (1.1.1). We set

$$\underline{\omega}_{/R} := \underline{\mathrm{Lie}}(\mathcal{E}^{\mathrm{reg}})^\vee \tag{1.1.3}$$

the dual of the sheaf of Lie algebras. If $Y_\mu(N)_{/R}$ denotes the open subscheme of $X_\mu(N)_{/R}$ which classifies the pairs (E, α) with E a genuine elliptic curve, the restriction of $\underline{\omega}_{/R}$ to $Y_\mu(N)_{/R}$ is isomorphic to $\pi_*(\Omega^1_{\mathcal{E}/Y_\mu(N)_{/R}})$. (See [**G**, Section 2] for these.)

Let

$$C_{/R} := X_\mu(N)_{/R} - Y_\mu(N)_{/R} \tag{1.1.4}$$

considered as a reduced closed subscheme of $X_\mu(N)_{/R}$, be the scheme of cusps of $X_\mu(N)_{/R}$. It is finite and étale over R.

Let $X_0(N)_{/R}$ be the (coarse) moduli scheme classifying generalized elliptic curves together with a locally free subgroup scheme of rank N in place of α above. Its subscheme of cusps is a disjoint union of two copies of $\mathrm{Spec}(R)$, usually called ∞ and 0 (cf. [**DI**, Example 9.3.4] for their descriptions in terms of Tate curves). We denote by $C_{\infty/R}$ and $C_{0/R}$ their inverse images by the natural morphism $X_\mu(N)_{/R} \to X_0(N)_{/R}$. Thus

$$C_{/R} = C_{\infty/R} \coprod C_{0/R}. \tag{1.1.5}$$

$C_{\infty/\mathbb{Z}[1/N]}$ is isomorphic to the disjoint sum of $(N-1)/2$ copies of $\mathrm{Spec}(\mathbb{Z}[1/N])$, while $C_{0/\mathbb{Z}[1/N]}$ is isomorphic to $\mathrm{Spec}(\mathbb{Z}[\zeta_N]^+[1/N])$. Here, $\zeta_N \in \overline{\mathbb{Q}}$ is a primitive N-th root of unity, and $\mathbb{Z}[\zeta_N]^+$ is the ring of integers of the maximal real subfield of $\mathbb{Q}(\zeta_N)$. Points of $C_{\infty/R}$ or $C_{0/R}$ (with values in R-algebras) will be called ∞-cusps or 0-cusps, respectively. We may consider $C_{/R}$, $C_{\infty/R}$ and $C_{0/R}$ as effective Cartier divisors in $X_\mu(N)_{/R}$.

Recall that there is the Kodaira-Spencer isomorphism

$$\underline{\omega}^{\otimes 2}_{/R} \cong \Omega^1_{/R}(C_{/R}) \quad \text{with} \quad \Omega^1_{/R} := \Omega^1_{X_\mu(N)_{/R}/R}. \tag{1.1.6}$$

Definition 1.1.7. For a $\mathbb{Z}[1/N]$-algebra R, we set

$$\begin{cases} S_2(\Gamma_1(N);R) := H^0\big(X_\mu(N)_{/R}, \underline{\omega}^{\otimes 2}_{/R}(-C_{/R})\big) \cong H^0\big(X_\mu(N)_{/R}, \Omega^1_{/R}\big), \\ M_2^\infty(\Gamma_1(N);R) := H^0\big(X_\mu(N)_{/R}, \underline{\omega}^{\otimes 2}_{/R}(-C_{0/R})\big) \cong H^0\big(X_\mu(N)_{/R}, \Omega^1_{/R}(C_{\infty/R})\big), \\ M_2(\Gamma_1(N);R) := H^0\big(X_\mu(N)_{/R}, \underline{\omega}^{\otimes 2}_{/R}\big) \cong H^0\big(X_\mu(N)_{/R}, \Omega^1_{/R}(C_{/R})\big). \end{cases}$$

If f is an element of one of the spaces in the left hand side, we denote by ω_f the corresponding differential in the right hand side.

$S_2(\Gamma_1(N);R)$ and $M_2(\Gamma_1(N);R)$ are of course the spaces of cusp forms and modular forms in the usual sense, and $M_2^\infty(\Gamma_1(N);R)$ lies between them:

$$S_2(\Gamma_1(N);R) \subseteq M_2^\infty(\Gamma_1(N);R) \subseteq M_2(\Gamma_1(N);R).$$

PROPOSITION 1.1.8. *The formation of the above spaces commutes with change of base rings. Namely for any $\mathbb{Z}[1/N]$-algebra R, we have canonical isomorphisms*

$$\begin{cases} S_2(\Gamma_1(N);\mathbb{Z}[1/N]) \otimes_{\mathbb{Z}[1/N]} R \cong S_2(\Gamma_1(N);R), \\ M_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N]) \otimes_{\mathbb{Z}[1/N]} R \cong M_2^\infty(\Gamma_1(N);R), \\ M_2(\Gamma_1(N);\mathbb{Z}[1/N]) \otimes_{\mathbb{Z}[1/N]} R \cong M_2(\Gamma_1(N);R). \end{cases}$$

PROOF. The first and the third isomorphisms are well-known (cf. [**DI**, Theorem 12.3.2]), and the second one can be obtained in a similar manner, as follows. Set $S = \mathrm{Spec}(\mathbb{Z}[1/N])$, $X = X_\mu(N)_{/\mathbb{Z}[1/N]}$ and $C_\infty = C_{\infty/\mathbb{Z}[1/N]}$, and let $f : X \to S$ be the structural morphism. In view of [**EGAIII**, (7.7.5) and (7.8.5)], it is enough to show that $R^1 f_*(\Omega^1_{/\mathbb{Z}[1/N]}(C_\infty))$ is a locally free $\mathcal{O}_S$-module. For a point $s \in S$, indicate by the subscript "$_s$" the base change to the residue field $\kappa(s)$ at s. Then we see that $H^1(X_s, \Omega^1_{/\mathbb{Z}[1/N]}(C_\infty)_s)$ vanishes for each s since it is Serre dual to $H^0(X_s, \mathcal{O}_{X_s}(-C_{\infty/\kappa(s)}))$. It follows from Mumford [**Mu**, II, 5, Corollary 2] that we in fact have $R^1 f_*(\Omega^1_{/\mathbb{Z}[1/N]}(C_\infty)) = 0$. □

We have the q-expansion mappings (at the cusp ∞ of $X_\mu(N)_{/R}$)

$$\begin{cases} S_2(\Gamma_1(N);R) \to qR[[q]], \\ M_2^\infty(\Gamma_1(N);R) \to R[[q]], \\ M_2(\Gamma_1(N);R) \to R[[q]] \end{cases} \tag{1.1.9}$$

(cf. [**G**, Section 2]). The image under any one of the above mappings of f is denoted by $f(q)$, and called the q-expansion of f. The differential ω_f corresponding to f

then has the expansion $f(q)dq/q$ around the cusp ∞. We have the following q-expansion principle:

PROPOSITION 1.1.10. (1) *The above q-expansion mappings are injective.*
(2) *If R_0 is a $\mathbb{Z}[1/N]$-subalgebra of R, an element f in one of the spaces in the left hand side of* (1.1.9) *is defined over R_0 if and only if $f(q)$ belongs to $R_0[[q]]$.*

PROOF. For $M_2(\Gamma_1(N);R)$, this is [**G**, Proposition 2.7], and the same holds for its subspaces $M_2^\infty(\Gamma_1(N);R)$ and $S_2(\Gamma_1(N);R)$. Indeed, for any $\mathbb{Z}[1/N]$-module K, we can define

$$M_2(\Gamma_1(N);K) := H^0\Big(X_\mu(N)_{/\mathbb{Z}[1/N]}, \underline{\omega}^{\otimes 2}_{/\mathbb{Z}[1/N]} \otimes_{\mathbb{Z}[1/N]} K\Big)$$

and similarly $M_2^\infty(\Gamma_1(N);K)$ and $S_2(\Gamma_1(N);K)$, which coincide with the previous ones when K is a $\mathbb{Z}[1/N]$-algebra. The first assertion for $M_2(\Gamma_1(N);R)$ implies the injectivity of the q-expansion mapping $M_2(\Gamma_1(N);K) \to K[[q]]$, and hence the same holds for the subspaces $M_2^\infty(\Gamma_1(N);K)$ and $S_2(\Gamma_1(N);K)$ of $M_2(\Gamma_1(N);K)$. The second assertion then follows from this (cf. [**Kat1**, 1.6]). □

It follows from this that $M_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N])$ is the submodule of $M_2^\infty(\Gamma_1(N);\mathbb{C})$ consisting of forms that have q-expansions in $\mathbb{Z}[1/N][[q]]$, and similarly for $S_2(\Gamma_1(N);\mathbb{Z}[1/N])$ and $M_2(\Gamma_1(N);\mathbb{Z}[1/N])$. Now set

$$\begin{cases} S_2(\Gamma_1(N);\mathbb{Z}) := \{f \in S_2(\Gamma_1(N);\mathbb{Z}[1/N]) \mid f(q) \in q\mathbb{Z}[[q]]\}, \\ M_2^\infty(\Gamma_1(N);\mathbb{Z}) := \{f \in M_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N]) \mid f(q) \in \mathbb{Z}[[q]]\}, \\ M_2(\Gamma_1(N);\mathbb{Z}) := \{f \in M_2(\Gamma_1(N);\mathbb{Z}[1/N]) \mid f(q) \in \mathbb{Z}[[q]]\} \end{cases} \tag{1.1.11}$$

(see [**DI**, Theorem 12.3.7] for geometric descriptions). Then we see from the remark above that

$$\begin{cases} S_2(\Gamma_1(N);\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}[1/N] = S_2(\Gamma_1(N);\mathbb{Z}[1/N]), \\ M_2^\infty(\Gamma_1(N);\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}[1/N] = M_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N]), \\ M_2(\Gamma_1(N);\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}[1/N] = M_2(\Gamma_1(N);\mathbb{Z}[1/N]) \end{cases} \tag{1.1.12}$$

since the coefficients of the q-expansion of every element in the right hand side have bounded denominators. For *any* ring R, we set

$$\begin{cases} S_2(\Gamma_1(N);R) := S_2(\Gamma_1(N);\mathbb{Z}) \otimes_{\mathbb{Z}} R, \\ M_2^{\infty}(\Gamma_1(N);R) := M_2^{\infty}(\Gamma_1(N);\mathbb{Z}) \otimes_{\mathbb{Z}} R, \\ M_2(\Gamma_1(N);R) := M_2(\Gamma_1(N);\mathbb{Z}) \otimes_{\mathbb{Z}} R. \end{cases} \tag{1.1.13}$$

In view of Proposition 1.1.8 and (1.1.12), this notation coincides with the previous one when R is a $\mathbb{Z}[1/N]$-algebra. The formation of these spaces clearly commutes with arbitrary change of base rings.

1.2. Hecke operators.

For the moment, we again work over a $\mathbb{Z}[1/N]$-algebra R. Set

$$G := (\mathbb{Z}/N\mathbb{Z})^{\times}/\{\pm 1\}. \tag{1.2.1}$$

For each $a \in G$, we have an automorphism $\langle a \rangle$ of $X_{\mu}(N)_{/R}$ over $X_0(N)_{/R}$, which sends an S-valued point (corresponding to the pair) (E, α) as in (1.1.1) to $(E, a\alpha)$. $X_{\mu}(N)_{/R}$ is a Galois covering of $X_0(N)_{/R}$ whose Galois group is isomorphic to G via $\langle - \rangle$.

On the other hand, we have the Hecke correspondence on $X_{\mu}(N)_{/R}$, for each prime number l (cf. [**G**, Section 3]): We denote by $X_{\mu}(N;l)_{/R}$ the moduli scheme which classifies the triples (E, α, C), where (E, α) is the same as in (1.1.1), and C is a locally free subgroup scheme of E^{reg} of rank l. Here we require that (image of α) $\times$ C meets every geometric irreducible component of E/S; and moreover that (image of α) $\cap$ C is trivial when $l = N$. We then have two morphisms

$$\begin{cases} \pi_1 : X_{\mu}(N;l)_{/R} \to X_{\mu}(N)_{/R}, \\ \pi_2 : X_{\mu}(N;l)_{/R} \to X_{\mu}(N)_{/R} \end{cases} \tag{1.2.2}$$

which are uniquely determined by the following rules for points of $Y_{\mu}(N)_{/R}$, i.e. with genuine elliptic curves E,

$$\begin{cases} \pi_1(E, \alpha, C) = (E, \alpha), \\ \pi_2(E, \alpha, C) = (E/C, \alpha') \end{cases} \tag{1.2.3}$$

where α' is the composite of α and the quotient morphism $E \to E/C$.

Actually, we need such correspondences only over $\mathbb{Q}$. When f is in one of the spaces $S_2(\Gamma_1(N);\mathbb{Q})$, $M_2^{\infty}(\Gamma_1(N);\mathbb{Q})$ or $M_2(\Gamma_1(N);\mathbb{Q})$, and ω_f is the corresponding differential on $X_{\mu}(N)_{/\mathbb{Q}}$, we can define the endomorphisms $\langle a \rangle$ and $T(l)$ of the above spaces by the formulas

$$\begin{cases} \omega_{f|\langle a\rangle} = \omega_f \mid \langle a\rangle := \langle a\rangle^*(\omega_f), \\ \omega_{f|T(l)} = \omega_f \mid T(l) := \pi_{1*} \circ \pi_2^*(\omega_f) \end{cases} \tag{1.2.4}$$

where the superscript "*" and the subscript "$_*$" mean the pullback and the trace of differentials, respectively. This is well-known for $S_2(\Gamma_1(N);\mathbb{Q})$ and $M_2(\Gamma_1(N);\mathbb{Q})$. As for $M_2^\infty(\Gamma_1(N);\mathbb{Q})$, in 2.1 below, we will explicitly describe the Eisenstein series belonging to $M_2^\infty(\Gamma_1(N);\mathbb{C})$ and show that this latter space has a basis consisting of Hecke eigenforms. The subspace $M_2^\infty(\Gamma_1(N);\mathbb{Q})$ of $M_2(\Gamma_1(N);\mathbb{Q})$ is thus stable under $\langle a\rangle$ and $T(l)$. Then it is known that these operators preserve the subspaces in (1.1.11) ([**DI**, Propositions 12.3.11 and 12.4.1]), and hence induce endomorphisms of the spaces in (1.1.13) for arbitrary R. All these operators will be denoted by the same symbols $\langle a\rangle$ and $T(l)$.

Definition 1.2.5. For any ring R, we let $h_2(\Gamma_1(N);R)$, $H_2^\infty(\Gamma_1(N);R)$ and $H_2(\Gamma_1(N);R)$ be the R-subalgebra of $\mathrm{End}(S_2(\Gamma_1(N);R))$, $\mathrm{End}(M_2^\infty(\Gamma_1(N);R))$ and $\mathrm{End}(M_2(\Gamma_1(N);R))$ generated by all $\langle a\rangle$ and $T(l)$, respectively. We consider them as algebras over the group ring $R[G]$ via $G \ni a \mapsto \langle a\rangle$.

Let $J_\mu(N)_{/\mathbb{Q}} = J_\mu(N)$ be the Jacobian variety of $X_\mu(N)_{/\mathbb{Q}}$ defined over $\mathbb{Q}$. The automorphism $\langle a\rangle$ of $X_\mu(N)_{/\mathbb{Q}}$ (resp. the Hecke correspondence above on $X_\mu(N)_{/\mathbb{Q}}$) induces covariantly (i.e. by "Albanese functoriality") an automorphism (resp. an endomorphism) of $J_\mu(N)$ over $\mathbb{Q}$, which we call $\langle a\rangle$ (resp. $T(l)$) again. The cotangent space of $J_\mu(N)$ at the origin is canonically isomorphic to $H^0(X_\mu(N)_{/\mathbb{Q}}, \Omega^1_{/\mathbb{Q}})$. The (contravariant) action of the endomorphisms $\langle a\rangle$ and $T(l)$ of $J_\mu(N)$ on this cotangent space then corresponds to $\langle a\rangle$ and $T(l)$ defined in (1.2.4) on differentials. The subalgebra of $\mathrm{End}(J_\mu(N))$ generated by all $\langle a\rangle$ and $T(l)$ is thus canonically isomorphic to $h_2(\Gamma_1(N);\mathbb{Z})$, and we identify these two rings.

Let $\zeta_N = \zeta \in \overline{\mathbb{Q}}$ be a primitive N-th root of unity. When R is a $\mathbb{Z}[1/N,\zeta]$-algebra, we have an involutive R-automorphism w_ζ of $X_\mu(N)_{/R}$; cf. [**G**, Section 6]. It sends an S-valued point (E,α) of $Y_\mu(N)_{/R}$ to (E',α'), where $E' = E/\alpha(\boldsymbol{\mu}_N)$ and α' sends ζ to the image to E' of an N-division point t of E satisfying $e_N(\alpha(\zeta),t) = \zeta$. For a cusp form f over R as in Definition 1.1.7, we set

$$\omega_{f|w_\zeta} = \omega_f|w_\zeta := w_\zeta^*(\omega_f). \tag{1.2.6}$$

We denote by the same symbol w_ζ the endomorphism of $J_\mu(N)_{/\mathbb{Q}(\zeta)} = J_\mu(N) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta)$ induced (covariantly) by w_ζ. It is in fact defined over $\mathbb{Q}(\zeta)^+$, the maximal real subfield of $\mathbb{Q}(\zeta)$. We have the following relations in $\mathrm{End}(J_\mu(N)_{/\mathbb{Q}(\zeta)^+})$

$$\begin{cases} w_\zeta^{-1} \circ \langle a \rangle \circ w_\zeta = \langle a^{-1} \rangle \text{ for } a \in G, \\ w_\zeta^{-1} \circ T(l) \circ w_\zeta = T(l) \circ \langle l \rangle^{-1} \text{ for } l \neq N. \end{cases} \tag{1.2.7}$$

Finally, we recall the effect of the above operators on cusps. In Shimura's notation, the set of cusps $C_{/\mathbb{Q}}(\overline{\mathbb{Q}})$ is identified with the set of equivalence classes

$$\left\{ \begin{bmatrix} x \\ y \end{bmatrix} \,\middle|\, x, y \in \mathbb{Z}/N\mathbb{Z},\ x \neq 0 \text{ or } y \neq 0 \right\} / \sim$$

where $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} x' \\ y' \end{smallmatrix}\right]$ if and only if $\left[\begin{smallmatrix} x' \\ y' \end{smallmatrix}\right] = \pm \left[\begin{smallmatrix} x+cy \\ y \end{smallmatrix}\right]$ with some $c \in \mathbb{Z}/N\mathbb{Z}$. We use the same symbol $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$ to denote its equivalence class. Then we have

$$\begin{cases} C_{\infty/\mathbb{Q}}(\overline{\mathbb{Q}}) = \left\{ \begin{bmatrix} x \\ 0 \end{bmatrix} \,\middle|\, x \in G \right\}, \\ C_{0/\mathbb{Q}}(\overline{\mathbb{Q}}) = \left\{ \begin{bmatrix} 0 \\ y \end{bmatrix} \,\middle|\, y \in G \right\} \end{cases} \tag{1.2.8}$$

and each set consists of $(N-1)/2$ elements. The action of w_ζ, $\langle a \rangle$ and $T(l)$, considered as correspondences on $X_\mu(N)_{/\overline{\mathbb{Q}}}$, on cusps is given as follows (cf. Wiles [**Wi**, Section 2]):

$$\begin{cases} w_\zeta : \begin{bmatrix} x \\ 0 \end{bmatrix} \leftrightarrow \begin{bmatrix} 0 \\ x \end{bmatrix} \quad \text{when } \zeta = e^{2\pi i/N}, \\ \langle a \rangle : \begin{cases} \begin{bmatrix} x \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} a^{-1}x \\ 0 \end{bmatrix} \\ \begin{bmatrix} 0 \\ y \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ ay \end{bmatrix} \end{cases} \quad \text{for } a \in G, \\ T(l) : \begin{cases} \begin{bmatrix} x \\ 0 \end{bmatrix} \mapsto l \begin{bmatrix} x \\ 0 \end{bmatrix} + \begin{bmatrix} l^{-1}x \\ 0 \end{bmatrix} = (l + \langle l \rangle) \begin{bmatrix} x \\ 0 \end{bmatrix} \\ \begin{bmatrix} 0 \\ y \end{bmatrix} \mapsto l \begin{bmatrix} 0 \\ ly \end{bmatrix} + \begin{bmatrix} 0 \\ y \end{bmatrix} = (l\langle l \rangle + 1) \begin{bmatrix} 0 \\ y \end{bmatrix} \end{cases} \quad \text{for } l \neq N, \\ T(N) : \begin{cases} \begin{bmatrix} x \\ 0 \end{bmatrix} \mapsto N \begin{bmatrix} x \\ 0 \end{bmatrix} \\ \begin{bmatrix} 0 \\ y \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ y \end{bmatrix} + 2 \sum_{z \in G} \begin{bmatrix} z \\ 0 \end{bmatrix}. \end{cases} \end{cases} \tag{1.2.9}$$

Especially, G acts on $C_{\infty/\mathbb{Q}}(\overline{\mathbb{Q}})$ and $C_{0/\mathbb{Q}}(\overline{\mathbb{Q}})$ simply transitively.

1.3. Duality between modular forms and Hecke algebras.

In each Hecke algebra in Definition 1.2.5, we can define the operator $T(n)$ for every positive integer n by the usual formulas, and it is well-known that all $T(n)$ generate that Hecke algebra over R (cf. e.g. [**DI**, Proposition 3.5.1]). If a modular form f has the q-expansion

$$f(q) = \sum_{n=0}^{\infty} a(n; f)q^n$$

then we have

$$a(1; f \mid T(n)) = a(n; f). \tag{1.3.1}$$

It is also well-known that the pairing

$$S_2(\Gamma_1(N); \mathbb{Z}) \times h_2(\Gamma_1(N); \mathbb{Z}) \xrightarrow{(\ ,\ )} \mathbb{Z} \ \text{ defined by } \ (f, t) := a(1; f \mid t) \tag{1.3.2}$$

gives a perfect duality between free $\mathbb{Z}$-modules of finite rank (cf. e.g. [**DI**, Proposition 12.4.13]).

Proposition 1.3.3. *The pairing*

$$M_2^{\infty}(\Gamma_1(N); \mathbb{Z}[1/N]) \times H_2^{\infty}(\Gamma_1(N); \mathbb{Z}[1/N]) \xrightarrow{(\ ,\ )} \mathbb{Z}[1/N]$$

defined by the same formula $(f, t) := a(1; f|t)$ *sets up a perfect duality between free* $\mathbb{Z}[1/N]$*-modules of finite rank.*

For the proof, we need the following

Lemma 1.3.4. (1) ([**Ma**, II, Lemma 5.9], [**Kam1**, Lemma 5.2]) *Let R be a $\mathbb{Z}[1/N]$-algebra. If the q-expansion of an element $f \in M_2(\Gamma_1(N); R)$ is a power series in q^N : $f(q) = \xi(q^N)$ with $\xi(q) \in R[[q]]$, then $\xi(q)$ is the q-expansion of a modular form g of level 1 and weight 2 over R in the sense of Katz* [**Kat1**].

(2) *Let k be a field of characteristic $p \neq N$. If the q-expansion of $f \in M_2^{\infty}(\Gamma_1(N); k)$ is a power series in q^N, then $f = 0$.*

Proof. We first review the proof of (1) for later use. We may assume that R is a $\mathbb{Z}[1/N, \zeta]$-algebra. The general case then follows from the q-expansion principle (for modular forms of level 1; [**Kat1**, Corollary 1.9.1]). We can thus fix an isomorphism $\boldsymbol{\mu}_N \cong \mathbb{Z}/N\mathbb{Z}$ over R by $\zeta \leftrightarrow 1 \bmod N$.

Let $Y(N)_{/R}$ be the moduli scheme classifying the pairs (E,ϕ) where E is an elliptic curve over an R-scheme S and ϕ is a ("naive") level N structure

$$\phi : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} E[N] \ (= \text{the kernel of multiplication by } N)$$

of determinant ζ over S. Let $M(R,N,2)$ be the space of modular forms (not necessarily holomorphic at cusps) associated with this moduli problem, i.e. its element is a rule that assigns to each pair as above a section of $\underline{\omega}_{E/S}^{\otimes 2}$ over S compatibly with cartesian squares (cf. [**Kat1**, 1.2]). We let $\gamma \in SL_2(\mathbb{Z}/N\mathbb{Z})$ act on $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ by $(m,n) \mapsto (m,n)^t\gamma$, and for $F \in M(R,N,2)$ set $\gamma F(E,\phi) := F(E, \phi \circ {}^t\gamma)$. This defines a left action of $SL_2(\mathbb{Z}/N\mathbb{Z})$ on $M(R,N,2)$.

We also consider an element of $M_2(\Gamma_1(N);R)$ as a similar rule as above, replacing (E,ϕ) by (E,α) as in (1.1.1). For (E,ϕ) as above, let $\alpha_\phi : \boldsymbol{\mu}_N \hookrightarrow E[N]$ be the composite of $\boldsymbol{\mu}_N \cong \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, the right mapping being given by $m \mapsto (m,0)$, and ϕ. We have a natural injection $M_2(\Gamma_1(N);R) \hookrightarrow M(R,N,2)$ by setting $h(E,\phi) := h(E,\alpha_\phi)$ for $h \in M_2(\Gamma_1(N);R)$, whose image is invariant under the subgroup $\left\{ \left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right] \right\}$ of $SL_2(\mathbb{Z}/N\mathbb{Z})$.

Let $\mathrm{Tate}(q) = \text{"}\mathbb{G}_m/q^{\mathbb{Z}}\text{"}$ be the Tate curve over $R((q^{1/N}))$. It carries a canonical level N structure

$$\phi_{\mathrm{can}} : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \cong \boldsymbol{\mu}_N \times \mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \mathrm{Tate}(q)[N]$$

which has determinant ζ, and a canonical invariant differential ω_{can} (cf. [**DR**, VII, 1.16], [**Kat2**, 2.2]). We recall that the q-expansion $F(q) \in R((q^{1/N}))$ of $F \in M(R,N,2)$ (at ∞) is given by $F(\mathrm{Tate}(q), \phi_{\mathrm{can}}) = F(q)\omega_{\mathrm{can}}^{\otimes 2}$.

For $h \in M_2(\Gamma_1(N);R)$, we define $w_\zeta h$ by $w_\zeta h(E,\alpha) := \varphi^* h(E',\alpha')$, where $w_\zeta(E,\alpha) = (E',\alpha')$ and $\varphi : E \to E'$ is the quotient morphism. We have $w_\zeta h = Nh|w_\zeta$ by [**G**, (6.8)], and $w_\zeta(w_\zeta h) = N^2 h$. We claim that

$$\left(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} w_\zeta h \right)(q) = h(q^{1/N})$$

the right hand side being the power series obtained by substituting $q^{1/N}$ for q in $h(q) \in R[[q]]$. Indeed, we have

$$\left(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} w_\zeta h \right)(q)\omega_{\mathrm{can}}^{\otimes 2} = w_\zeta h\left(\mathrm{Tate}(q), \phi_{\mathrm{can}} \circ \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right) = w_\zeta h(\mathrm{Tate}(q), \alpha'').$$

Here, $\alpha'' : \boldsymbol{\mu}_N \hookrightarrow \mathrm{Tate}(q)$ sends ζ to $\phi_{\mathrm{can}}(0,-1)$. We then see that $w_\zeta(\mathrm{Tate}(q),$

$\alpha'') = (\mathrm{Tate}(q^{1/N}), \alpha''')$ with $\alpha''' : \boldsymbol{\mu}_N \hookrightarrow \mathrm{Tate}(q^{1/N})$ the natural inclusion corresponding to $\boldsymbol{\mu}_N \hookrightarrow \mathbb{G}_m$ (cf. [**Kat2**, 2.3.3]). Our claim follows from this.

Now consider $f \in M_2(\Gamma_1(N); R)$ in the proposition. Our hypothesis and the above relation show that $\left(\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right] w_\zeta f\right)(q)$ is a power series in q. It follows that $\left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right] w_\zeta f$ has the same q-expansion as $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right] w_\zeta f$ (cf. [**DR**, VII, (3.8.1)]). This implies that $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right] w_\zeta f$ is invariant under the subgroup $\left\{\left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right]\right\}$ of $SL_2(\mathbb{Z}/N\mathbb{Z})$ by the q-expansion principle (cf. [**Kat1**, Theorem 1.6.1]; note that our $Y(N)_{/\mathbb{Z}[1/N,\zeta]}$ is connected). Consequently, $w_\zeta f$ is invariant under the subgroup $\left\{\left[\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right]\right\}$. Since $w_\zeta f$ is *a priori* invariant under $\left\{\left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right]\right\}$, it is invariant under the whole group $SL_2(\mathbb{Z}/N\mathbb{Z})$. Therefore there is a modular form g of level 1 and weight 2 over R (necessarily holomorphic at the cusp) such that $w_\zeta f = g$, i.e.

$$f = N^{-2} w_\zeta g = N^{-1} g \mid w_\zeta.$$

It is easy to check that this g has the q-expansion $\xi(q)$.

We next prove (2). We may assume that k is an algebra over $\mathbb{Z}[1/N, \zeta]$. Let g be the modular form as in (1) for f, and assume that $g \neq 0$. By [**Ma**, II, Proposition (4.10)] g is not a cusp form. ([**Ma**, II, Proposition (5.6)] actually implies that $p = 2$ or 3, and the q-expansion of g is a nonzero constant.) It follows from the relation above that f does not vanish at (0-)cusps, and hence cannot belong to $M_2^\infty(\Gamma_1(N); k)$. □

Proof of Proposition 1.3.3. Standard argument shows that the pairing

$$M_2^\infty(\Gamma_1(N); \mathbb{Q}) \times H_2^\infty(\Gamma_1(N); \mathbb{Q}) \xrightarrow{(\ ,\ )} \mathbb{Q}$$

is perfect, and that the mapping

$$M_2^\infty(\Gamma_1(N); \mathbb{Z}[1/N]) \to \mathrm{Hom}_{\mathbb{Z}[1/N]}(H_2^\infty(\Gamma_1(N); \mathbb{Z}[1/N]), \mathbb{Z}[1/N])$$

induced from the pairing is injective. We want to show that this is surjective.

Let φ be an element of the right hand side. By the first remark, there is an $f \in M_2^\infty(\Gamma_1(N); \mathbb{Q})$ such that

$$\varphi(t) = (f, t) \quad \text{for all } t \in H_2^\infty(\Gamma_1(N); \mathbb{Z}[1/N]).$$

By (1.3.1), we have $a(n; f) \in \mathbb{Z}[1/N]$ for all $n \geq 1$. If f does not belong to $M_2^\infty(\Gamma_1(N); \mathbb{Z}[1/N])$, there is a prime number $p \neq N$ and a positive integer c such that the q-expansion of $p^c f$ reduced modulo p is a nonzero constant. This contradicts the previous lemma. □

We now list some consequences of the duality given in Proposition 1.3.3.

COROLLARY 1.3.5. *For any $\mathbb{Z}[1/N]$-algebra R, the canonical homomorphism*

$$H_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N]) \otimes_{\mathbb{Z}[1/N]} R \to H_2^\infty(\Gamma_1(N);R)$$

is an isomorphism.

PROOF. Since $H_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N]) \otimes_{\mathbb{Z}[1/N]} R$ acts on

$$M_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N]) \otimes_{\mathbb{Z}[1/N]} R \underset{(1.1.8)}{\cong} M_2^\infty(\Gamma_1(N);R)$$

we have the above homomorphism, which is clearly surjective. But the pairing in Proposition 1.3.3 tensored with R remains perfect, and hence the above action is faithful, which shows the injectivity of the homomorphism. □

COROLLARY 1.3.6. *For any $\mathbb{Z}[1/N]$-algebra R, the pairing*

$$M_2^\infty(\Gamma_1(N);R) \times H_2^\infty(\Gamma_1(N);R) \xrightarrow{(\ ,\ )} R$$

defined by the formula $(f,t) := a(1;f|t)$ is perfect.

PROOF. This follows from Proposition 1.1.8, Proposition 1.3.3 and Corollary 1.3.5. □

COROLLARY 1.3.7. *For any $\mathbb{Z}[1/N]$-algebra R, $H_2^\infty(\Gamma_1(N);R)$ is generated over R by all $T(n)$ with n not divisible by N.*

PROOF. Denote by $H_2^{\infty(N)}(\Gamma_1(N);R)$ the R-subalgebra generated by $T(n)$ with $N \nmid n$.

It is enough to prove our assertion when $R = \mathbb{Z}[1/N]$. If the assertion is false in this case, there is a prime number $p \neq N$ such that

$$H_2^{\infty(N)}(\Gamma_1(N);\mathbb{Z}/p\mathbb{Z}) \subsetneq H_2^\infty(\Gamma_1(N);\mathbb{Z}/p\mathbb{Z})$$

by Corollary 1.3.5. Then there is a non-zero $f \in M_2^\infty(\Gamma_1(N);\mathbb{Z}/p\mathbb{Z})$ which annihilates $H_2^{\infty(N)}(\Gamma_1(N);\mathbb{Z}/p\mathbb{Z})$ under the pairing in Corollary 1.3.6 for $R = \mathbb{Z}/p\mathbb{Z}$. By (1.3.1), the q-expansion of f is a power series in q^N. This contradicts Lemma 1.3.4. □

REMARK 1.3.8. The same argument as above shows that the assertions in

Corollaries 1.3.5 through 1.3.7 also hold for cusp forms and the associated Hecke algebras. Precisely, we have

(1) $h_2(\Gamma_1(N);\mathbb{Z})\otimes_{\mathbb{Z}} R \to h_2(\Gamma_1(N);R)$ is an isomorphism, and
(2) $S_2(\Gamma_1(N);R)\times h_2(\Gamma_1(N);R) \xrightarrow{(\ ,\ )} R$ is perfect for *any* ring R; and
(3) $h_2(\Gamma_1(N);R)$ is generated over R by $T(n)$ with $N\nmid n$ for any $\mathbb{Z}[1/N]$-algebra R. (But we do not know whether this assertion remains true for general R or not.)

We also remark that the pairing in Corollary 1.3.6 is not perfect unless we assume that N is invertible in R.

Finally, we add the following

PROPOSITION 1.3.9. *The involution of* $\mathrm{End}(J_\mu(N)_{/\mathbb{Q}(\zeta)^+})$ *defined by* $t\mapsto w_\zeta^{-1}\circ t\circ w_\zeta$ *induces an involution of* $h_2(\Gamma_1(N);R)$ *for any* $\mathbb{Z}[1/N]$*-algebra* R.

PROOF. This follows from the third assertion above and the formula (1.2.7). □

2. Eisenstein ideals.

2.1. Eisenstein series and Eisenstein ideals.

As in Section 1, we fix a prime number $N\geq 5$, and recall that we have set $G=(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$. We denote by $\widehat{G}$ the character group of G (with values in $\overline{\mathbb{Q}}^\times$), and write $\mathbf{1}$ for its unit element. We also set

$$\widehat{G}^0 := \widehat{G}-\{\mathbf{1}\}. \tag{2.1.1}$$

As usual, we identify an element $\chi\in\widehat{G}$ with an even Dirichlet character defined modulo N, so that we have $\chi(n)=0$ for an integer n divisible by N when $\chi\neq\mathbf{1}$.

As is well-known, $M_2(\Gamma_1(N);\mathbb{C})$ contains three kinds of Eisenstein series E_2, $E_{2,\chi}$ and $E'_{2,\chi}$ which have the following q-expansions:

$$E_2(q)=\frac{N-1}{24}+\sum_{n=1}^{\infty}\Bigg(\sum_{\substack{0<t|n\\ N\nmid t}} t\Bigg)q^n, \tag{2.1.2}$$

$$E_{2,\chi}(q)=-\frac{B_{2,\chi}}{4}+\sum_{n=1}^{\infty}\Bigg(\sum_{0<t|n}\chi(t)t\Bigg)q^n \quad \text{for } \chi\in\widehat{G}^0, \tag{2.1.3}$$

$$E'_{2,\chi}(q)=\sum_{n=1}^{\infty}\Bigg(\sum_{0<t|n}\chi(\frac{n}{t})t\Bigg)q^n \quad \text{for } \chi\in\widehat{G}^0 \tag{2.1.4}$$

where $B_{2,\chi}$ is the second generalized Bernoulli number, which is explicitly given by

$$B_{2,\chi} = \frac{1}{N}\sum_{a=1}^{N}\chi(a)a^2 \tag{2.1.5}$$

(cf. Washington [**Wa**, Exercise 4.2]). These $N-2$ Eisenstein series are linearly independent over $\mathbb{C}$, and generate the orthogonal complement of $S_2(\Gamma_1(N);\mathbb{C})$ with respect to the Petersson metric.

It is also well-known that these Eisenstein series are Hecke eigenforms: The series E_2 belongs to $M_2(\Gamma_0(N);\mathbb{C})$, while $E_{2,\chi}$ and $E'_{2,\chi}$ have the (Nebentypus) character χ, and

$$\begin{cases} E_2 \mid T(n) = \Big(\sum_{\substack{0<t\mid n \\ N\nmid t}} t\Big)E_2, \\ E_{2,\chi} \mid T(n) = \big(\sum_{0<t\mid n}\chi(t)t\big)E_{2,\chi}, \\ E'_{2,\chi} \mid T(n) = \big(\sum_{0<t\mid n}\chi(\frac{n}{t})t\big)E'_{2,\chi}. \end{cases} \tag{2.1.6}$$

$E_{2,\chi}$ belongs to $M_2^\infty(\Gamma_1(N);\mathbb{C})$, but E_2 and $E'_{2,\chi}$ do not (cf. [**Oh1**, (2.5.5)] for the explicit calculation of the constant terms of the Fourier expansions of $E_{2,\chi}$ and $E'_{2,\chi}$ at various cusps). Since $\dim_{\mathbb{C}} M_2^\infty(\Gamma_1(N);\mathbb{C}) - \dim_{\mathbb{C}} S_2(\Gamma_1(N);\mathbb{C}) = \#(\infty\text{-cusps}) - 1 = (N-3)/2$ by the Riemann-Roch theorem, we see that

$$M_2^\infty(\Gamma_1(N);\mathbb{C}) = S_2(\Gamma_1(N);\mathbb{C}) \oplus \sum_{\chi\in\widehat{G}^0}\mathbb{C}E_{2,\chi}. \tag{2.1.7}$$

More generally, when K is a field of characteristic zero, we have the unique direct sum decomposition as a module over $H_2^\infty(\Gamma_1(N);K)$:

$$M_2^\infty(\Gamma_1(N);K) = S_2(\Gamma_1(N);K) \oplus \mathrm{Eis}_2^\infty(K) \tag{2.1.8}$$

where we have set

$$\mathrm{Eis}_2^\infty(K) := \mathrm{Ker}\Big(\prod_{\chi\in\widehat{G}^0}(T(l) - (1+\chi(l)l)) \text{ acting on } M_2^\infty(\Gamma_1(N);K)\Big) \tag{2.1.9}$$

for any prime $l \geq 7$ different from N. When K contains all values of $\chi \in \widehat{G}$, we of course have $\mathrm{Eis}_2^\infty(K) = \sum_{\chi\in\widehat{G}^0} KE_{2,\chi}$.

Now set

$$\eta(l) := T(l) - (1 + l\langle l\rangle) \quad \text{for each prime number } l \neq N, \tag{2.1.10}$$

$$\tau := \sum_{a\in G} \langle a\rangle \tag{2.1.11}$$

in either of $H_2^\infty(\Gamma_1(N); R)$ or $h_2(\Gamma_1(N); R)$. We denote by the same symbol τ the element $\sum_{a\in G} a$ of $R[G]$.

Definition 2.1.12. For any ring R, we denote by $\mathcal{I}_{\infty,R}$ (resp. $I_{\infty,R}$) the ideal of $H_2^\infty(\Gamma_1(N); R)$ (resp. $h_2(\Gamma_1(N); R)$) generated by all $\eta(l)$ (with prime numbers $l \neq N$), $T(N) - 1$ and τ. $\mathcal{I}_{\infty,R}$ (resp. $I_{\infty,R}$) is called the *Eisenstein ideal* of $H_2^\infty(\Gamma_1(N); R)$ (resp. $h_2(\Gamma_1(N); R)$ relative to the inclusion $S_2(\Gamma_1(N); R) \subseteq M_2^\infty(\Gamma_1(N); R)$).

$I_{\infty,R}$ is thus the image of $\mathcal{I}_{\infty,R}$ under the canonical surjective homomorphism $H_2^\infty(\Gamma_1(N); R) \twoheadrightarrow h_2(\Gamma_1(N); R)$. The following proposition may justify the above terminology.

Proposition 2.1.13. *Let R be an integral domain of characteristic zero, and K its quotient field. Then $\mathcal{I}_{\infty,R}$ is the annihilator ideal of* $\mathrm{Eis}_2^\infty(K)$ *in $H_2^\infty(\Gamma_1(N); R)$, and $H_2^\infty(\Gamma_1(N); R)/\mathcal{I}_{\infty,R}$ is isomorphic to $R[G]/(\tau)$ as an $R[G]$-algebra.*

Proof. Let K' be an extension of K containing all values of $\chi \in \widehat{G}$. Then the R-algebra homomorphism

$$R[G]/(\tau) \to \oplus_{\chi\in\widehat{G}^0} K' \quad (\text{direct sum indexed by } \chi \in \widehat{G}^0)$$

sending $a \in G$ to $(\chi(a))_{\chi\in\widehat{G}^0}$ is injective, and we may identify $R[G]/(\tau)$ with its image.

The action of $H_2^\infty(\Gamma_1(N); R)$ on $\oplus_{\chi\in\widehat{G}^0} K' E_{2,\chi}$ gives a homomorphism of $H_2^\infty(\Gamma_1(N); R)$ to $\oplus_{\chi\in\widehat{G}^0} K'$ whose kernel $\mathcal{J}$ is the annihilator ideal of $\mathrm{Eis}_2^\infty(K)$. By (2.1.6), this homomorphism factors through $R[G]/(\tau)$, and $\mathcal{J}$ contains $\mathcal{I}_{\infty,R}$.

On the other hand, by the definition of $\mathcal{I}_{\infty,R}$, there is a canonical surjective homomorphism $R[G]/(\tau) \to H_2^\infty(\Gamma_1(N); R)/\mathcal{I}_{\infty,R}$. We thus have a sequence of $R[G]$-algebra homomorphisms

$$R[G]/(\tau) \twoheadrightarrow H_2^\infty(\Gamma_1(N); R)/\mathcal{I}_{\infty,R} \twoheadrightarrow H_2^\infty(\Gamma_1(N); R)/\mathcal{J} \twoheadrightarrow R[G]/(\tau)$$

whose composite is the identity. Our conclusion follows from this. □

It follows that $\mathcal{I}_{\infty,R}$ is always a proper ideal of $H_2^\infty(\Gamma_1(N);R)$, but we remark that $I_{\infty,R}$ is not necessarily a proper ideal of $h_2(\Gamma_1(N);R)$.

COROLLARY 2.1.14. *Let R be a $\mathbb{Z}[1/N]$-algebra. Then the ideal $\mathcal{I}_{\infty,R}$ of $H_2^\infty(\Gamma_1(N);R)$ is generated by all $\eta(l)$ and τ (i.e. without $T(N)-1$), and consequently the same holds for $I_{\infty,R}$.*

PROOF. In Corollary 1.3.7, we have shown that $H_2^\infty(\Gamma_1(N);R)$ coincides with its R-subalgebra $H_2^{\infty(N)}(\Gamma_1(N);R)$ generated by $T(n)$ with $N \nmid n$. Let $\mathcal{I}_{\infty,R}^{(N)}$ be the ideal generated by all $\eta(l)$ and τ. We again obtain a sequence of $R[G]$-algebra homomorphisms whose composite is the identity

$$R[G]/(\tau) \twoheadrightarrow H_2^{\infty(N)}(\Gamma_1(N);R)/\mathcal{I}_{\infty,R}^{(N)} \twoheadrightarrow H_2^\infty(\Gamma_1(N);R)/\mathcal{I}_{\infty,R} \xrightarrow{\sim} R[G]/(\tau).$$

We thus conclude that $\mathcal{I}_{\infty,R}^{(N)} = \mathcal{I}_{\infty,R}$. □

The purpose of the rest of this section is to compute the (finite) index $|h_2(\Gamma_1(N);\mathbb{Z}_p) : I_{\infty,\mathbb{Z}_p}|$ for prime numbers $p \neq 2, N$; cf. Theorem 2.4.2 below. To do this, we need the following two preliminary subsections.

2.2. Residue mapping for $M_2^\infty(\Gamma_1(N);R)$.

Recall that $C_{\infty/R} \subset X_\mu(N)_{/R}$ is a disjoint sum of $(N-1)/2$ copies of $\mathrm{Spec}(R)$ for any $\mathbb{Z}[1/N]$-algebra R, and that $C_{\infty/\mathbb{Q}}(\overline{\mathbb{Q}})$ consists of $(N-1)/2$ elements $\left[\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right]$ $(a \in G)$, in the notation of 1.1 and 1.2.

DEFINITION 2.2.1. We write $[a]_\infty$ for $\left[\begin{smallmatrix} a \\ 0 \end{smallmatrix}\right]$. For any ring R, we denote by $R[C_\infty]$ the free R-module on the set $\{[a]_\infty \mid a \in G\}$. Its degree zero part $R[C_\infty]^0$ is defined as the kernel of the homomorphism $R[C_\infty] \to R$ sending $\sum_{a\in G} c_a[a]_\infty$ to $\sum_{a\in G} c_a$. We consider $R[C_\infty]$ and $R[C_\infty]^0$ as modules over $R[G]$ by the second formula in (1.2.9): $G \ni a$ sends $[b]_\infty$ to $\langle a\rangle[b]_\infty = [a^{-1}b]_\infty$.

For $f \in M_2^\infty(\Gamma_1(N);\mathbb{Q})$, denote by $\mathrm{Res}_{[a]_\infty}\omega_f \in \mathbb{Q}$ the residue of the corresponding differential at $[a]_\infty$. It is clear from the definition (1.2.4) that

$$\mathrm{Res}_{\langle a\rangle[b]_\infty}\omega_f = \mathrm{Res}_{[b]_\infty}\omega_{f|\langle a\rangle}. \tag{2.2.2}$$

Consider the mapping

$$\mathbf{Res} : M_2^\infty(\Gamma_1(N);\mathbb{Q}) \to \mathbb{Q}[C_\infty]^0 \ \text{ defined by } f \mapsto \sum_{a\in G} \mathrm{Res}_{[a]_\infty}\omega_f \cdot [a]_\infty. \tag{2.2.3}$$

Then comparing the dimensions, we have an exact sequence

$$0 \to S_2(\Gamma_1(N);\mathbb{Q}) \to M_2^\infty(\Gamma_1(N);\mathbb{Q}) \xrightarrow{\mathbf{Res}} \mathbb{Q}[C_\infty]^0 \to 0. \tag{2.2.4}$$

If $f \in M_2^\infty(\Gamma_1(N);\mathbb{Q})$ has the q-expansion $f(q) = \sum_{n=0}^\infty a(n;f)q^n$, then $\mathrm{Res}_{[1]_\infty}\omega_f = a(0;f)$. It follows from (2.2.2) that we have

$$\mathbf{Res}(f) = \sum_{a\in G} a(0; f \mid \langle a^{-1}\rangle)[a]_\infty. \tag{2.2.5}$$

Proposition 2.2.6. *The exact sequence* (2.2.4) *induces the following exact sequence*

$$0 \to S_2(\Gamma_1(N);\mathbb{Z}[1/N]) \to M_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N]) \xrightarrow{\mathbf{Res}} \mathbb{Z}[1/N][C_\infty]^0 \to 0.$$

Proof. It is clear from the description (2.2.5) that $\mathbf{Res}(f) \in \mathbb{Z}[1/N][C_\infty]^0$ whenever $f \in M_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N])$, and we obtain the exact sequence

$$0 \to S_2(\Gamma_1(N);\mathbb{Z}[1/N]) \to M_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N]) \xrightarrow{\mathbf{Res}} \mathbb{Z}[1/N][C_\infty]^0.$$

Let p be a prime number different from N. By tensoring $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{Z}[1/N]$, the above sequence yields the sequence

$$0 \to S_2(\Gamma_1(N);\mathbb{Z}/p\mathbb{Z}) \to M_2^\infty(\Gamma_1(N);\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\mathbf{Res}} \mathbb{Z}/p\mathbb{Z}[C_\infty]^0$$

by Proposition 1.1.8. Here, the mapping **Res** is given by the formula (2.2.5). We then see that this sequence is exact, and hence, again comparing the dimensions, **Res** above is surjective.

Consequently, we have

$$\mathrm{Coker}\big(M_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N]) \xrightarrow{\mathbf{Res}} \mathbb{Z}[1/N][C_\infty]^0\big) \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}/p\mathbb{Z} = \{0\}$$

for all primes $p \neq N$, which completes the proof. □

Corollary 2.2.7. *We have the exact sequence*

$$0 \to S_2(\Gamma_1(N);R) \to M_2^\infty(\Gamma_1(N);R) \xrightarrow{\mathbf{Res}} R[C_\infty]^0 \to 0$$

for any $\mathbb{Z}[1/N]$-algebra R, where the mapping **Res** *is given by the formula* (2.2.5).

PROOF. This follows from the proposition above and Proposition 1.1.8. □

In our computation of the congruence module in 2.4 below, we will also need the following fact.

PROPOSITION 2.2.8. *Let K be a field of characteristic zero containing the values of $\chi \in \widehat{G}^0$, and consider $E_{2,\chi}$ as an element of $M_2^\infty(\Gamma_1(N); K)$. Then we have*

$$\mathbf{Res}(E_{2,\chi}) = \sum_{a \in G} \chi(a)(-B_{2,\chi}/4)[a^{-1}]_\infty \in K[C_\infty].$$

PROOF. By (2.1.3), we have $\mathrm{Res}_{[1]_\infty}\omega_{E_{2,\chi}} = a(0; E_{2,\chi}) = -B_{2,\chi}/4$. Since $E_{2,\chi}|\langle a\rangle = \chi(a)E_{2,\chi}$, our conclusion follows from (2.2.5). □

2.3. Congruence modules and duality.

We first recall the notion of congruence modules (cf. [**Oh1**, 1.1]). Let R be an integral domain and K its quotient field. Suppose we are given an exact sequence of flat R-modules together with its splitting over K:

$$\begin{cases} 0 \to A \xrightarrow{i} B \xrightarrow{\pi} C \to 0 \text{ (exact)}, \\ 0 \leftarrow A \otimes_R K \xleftarrow{t} B \otimes_R K \xleftarrow{s} C \otimes_R K \leftarrow 0 \text{ (exact)}. \end{cases} \tag{2.3.1}$$

Namely, if we denote by i_K (resp. π_K) the base extension of i (resp. π) to K, $t \circ i_K$ and $\pi_K \circ s$ are the identity mappings. We then have the following commutative square of canonical isomorphisms

$$\begin{array}{ccc} B/(i(A) + B \cap s(C)) & \xrightarrow[\sim]{\pi} & C/\pi(B \cap s(C)) \\ {\scriptstyle t}\downarrow\wr & & \wr\downarrow \\ t(B)/A & \xrightarrow[\sim]{} & (t(B) \oplus C)/B. \end{array} \tag{2.3.2}$$

We identify these four modules, and call any one of them the *congruence module* attached to the situation (2.3.1). The formation of congruence modules commutes with flat base extensions of integral domains.

Now assume that A, B and C are free R-modules of finite rank. Indicating by "$^\vee$" the R- or K-dual, we obtain from (2.3.1) the following exact sequence with its splitting over K:

$$\begin{cases} 0 \to C^\vee \xrightarrow{\pi^\vee} B^\vee \xrightarrow{i^\vee} A^\vee \to 0 \text{ (exact)}, \\ 0 \leftarrow C^\vee \otimes_R K \xleftarrow{s^\vee} B^\vee \otimes_R K \xleftarrow{t^\vee} A^\vee \otimes_R K \leftarrow 0 \text{ (exact)}. \end{cases} \tag{2.3.3}$$

PROPOSITION 2.3.4. *Let the notation and the assumption be as above, and denote by* $\mathfrak{C}$ *(resp.* $\mathfrak{C}^\vee$*) the congruence module attached to* (2.3.1) *(resp.* (2.3.3)*). If* R *is a principal ideal domain, then* $\mathfrak{C}$ *and* $\mathfrak{C}^\vee$ *are isomorphic.*

PROOF. There is a nonzero element $c \in R$ such that cs sends C to B. By the theory of elementary divisors, there are bases $\{f_1, \ldots, f_k\}$ and $\{e_1, \ldots, e_n\}$ of C and B such that $(cs)(f_i) = a_i e_i$ $(1 \le i \le k)$ with $a_i \in R$.

Thus, from the beginning, we may assume that $A = R^m$, $B = R^n$, $C = R^k$ (the set of column vectors), and that s is given by the $n \times k$ matrix

$$S = \begin{bmatrix} \alpha_1 & & 0 \\ & \ddots & \\ & & \alpha_k \\ 0 & & \end{bmatrix}, \quad (\alpha_i \in K, \alpha_i \neq 0).$$

If P is the $k \times n$ matrix giving $\pi : R^n \twoheadrightarrow R^k$, then since $\pi_K \circ s$ is the identity, we see that P is of the form:

$$P = \begin{bmatrix} p_1 & & 0 & \\ & \ddots & & * \\ 0 & & p_k & \end{bmatrix}, \quad (p_i \in R)$$

with $\alpha_i p_i = 1$, i.e. $\alpha_i = 1/p_i$.

We therefore see that

$$\pi(R^n \cap s(R^k)) = \left\{ \begin{bmatrix} p_1 x_1 \\ \vdots \\ p_k x_k \end{bmatrix} \,\middle|\, x_1, \ldots, x_k \in R \right\}$$

and hence

$$\mathfrak{C} = R^k / \pi(R^n \cap s(R^k)) \cong \oplus_{i=1}^k R/(p_i).$$

On the other hand, we may identify $R^{r\vee}$ (resp. $K^{r\vee}$) with R^r (resp. K^r) via

the standard inner product. Then $s^\vee : K^n \to K^k$ is given by the transposed matrix ${}^tS$. Thus we have

$$\mathfrak{C}^\vee = s^\vee(R^n)/R^k \cong \oplus_{i=1}^k \frac{1}{p_i} R/R. \qquad \square$$

We now apply the above consideration to the setting of the previous subsection. Let $\mathfrak{o}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ with $p \neq N$, and F its quotient field. We have the exact sequence obtained in Corollary 2.2.7:

$$0 \to S_2(\Gamma_1(N); \mathfrak{o}) \xrightarrow{i} M_2^\infty(\Gamma_1(N); \mathfrak{o}) \xrightarrow{\pi} \mathfrak{o}[C_\infty]^0 \to 0 \tag{2.3.5}$$

where $\pi = \mathbf{Res}$. Recall that $M_2^\infty(\Gamma_1(N); F)$ is a direct sum of $S_2(\Gamma_1(N); F)$ and $\mathrm{Eis}_2^\infty(F)$ by (2.1.8). The mapping $\pi = \mathbf{Res}$ induces an isomorphism $\mathrm{Eis}_2^\infty(F) \xrightarrow{\sim} F[C_\infty]^0$, and we take $s : F[C_\infty]^0 \to M_2^\infty(\Gamma_1(N); F)$ to be the inverse of this isomorphism. Also, let $t : M_2^\infty(\Gamma_1(N); F) \to S_2(\Gamma_1(N); F)$ be the projection with respect to the above direct sum decomposition. These s and t give a splitting of the exact sequence

$$0 \to S_2(\Gamma_1(N); F) \xrightarrow{i_F} M_2^\infty(\Gamma_1(N); F) \xrightarrow{\pi_F} F[C_\infty]^0 \to 0$$

which is the unique splitting as $H_2^\infty(\Gamma_1(N); F)$-modules provided that we endow $F[C_\infty]^0$ with the quotient module structure of $M_2^\infty(\Gamma_1(N); F)$ (which is different from the action described in (1.2.9)).

Let $\mathfrak{C}_{\mathfrak{o}}^{\mathrm{mod}}$ be the associated congruence module.

PROPOSITION 2.3.6. *Let the notation be as above. Then we have an isomorphism of $\mathfrak{o}$-modules*

$$h_2(\Gamma_1(N); \mathfrak{o})/I_{\infty,\mathfrak{o}} \cong \mathfrak{C}_{\mathfrak{o}}^{\mathrm{mod}}.$$

PROOF. We show that the congruence module attached to the situation dual to the above is isomorphic to $h_2(\Gamma_1(N); \mathfrak{o})/I_{\infty,\mathfrak{o}}$. Our conclusion then follows from the previous proposition.

We obtain from the duality in Corollary 1.3.6 (cf. also Remark 1.3.8) the following isomorpisms

$$\begin{cases} M_2^\infty(\Gamma_1(N); \mathfrak{o})^\vee \cong H_2^\infty(\Gamma_1(N); \mathfrak{o}), \\ S_2(\Gamma_1(N); \mathfrak{o})^\vee \cong h_2(\Gamma_1(N); \mathfrak{o}). \end{cases}$$

Identifying the both sides of these isomorphisms, we see that

$$i^\vee : H_2^\infty(\Gamma_1(N);\mathfrak{o}) \to h_2(\Gamma_1(N);\mathfrak{o})$$

is the canonical homomorphism sending $T(n)$ to $T(n)$.

On the other hand, we see that

$$H_2^\infty(\Gamma_1(N);\mathfrak{o}) \cap t^\vee(h_2(\Gamma_1(N);\mathfrak{o})) = H_2^\infty(\Gamma_1(N);\mathfrak{o}) \cap t^\vee(h_2(\Gamma_1(N);F)) =: \mathcal{X}$$

(cf. [**Oh1**, (1.1.5)]), and $T \in H_2^\infty(\Gamma_1(N);\mathfrak{o})$ belongs to $\mathcal{X}$ if and only if $(f,T) = a(1;f|T) = 0$ for all $f \in \mathrm{Eis}_2^\infty(F)$. This latter condition is equivalent to that $a(1;f|T(n)T) = a(n;f|T) = 0$ for all $f \in \mathrm{Eis}_2^\infty(F)$ and arbitrary $n \geq 1$. Consequently, $\mathcal{X}$ is the annihilator ideal of $\mathrm{Eis}_2^\infty(F)$ in $H_2^\infty(\Gamma_1(N);\mathfrak{o})$, that is, $\mathcal{X} = \mathcal{I}_{\infty,\mathfrak{o}}$ by Proposition 2.1.13.

Combining these, we conclude that the congruence module in question is isomorphic to $h_2(\Gamma_1(N);\mathfrak{o})/i^\vee(\mathcal{I}_{\infty,\mathfrak{o}}) = h_2(\Gamma_1(N);\mathfrak{o})/I_{\infty,\mathfrak{o}}$. □

2.4. Index of the Eisenstein ideal.

Recall that we put

$$c(N) := N \prod_{\chi \in \widehat{G}^0} \frac{B_{2,\chi}}{4} \quad (\in \mathbb{Z}) \tag{2.4.1}$$

in the introduction, and note that this is the product of the constant terms of $E_{2,\chi}(q)$ ($\chi \in \widehat{G}^0$) multiplied by N, up to sign. The following theorem is the main result of this section.

THEOREM 2.4.2. *Let p be a prime number different from 2 and N, and $\mathfrak{o}$ the ring of integers of a finite extension F of $\mathbb{Q}_p$. Then, under the terminology of the previous subsection, we have*

$$|h_2(\Gamma_1(N);\mathfrak{o}) : I_{\infty,\mathfrak{o}}| = |\mathfrak{C}_{\mathfrak{o}}^{\mathrm{mod}}| = |\mathfrak{o} : c(N)\mathfrak{o}|.$$

Since the formation of congruence modules commutes with flat extensions of base domains, we may assume that $\mathfrak{o}$ is sufficiently large, to prove the theorem. We thus assume that $\mathfrak{o}$ *contains the values of all* $\chi \in \widehat{G}^0$, and proceed to compute $|\mathfrak{C}_{\mathfrak{o}}^{\mathrm{mod}}|$.

Now we look at the exact sequence (2.3.5), whose canonical splitting over F is given by s and t described in the previous subsection. Consider the following $\mathfrak{o}$-lattices in $\mathrm{Eis}_2^\infty(F)$

$$\begin{cases} L_1 := M_2^\infty(\Gamma_1(N);\mathfrak{o}) \cap s(\mathfrak{o}[C_\infty]^0) = M_2^\infty(\Gamma_1(N);\mathfrak{o}) \cap s(F[C_\infty]^0) \\ \quad\ = M_2^\infty(\Gamma_1(N);\mathfrak{o}) \cap \mathrm{Eis}_2^\infty(F), \\ L_2 := \sum_{\chi\in\widehat{G}^0} \mathfrak{o}E_{2,\chi}. \end{cases} \tag{2.4.3}$$

Here, each $E_{2,\chi}$ belongs to $M_2^\infty(\Gamma_1(N);\mathfrak{o})$ by (2.1.3) and (2.1.5), and hence we have $L_1 \supseteq L_2$. We are going to compute the indices $|L_1 : L_2| = |\pi(L_1) : \pi(L_2)|$ and $|\mathfrak{o}[C_\infty]^0 : \pi(L_2)|$. To do this, we set

$$r := \frac{N-3}{2} \tag{2.4.4}$$

and fix a generator g (resp. χ_0) of the cyclic group G (resp. $\widehat{G}$) so that

$$\begin{cases} G = \{1, g, \dots, g^r\}, \\ \widehat{G} = \{\mathbf{1}, \chi_0, \dots, \chi_0^r\}. \end{cases} \tag{2.4.5}$$

LEMMA 2.4.6. *Under the same assumption as in Theorem* 2.4.2, *let* $F^r \to \mathrm{Eis}_2^\infty(F)$ *be the isomorphism defined by*

$$\begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} \mapsto \sum_{i=1}^r x_i E_{2,\chi_0^i}.$$

Then the inverse image of L_1 *under this mapping is*

$$L_1' = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} \in F^r \;\middle|\; \sum_{i=1}^r x_i \chi_0^i(a) \in \mathfrak{o} \text{ for all } a \in G \right\}.$$

PROOF. An element $\begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} \in F^r$ is mapped to L_1 if and only if

(i) $\sum_{i=1}^r x_i(B_{2,\chi_0^i}/4) \in \mathfrak{o}$, and

(ii) $\sum_{i=1}^r x_i(\sum_{0<t|n} \chi_0^i(t)t) \in \mathfrak{o}$ for all $n \geq 1$.

Subtracting the relation (ii) for $n = N$ from that for $n = l$, a prime different from N and p, we obtain $\sum_{i=1}^r x_i \chi_0^i(l) \in \mathfrak{o}$. By this and the well-known theorem of Dirichlet, we see that the condition (ii) implies the condition

(iii) $\sum_{i=1}^{r} x_i \chi_0^i(a) \in \mathfrak{o}$ for all $a \in G$

in our statement.

Conversely, if we assume (iii), we have

$$\sum_{i=1}^{r} x_i \Big(\sum_{0<t|n} \chi_0^i(t) t \Big) = \sum_{0<t|n} \Big(\sum_{i=1}^{r} x_i \chi_0^i(t) \Big) t \in \mathfrak{o}$$

and thus (ii) follows from (iii). Similar argument, using (2.1.5), shows that (iii) also implies (i), since $p \neq 2$. □

Under the notation (2.4.5), set $\xi = \chi_0(g)$ and let

$$A := [\chi_0^j(g^i)]_{\substack{1 \le i \le r \\ 1 \le j \le r}} = [\xi^{ij}]_{\substack{1 \le i \le r \\ 1 \le j \le r}} \tag{2.4.7}$$

be the $r \times r$ symmetric matrix whose (i,j)-th entry is ξ^{ij}. It is clear that $\det A \neq 0$.

LEMMA 2.4.8. *Under the same notation as above, we have*

$$|L_1 : L_2| = |\pi(L_1) : \pi(L_2)| = |\mathfrak{o} : \det A \cdot \mathfrak{o}|.$$

PROOF. Since π gives an isomorphism $\mathrm{Eis}_2^{\infty}(F) \xrightarrow{\sim} F[C_\infty]^0$, the first equality is obvious.

On the other hand, we have $|L_1 : L_2| = |L_1' : \mathfrak{o}^r|$. Since $\sum_{a \in G} \chi_0^i(a) = 0$ for $1 \le i \le r$, we see that the condition (iii) above holds if we require the same condition only for $a \neq 1$. Thus the previous lemma shows that $L_1' = A^{-1}\mathfrak{o}^r$, from which our conclusion follows. □

We next turn to the computation of $|\mathfrak{o}[C_\infty]^0 : \pi(L_2)|$.

LEMMA 2.4.9. *Let the notation be as above. We have*

$$|\mathfrak{o}[C_\infty]^0 : \pi(L_2)| = |\mathfrak{o} : c(N) \det A \cdot \mathfrak{o}|.$$

PROOF. We can take

$$\{[g^{-i}]_\infty - [1]_\infty \mid 1 \le i \le r\}$$

as an $\mathfrak{o}$-basis of $\mathfrak{o}[C_\infty]^0$.

By Proposition 2.2.8, we have

$$\pi(E_{2,\chi_0^i}) = \big(-B_{2,\chi_0^i}/4\big)\sum_{a\in G}\chi_0^i(a)([a^{-1}]_\infty - [1]_\infty)$$

for $1 \le i \le r$. Therefore, if we denote by B the $r \times r$ diagonal matrix whose i-th diagonal entry is $-B_{2,\chi_0^i}/4$, we see that

$$\big(\pi(E_{2,\chi_0}),\dots,\pi(E_{2,\chi_0^r})\big) = \big([g^{-1}]_\infty - [1]_\infty,\dots,[g^{-r}]_\infty - [1]_\infty\big)AB$$

which shows that $|\mathfrak{o}[C_\infty]^0 : \pi(L_2)| = |\mathfrak{o} : \det(AB)\cdot\mathfrak{o}|$. Since $p \neq N$, our claim follows. □

We can now complete the proof of Theorem 2.4.2. By the definition (2.3.2) of the congruence module, we have $\mathfrak{C}_\mathfrak{o}^{\mathrm{mod}} = \mathfrak{o}[C_\infty]^0/\pi(L_1)$. Therefore we have

$$|\mathfrak{C}_\mathfrak{o}^{\mathrm{mod}}| = \frac{|\mathfrak{o}[C_\infty]^0 : \pi(L_2)|}{|\pi(L_1) : \pi(L_2)|} = \frac{|\mathfrak{o} : c(N)\det A\cdot\mathfrak{o}|}{|\mathfrak{o} : \det A\cdot\mathfrak{o}|} = |\mathfrak{o} : c(N)\mathfrak{o}|$$

by the previous two lemmas.

3. Rational torsion subgroups of modular Jacobians.

3.1. Annihilators of $J_1(N)(\mathbb{Q})_{\mathbf{tors}}$.

So far we worked with $X_\mu(N)_{/R}$. We now turn our attention to another model of the modular curve attached to $\Gamma_1(N)$. (We will come back to $X_\mu(N)_{/R}$ and $J_\mu(N)$ in the final subsection 3.4.)

As before, we fix a prime number $N \ge 5$. Let R be a $\mathbb{Z}[1/N]$-algebra. In the following, we denote by $X_1(N)_{/R}$ the moduli scheme classifying the pairs (E,β) as in (1.1.1), replacing α there by $\beta : \mathbb{Z}/N\mathbb{Z} \hookrightarrow E^{\mathrm{reg}}$. One can define the diamond operators $\langle a\rangle$ and the Hecke correspondences on $X_1(N)_{/R}$ exactly in the same manner as in 1.2, again replacing α by β. Over the ring $\mathbb{Z}[1/N,\zeta_N]$, there is an isomorphism of group schemes $\boldsymbol{\mu}_N \cong \mathbb{Z}/N\mathbb{Z}$, and if we fix such an isomorphism, it gives an isomorphism $X_\mu(N)_{/R} \cong X_1(N)_{/R}$ for each $\mathbb{Z}[1/N,\zeta_N]$-algebra R. The diamond operators and the Hecke correspondences on both sides may be identified through this isomorphism.

Let $J_1(N)_{/\mathbb{Q}} = J_1(N)$ be the Jacobian variety of $X_1(N)_{/\mathbb{Q}}$ defined over $\mathbb{Q}$. We denote by $J_1(N)_{/A}$ its Néron model over A when A is the ring of integers of a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$, or a localization of the former. We use similar notation for the Jacobian $J_0(N)_{/\mathbb{Q}} = J_0(N)$ of $X_0(N)_{/\mathbb{Q}}$. It is well-known that $J_1(N)_{/\mathbb{Z}[1/N]}$ and $J_0(N)_{/\mathbb{Z}[1/N]}$ are abelian schemes. The diamond operators and the Hecke correspondences act (covariantly, as before) on $J_1(N)_{/\mathbb{Q}}$ and hence on $J_1(N)_{/A}$, for which we use the same symbols $\langle a\rangle$ and $T(l)$ as in 1.2. We thus

obtain an embedding

$$h_2(\Gamma_1(N);\mathbb{Z}) \hookrightarrow \mathrm{End}_{\mathbb{Q}}(J_1(N)) = \mathrm{End}_{\mathbb{Z}}(J_1(N)_{/\mathbb{Z}}). \tag{3.1.1}$$

The purpose of this subsection is to prove the following

THEOREM 3.1.2. *Let p be a prime number different from 2 and N. Then the Eisenstein ideal $I_{\infty,\mathbb{Z}_p}$ of $h_2(\Gamma_1(N);\mathbb{Z}_p)$ (cf. Definition 2.1.12) annihilates $J_1(N)(\mathbb{Q})[p^\infty]$.*

Here, as before, "$[M]$" indicates the kernel of multiplication by M, and "$[p^\infty]$" means the union of the kernels of multiplication by p^n for all $n \geq 1$, for abelian groups, commutative group schemes, and p-divisible groups. Also, for any ideal $\mathfrak{a}$ of a commutative subring of the endomorphism algebra of such objects, we use the symbol "$[\mathfrak{a}]$" to denote the kernel of $\mathfrak{a}$.

We already know that $I_{\infty,\mathbb{Z}_p}$ is generated by $\eta(l)$ for prime numbers $l \neq N$ and τ (cf. (2.1.10) and (2.1.11)), by Corollary 2.1.14. Thus, to prove the theorem above, it is enough to show that these elements annihilate $J_1(N)(\mathbb{Q})[p^\infty]$. As for the first ones, this is a rather well-known fact which we review below. Let $\mathbb{Z}_{(l)}$ be the localization of $\mathbb{Z}$ at (l), and $\mathbb{F}_l = \mathbb{Z}/l\mathbb{Z}$ its residue field.

LEMMA 3.1.3. *Let p be as above. For any prime number $l \neq N$, $\eta(l)$ annihilates $J_1(N)(\mathbb{Q})[p^\infty]$.*

PROOF. The Eichler-Shimura congruence relation asserts that

$$T(l) = \mathrm{Frob}_l + \langle l\rangle \mathrm{Ver}_l$$

on $J_1(N)_{/\mathbb{F}_l} = J_1(N)_{/\mathbb{Z}_{(l)}} \otimes_{\mathbb{Z}_{(l)}} \mathbb{F}_l$, where Frob_l (resp. Ver_l) denotes the Frobenius endomorphism (resp. the Verschiebung).

On the other hand, the schematic closure of $J_1(N)(\mathbb{Q})[p^\infty]$ (considered as a finite constant subgroup scheme of $J_1(N)_{/\mathbb{Q}}$) in $J_1(N)_{/\mathbb{Z}_{(l)}}$ is an (étale) constant group scheme. This is well-known for $l \neq p$, and for $l = p$ this follows from Raynaud [**Ra**, Théorème 3.3.3] because $p > 2$.

It then follows that $T(l) = 1 + \langle l\rangle l$ on $J_1(N)(\mathbb{Q})[p^\infty]$. □

REMARK 3.1.4. The same argument shows that $\eta(l)$ also annihilates $J_1(N)(\mathbb{Q})[2^\infty]$ for l odd. The only (but serious) obstacle for $p = 2$ here lies in our ignorance of the annihilation by $\eta(2)$ of this group.

In contrast to this, the following argument will show that τ annihilates the whole $J_1(N)(\mathbb{Q})_{\mathrm{tors}}$. Let $\alpha : J_1(N) \to J_0(N)$ and $\pi : J_0(N) \to J_1(N)$ be the

natural (i.e. Albanese and Picard) morphisms.

LEMMA 3.1.5. *α annihilates $J_1(N)(\mathbb{Q})_{\mathrm{tors}}$:*

$$J_1(N)(\mathbb{Q})_{\mathrm{tors}} \subseteq \mathrm{Ker}(\alpha)(\mathbb{Q}).$$

PROOF. For the proof, we make use of two deep results, one due to Conrad, Edixhoven and Stein, and the other due to Mazur.

First, the main result (Theorem 1.1.1) of [**CES**] asserts that $J_1(N)_{/\mathbb{Z}} = J_1(N)^0_{/\mathbb{Z}}$, where the superscript "^{0}" means the "identity component" in the usual sense. Thus α induces homomorphisms

$$\begin{cases} J_1(N)_{/\mathbb{Z}} \to J_0(N)^0_{/\mathbb{Z}}, \\ J_1(N)(\mathbb{Q}) = J_1(N)_{/\mathbb{Z}}(\mathbb{Z}) \to J_0(N)^0_{/\mathbb{Z}}(\mathbb{Z}). \end{cases}$$

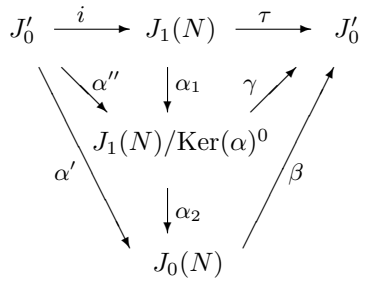
On the other hand, Mazur has constructed a retraction ρ of $M := J_0(N)(\mathbb{Q})$ to the cuspidal group C of $J_0(N)$, and also a direct product decomposition

$$M = M^0 \times C$$

where $M^0 = \mathrm{Ker}(\rho) = J_0(N)^0_{/\mathbb{Z}}(\mathbb{Z})$ ([**Ma**, II, (11.4)]). Then in the course of the proof of [**Ma**, III, Theorem (1.2)], Mazur proved that $M^0_{\mathrm{tors}} = \{0\}$. □

LEMMA 3.1.6. $\mathrm{Ker}(\alpha) \subseteq \mathrm{Ker}(\tau)$.

PROOF. Set $J_0' := \mathrm{Ker}(\langle g \rangle - 1)^0 \subseteq J_1(N)$, where g is a generator of the group G, and let $i : J_0' \to J_1(N)$ be the inclusion morphism. We are going to construct the following commutative diagram:



Here, α_1 is the quotient morphism, and α_2 is the unique isogeny such that $\alpha = \alpha_2 \circ \alpha_1$. Since J_0' is the maximal abelian subvariety of $J_1(N)$ on which G acts

trivially, $\alpha' := \alpha \circ i$ and $\alpha'' := \alpha_1 \circ i$ are isogenies.

It is clear that $(\langle g \rangle - 1) \circ \tau = 0$, and hence the endomorphism τ of $J_1(N)$ factors through $J_0' \overset{i}{\hookrightarrow} J_1(N)$. Let us denote by the same symbol τ the induced homomorphism $J_1(N) \to J_0'$. Then we see that $\alpha' \circ \tau = ((N-1)/2) \circ \alpha$. Since α' is an isogeny, we have

$$\mathrm{Ker}(\tau)^0 = \mathrm{Ker}(\alpha' \circ \tau)^0 = \mathrm{Ker}(((N-1)/2) \circ \alpha)^0 = \mathrm{Ker}(\alpha)^0.$$

It follow that τ factors as $\tau = \gamma \circ \alpha_1$ with a homomorphism $\gamma : J_1(N)/\mathrm{Ker}(\alpha)^0 \to J_0'$.

We have that $\alpha \circ \pi = (N-1)/2$, multiplication by the degree of the covering $X_1(N)_{/\mathbb{Q}} \to X_0(N)_{/\mathbb{Q}}$, and that π factors through an isogeny $J_0(N) \to J_0' \subseteq J_1(N)$. Thus if $x \in \mathrm{Ker}(\alpha')(\overline{\mathbb{Q}})$, there is an element $y \in J_0(N)(\overline{\mathbb{Q}})$ such that $x = \pi(y)$. Then the relation $\alpha'(x) = \alpha' \circ \pi(y) = 0$ implies that $y \in J_0(N)[(N-1)/2](\overline{\mathbb{Q}})$, and hence $x = \pi(y) \in J_0'[(N-1)/2](\overline{\mathbb{Q}})$. Consequently, we have $\tau(x) = 0$, showing that $\mathrm{Ker}(\alpha') \subseteq \mathrm{Ker}(\tau)$.

Thus, there is an isogeny $\beta : J_0(N) \to J_0'$ such that $\beta \circ \alpha' = \tau \circ i$, i.e. $\beta \circ \alpha_2 \circ \alpha'' = \gamma \circ \alpha''$. Since α'' is an isogeny, we conclude that $\beta \circ \alpha_2 = \gamma$. Therefore the above diagram commutes, and we have $\tau = \beta \circ \alpha$, from which our assertion follows. □

We have shown that τ annihilates $J_1(N)(\mathbb{Q})_{\mathrm{tors}}$. This, together with Lemma 3.1.3, completes the proof of Theorem 3.1.2.

3.2. 0-cuspidal group and the Eisenstein ideal.

As in 3.1, we fix a prime number p different from 2 and N. The Néron model $J_1(N)_{/\mathbb{Z}_p}$ is an abelian scheme over $\mathbb{Z}_p$, and hence we can consider the associated p-divisible group over $\mathbb{Z}_p$, which we denote by $\Gamma_{/\mathbb{Z}_p}$. Let $\Gamma_{/\mathbb{F}_p}$ be its closed fibre. We have the usual "connected-étale exact sequence"

$$0 \to \Gamma^0_{/\mathbb{Z}_p} \to \Gamma_{/\mathbb{Z}_p} \to \Gamma^{\text{ét}}_{/\mathbb{Z}_p} \to 0 \tag{3.2.1}$$

and its canonical splitting over $\mathbb{F}_p$

$$\Gamma_{/\mathbb{F}_p} = \Gamma^0_{/\mathbb{F}_p} \times \Gamma^{\text{ét}}_{/\mathbb{F}_p}. \tag{3.2.2}$$

The p-adic Hecke algebra $h_2(\Gamma_1(N); \mathbb{Z}_p)$ and $\mathbb{Z}_p[G]$ act on these p-divisible groups.

On the other hand, in our model $X_1(N)_{/\mathbb{Q}}$, the 0-cusps are rational over $\mathbb{Q}$, and the classes of divisors of degree zero supported at such cusps form a finite subgroup of $J_1(N)(\mathbb{Q})$. We denote this group by $\mathcal{C}_0$. Its order is given by Kubert

and Lang [**KL**, Chapter 6, Theorem 3.4], which seems originally due to Klimek:

$$|\mathcal{C}_0| = c(N). \tag{3.2.3}$$

We may consider $\mathcal{C}_0$ as a constant subgroup scheme of $J_1(N)$, and we denote by $\mathcal{C}_{0/\mathbb{Z}_p}$ (resp. $\mathcal{C}_{0/\mathbb{F}_p}$) its schematic closure in $J_1(N)_{/\mathbb{Z}_p}$ (resp. the closed fibre of $\mathcal{C}_{0/\mathbb{Z}_p}$). It is clear from (1.2.9) that all these group schemes are annihilated by $I_{\infty,\mathbb{Z}_p}$.

Our present aim is to prove the following theorem, which is an analogue of [**Wi**, Theorem 7.2].

THEOREM 3.2.4. *Let the notation and the assumption be as above. Then we have*

$$\mathcal{C}_{0/\mathbb{F}_p}[p^\infty] = \varGamma^{\text{ét}}_{/\mathbb{F}_p}[I_{\infty,\mathbb{Z}_p}].$$

To prove this theorem, we first note that, by Theorem 2.4.2 and (3.2.3), both group schemes in the theorem are trivial when $p \nmid c(N)$. We thus assume that $p \mid c(N)$, or equivalently, that $I_{\infty,\mathbb{Z}_p}$ is a proper ideal of $h_2(\varGamma_1(N);\mathbb{Z}_p)$, until we finish the proof.

Then since we have a surjective homomorphism

$$\mathbb{Z}_p[G] \twoheadrightarrow h_2(\varGamma_1(N);\mathbb{Z}_p)/I_{\infty,\mathbb{Z}_p}$$

a maximal ideal $\mathfrak{P}$ of $h_2(\varGamma_1(N);\mathbb{Z}_p)$ containing $I_{\infty,\mathbb{Z}_p}$ is generated by $I_{\infty,\mathbb{Z}_p}$ and the image of a maximal ideal of $\mathbb{Z}_p[G]$. The $I_{\infty,\mathbb{Z}_p}$-adic completion of $h_2(\varGamma_1(N);\mathbb{Z}_p)$ is a direct sum of the completions (or equivalently, the localizations) at such maximal ideals

$$h_2(\varGamma_1(N);\mathbb{Z}_p)_{I_{\infty,\mathbb{Z}_p}} = \bigoplus_{\mathfrak{P}\text{: as above}} h_2(\varGamma_1(N);\mathbb{Z}_p)_{\mathfrak{P}}. \tag{3.2.5}$$

Applying the idempotent $1_{\mathfrak{P}}$ of $h_2(\varGamma_1(N);\mathbb{Z}_p)$ corresponding to its direct factor $h_2(\varGamma_1(N);\mathbb{Z}_p)_{\mathfrak{P}}$, we obtain the "$\mathfrak{P}$-divisible group" $\varGamma_{\mathfrak{P}/\mathbb{Z}_p} := 1_{\mathfrak{P}} \cdot \varGamma_{/\mathbb{Z}_p}$, its connected part $\varGamma^0_{\mathfrak{P}/\mathbb{Z}_p}$, the étale quotient $\varGamma^{\text{ét}}_{\mathfrak{P}/\mathbb{Z}_p}$ over $\mathbb{Z}_p$, and their closed fibers $\varGamma_{\mathfrak{P}/\mathbb{F}_p}$, $\varGamma^0_{\mathfrak{P}/\mathbb{F}_p}$ and $\varGamma^{\text{ét}}_{\mathfrak{P}/\mathbb{F}_p}$. (3.2.1) and (3.2.2) hold with "$\varGamma$" replaced by "$\varGamma_{\mathfrak{P}}$". The algebra $h_2(\varGamma_1(N);\mathbb{Z}_p)_{\mathfrak{P}}$ acts on these $\mathfrak{P}$-divisible groups.

We now follow the argument of Mazur and Wiles [**MW1**, pp. 308–309] to prove Theorem 3.2.4. For this, we first have the following

LEMMA 3.2.6. *Put $\kappa(\mathfrak{P}) := h_2(\varGamma_1(N);\mathbb{Z}_p)/\mathfrak{P}$. Then the dimension of the $\kappa(\mathfrak{P})$-vector space $\varGamma^{\text{ét}}_{\mathfrak{P}/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[\mathfrak{P}]$ is at most one.*

PROOF. We have the well-known isomorphism of Cartier and Serre ([**Se**, Proposition 10])

$$J_1(N)_{/\mathbb{F}_p}[p](\overline{\mathbb{F}}_p) \xrightarrow{\sim} H^0\Big(X_1(N)_{/\overline{\mathbb{F}}_p}, \Omega^1_{/\overline{\mathbb{F}}_p}\Big)^{\mathcal{C}}$$

where $\mathcal{C}$ is the Cartier operator. This gives

$$\begin{aligned} J_1(N)_{/\mathbb{F}_p}[p](\overline{\mathbb{F}}_p) \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p &\xrightarrow{\sim} H^0\Big(X_1(N)_{/\overline{\mathbb{F}}_p}, \Omega^1_{/\overline{\mathbb{F}}_p}\Big)^{\mathcal{C}} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p \\ &\hookrightarrow H^0\Big(X_1(N)_{/\overline{\mathbb{F}}_p}, \Omega^1_{/\overline{\mathbb{F}}_p}\Big) = S_2\big(\Gamma_1(N); \overline{\mathbb{F}}_p\big) \end{aligned}$$

(cf. [**Ma**, II, Proposition (14.7)]; we have fixed an isomorphism $\mathbb{Z}/N\mathbb{Z} \cong \boldsymbol{\mu}_N$ at the last equality). The (covariant) action of $t \in h_2(\Gamma_1(N); \mathbb{Z}_p)$ on the left commutes with the covariant action of t, which coincides with the contravariant action (1.2.4) of $w_\zeta^{-1} \circ t \circ w_\zeta$ on the right (cf. [**Wi**, Section 6]).

Thus, further composing this with the automorphism w_ζ of $S_2(\Gamma_1(N); \overline{\mathbb{F}}_p)$, we obtain an injective $h_2(\Gamma_1(N); \mathbb{Z}_p)$-module homomorphism, which in turn gives an injection

$$\Gamma^{\text{ét}}_{\mathfrak{P}/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[\mathfrak{P}] \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p = J_1(N)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[\mathfrak{P}] \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p \hookrightarrow S_2\big(\Gamma_1(N); \overline{\mathbb{F}}_p\big)[\mathfrak{P}]$$

of $\kappa(\mathfrak{P}) \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$-modules. It is therefore enough to show that the last space, namely $S_2(\Gamma_1(N); \mathbb{F}_p)[\mathfrak{P}] \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ is a free module of rank one over $\kappa(\mathfrak{P}) \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$.

But from the duality in Remark 1.3.8, (2) for $R = \mathbb{F}_p$, we obtain a perfect pairing

$$S_2(\Gamma_1(N); \mathbb{F}_p)[\mathfrak{P}] \times h_2(\Gamma_1(N); \mathbb{F}_p)/\mathfrak{P} \to \mathbb{F}_p.$$

We conclude that $S_2(\Gamma_1(N); \mathbb{F}_p)[\mathfrak{P}]$ is isomorphic to $\mathrm{Hom}_{\mathbb{F}_p}(\kappa(\mathfrak{P}), \mathbb{F}_p)$ as a vector space over $\kappa(\mathfrak{P})$ which is clearly of dimension one, and our claim follows. □

PROOF OF THEOREM 3.2.4. By Raynaud's theorem, $\mathcal{C}_{0/\mathbb{Z}_p}[p^\infty]$ and $\mathcal{C}_{0/\mathbb{F}_p}[p^\infty]$ are constant group schemes, and hence the latter is contained in $\Gamma^{\text{ét}}_{/\mathbb{F}_p}[I_{\infty,\mathbb{Z}_p}]$. To prove the theorem, we need to show that the inclusion

$$\mathcal{C}_{0/\mathbb{F}_p}[p^\infty](\overline{\mathbb{F}}_p) \subseteq \Gamma^{\text{ét}}_{/\mathbb{F}_p}[I_{\infty,\mathbb{Z}_p}](\overline{\mathbb{F}}_p)$$

is an equality. These groups are modules over $h_2(\Gamma_1(N); \mathbb{Z}_p)_{I_{\infty,\mathbb{Z}_p}}$. According to the direct sum decomposition (3.2.5), we have the decomposition

$$\Gamma^{\text{ét}}_{/\mathbb{F}_p}[I_{\infty,\mathbb{Z}_p}](\overline{\mathbb{F}}_p) = \bigoplus_{\mathfrak{P}} \Gamma^{\text{ét}}_{\mathfrak{P}/\mathbb{F}_p}[I_{\infty,\mathbb{Z}_p}](\overline{\mathbb{F}}_p).$$

Now let us indicate by "$\widehat{\ }$" the Pontrjagin dual. Then we have

$$\Gamma^{\text{ét}}_{\mathfrak{P}/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[\mathfrak{P}]\widehat{\ } \cong \Gamma^{\text{ét}}_{\mathfrak{P}/\mathbb{F}_p}(\overline{\mathbb{F}}_p)\widehat{\ }/\mathfrak{P} \cdot \Gamma^{\text{ét}}_{\mathfrak{P}/\mathbb{F}_p}(\overline{\mathbb{F}}_p)\widehat{\ }.$$

By the previous lemma, this is a $\kappa(\mathfrak{P})$-vector space of dimension at most one. Nakayama's lemma implies that $(\Gamma^{\text{ét}}_{\mathfrak{P}/\mathbb{F}_p}(\overline{\mathbb{F}}_p))\widehat{\ }$ is a cyclic module over $h_2(\Gamma_1(N); \mathbb{Z}_p)_{\mathfrak{P}}$. It follows that

$$\Gamma^{\text{ét}}_{\mathfrak{P}/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[I_{\infty,\mathbb{Z}_p}]\widehat{\ } \cong \Gamma^{\text{ét}}_{\mathfrak{P}/\mathbb{F}_p}(\overline{\mathbb{F}}_p)\widehat{\ }/I_{\infty,\mathbb{Z}_p} \cdot \Gamma^{\text{ét}}_{\mathfrak{P}/\mathbb{F}_p}(\overline{\mathbb{F}}_p)\widehat{\ }$$

is also a cyclic $h_2(\Gamma_1(N); \mathbb{Z}_p)_{\mathfrak{P}}$-module whose order is less than or equal to $|h_2(\Gamma_1(N); \mathbb{Z}_p)_{\mathfrak{P}} : I_{\infty,\mathbb{Z}_p} h_2(\Gamma_1(N); \mathbb{Z}_p)_{\mathfrak{P}}|$. Since this holds for all $\mathfrak{P}$ figuring in (3.2.5), we conclude that

$$\left|\Gamma^{\text{ét}}_{/\mathbb{F}_p}[I_{\infty,\mathbb{Z}_p}](\overline{\mathbb{F}}_p)\right| \leq \left|h_2(\Gamma_1(N); \mathbb{Z}_p) : I_{\infty,\mathbb{Z}_p}\right|.$$

This, the main result Theorem 2.4.2 of the previous section, and (3.2.3) show that

$$\left|\Gamma^{\text{ét}}_{/\mathbb{F}_p}[I_{\infty,\mathbb{Z}_p}](\overline{\mathbb{F}}_p)\right| \leq \left|\mathcal{C}_{0/\mathbb{F}_p}[p^\infty](\overline{\mathbb{F}}_p)\right|.$$

This completes the proof of Theorem 3.2.4. □

It is now an easy matter to prove Theorem I in the introduction for the p-primary part of $J_1(N)(\mathbb{Q})_{\text{tors}}$ $(p \neq 2, N)$. Indeed, the schematic closure of $J_1(N)(\mathbb{Q})[p^\infty]$ in $J_1(N)_{/\mathbb{Z}_p}$ is constant, and it is annihilated by $I_{\infty,\mathbb{Z}_p}$ by Theorem 3.1.2. We therefore have

$$J_1(N)(\mathbb{Q})[p^\infty] \hookrightarrow \Gamma^{\text{ét}}_{/\mathbb{F}_p}[I_{\infty,\mathbb{Z}_p}](\mathbb{F}_p) = \mathcal{C}_{0/\mathbb{F}_p}[p^\infty](\mathbb{F}_p)$$

by Theorem 3.2.4, whence the equality

$$J_1(N)(\mathbb{Q})[p^\infty] = \mathcal{C}_0[p^\infty].$$

We close this subsection with another application of Theorem 2.4.2.

PROPOSITION 3.2.7. *$I_{\infty,\mathbb{Z}_p}$ is the annihilator ideal of $\mathcal{C}_0[p^\infty]$ in $h_2(\Gamma_1(N); \mathbb{Z}_p)$.*

PROOF. First note that $\mathcal{C}_0$ is a cyclic module over $h_2(\Gamma_1(N);\mathbb{Z})$. In fact, the degree zero part of the free abelian group on the set of 0-cusps, of which $\mathcal{C}_0$ is a quotient, is a cyclic module over $\mathbb{Z}[G]$ (cf. (1.2.9)).

Thus fixing a generator, we have a surjective homomorphism of $h_2(\Gamma_1(N);\mathbb{Z}_p)$-modules

$$h_2(\Gamma_1(N);\mathbb{Z}_p)/I_{\infty,\mathbb{Z}_p} \twoheadrightarrow \mathcal{C}_0[p^\infty].$$

By Theorem 2.4.2 and (3.2.3), this is an isomorphism. □

3.3. *N*-torsion part.

Recall that the natural homomorphisms $\alpha : J_1(N) \to J_0(N)$ and $\pi : J_0(N) \to J_1(N)$ satisfy $\alpha \circ \pi = (N-1)/2$. Set

$$A_{/\mathbb{Q}} = A := J_1(N)/\pi(J_0(N)). \tag{3.3.1}$$

α and the quotient morphism induce a homomorphism $\lambda : J_1(N) \to J_0(N) \times A$, and the above relation shows that $\mathrm{Ker}(\lambda) \subseteq J_1(N)[(N-1)/2]$. Hence there is an isogeny $\mu : J_0(N) \times A \to J_1(N)$ such that $\mu \circ \lambda = (N-1)/2$. It follows that λ induces an isomorphism

$$J_1(N)[N^\infty] \xrightarrow{\sim} J_0(N)[N^\infty] \times A[N^\infty]. \tag{3.3.2}$$

By [**Ma**, III, Theorem (1.2)], $J_0(N)[N^\infty](\mathbb{Q}) = \{0\}$, and we have

$$J_1(N)[N^\infty](\mathbb{Q}) \cong A[N^\infty](\mathbb{Q}). \tag{3.3.3}$$

On the other hand, $\langle a \rangle$ and $T(l)$ on $J_1(N)$ induce endomorphisms of A, which we denote by the same symbols. We let $h_2(\Gamma_1(N);\mathbb{Z})_A$ be the subalgebra of $\mathrm{End}_{\mathbb{Q}}(A)$ generated by these endomorphisms and set

$$h_2(\Gamma_1(N);R)_A := h_2(\Gamma_1(N);\mathbb{Z})_A \otimes_{\mathbb{Z}} R \tag{3.3.4}$$

for any ring R. Let $I_{A,R}$ be the image of $I_{\infty,R}$ under the natural homomorphism $h_2(\Gamma_1(N);R) \twoheadrightarrow h_2(\Gamma_1(N);R)_A$. Since the image of τ in $h_2(\Gamma_1(N);R)_A$ is zero, $I_{A,R}$ is in fact the "naive Eisenstein ideal":

$$I_{A,R} = (\eta(l) \text{ (for primes } l \neq N),\ T(N) - 1) \subseteq h_2(\Gamma_1(N);R)_A. \tag{3.3.5}$$

We remark here that the above argument equally applies to prime numbers not dividing $(N-1)/2$, instead of N. In this sense, to treat the rational p-torsion

subgroup of $J_1(N)$, the introduction of τ in the ideal $I_{\infty,R}$ was necessary only for a finite number of, but troublesome, primes p dividing $(N-1)/2$.

Now the group $\widehat{G}$, if we consider it as the set of $\overline{\mathbb{Q}}_N^\times$-valued characters, has a canonical generator ω^2, the square of the Teichmüller character taking values in $\mathbb{Z}_N^\times$. According to the action of $\mathbb{Z}_N[G]$, we have the direct sum decomposition

$$\begin{cases} h_2(\Gamma_1(N);\mathbb{Z}_N) = \oplus_{i=0}^{N-3} h_2(\Gamma_1(N);\mathbb{Z}_N)^{(i)} \supseteq \oplus_{i=0}^{N-3} I_{\infty,\mathbb{Z}_N}^{(i)}, \\ h_2(\Gamma_1(N);\mathbb{Z}_N)_A = \oplus_{i=2}^{N-3} h_2(\Gamma_1(N);\mathbb{Z}_N)^{(i)} \supseteq \oplus_{i=2}^{N-3} I_{\infty,\mathbb{Z}_N}^{(i)} = I_{A,\mathbb{Z}_N} \end{cases} \tag{3.3.6}$$

(the sum being over even i) of Hecke algebras and their ideals, and also the decomposition of abelian groups

$$\begin{cases} J_1(N)[N^\infty](\mathbb{Q}) = \oplus_{i=0}^{N-3} J_1(N)[N^\infty](\mathbb{Q})^{(i)}, \\ A[N^\infty](\mathbb{Q}) = \oplus_{i=2}^{N-3} A[N^\infty](\mathbb{Q})^{(i)} = \oplus_{i=2}^{N-3} J_1(N)[N^\infty](\mathbb{Q})^{(i)}. \end{cases} \tag{3.3.7}$$

Here, we used the superscript "$^{(i)}$" to denote the eigenspace on which G acts via the character ω^i. Thus $I_{\infty,\mathbb{Z}_N}^{(i)}$ is the ideal generated by $T(l)-(1+l\omega^i(l))$ for prime numbers $l \neq N$, and $T(N)-1$ for $i \not\equiv 0 \bmod (N-1)$.

Also, for an N-divisible group on which $G = \langle g \rangle$ acts, we use the superscript "$^{(i)}$" to mean the kernel of (the action of g)$-\omega^i(g)$. We clearly have $A[N^\infty](\mathbb{Q})^{(i)} = A[N^\infty]^{(i)}(\mathbb{Q})$ etc.

We have already seen that $J_1(N)[N^\infty](\mathbb{Q})^{(0)} = \{0\}$, and hence we turn our attention to $J_1(N)[N^\infty](\mathbb{Q})^{(i)} = A[N^\infty](\mathbb{Q})^{(i)}$ for $i \not\equiv 0 \bmod (N-1)$.

Let K be the the completion of $\mathbb{Q}(\zeta_N)^+$ at its unique prime above N, and $\mathfrak{o}$ the ring of integers of K. The Néron model $A_{/\mathfrak{o}}$ of A over $\mathfrak{o}$ is an abelian scheme. Let $A_{/\mathbb{F}_N}$ be its closed fibre.

PROPOSITION 3.3.8. *For each even integer $i \not\equiv 0 \bmod (N-1)$, $I_{\infty,\mathbb{Z}_N}^{(i)}$ annihilates $A[N^\infty](\mathbb{Q})^{(i)}$.*

PROOF. It follows from the Eichler-Shimura congruence relation that $T(l)-(1+l\omega^i(l))$ annihilates $A[N^\infty](\mathbb{Q})^{(i)}$ for prime numbers $l \neq N$, for the same reason as Lemma 3.1.3. So, it remains to show that $T(N)-1$ annihilates this group.[†]

[†]In [**Kam2**, Lemma 2.2], it is claimed that there is no element of $M_2(\Gamma_1(N);\mathbb{F}_N)^{(i)}$ ($i \not\equiv -2 \bmod (N-1)$) whose q-expansion is a non-zero power series in q^N, which will imply that $I_{\infty,\mathbb{Z}_N}^{(i)}$ can be generated without $T(N)-1$. However, the proof given there seems incomplete. (The reduction modulo N of Serre's N-adic modular forms of weight $(2,k+2) \in \mathbb{Z}_N \times \mathbb{Z}/(N-1)\mathbb{Z}$ contains many non-zero power series in q^N.) We thus prove this assertion and Lemma 3.3.9 directly, and deduce Theorem 3.3.13 and Theorem I for N from these.

Let K and $\mathfrak{o}$ be as above. Again by Raynaud's theorem, the schematic closure of $A[N^\infty](\mathbb{Q})$ in $A_{/\mathfrak{o}}$ is constant. The reduction modulo N mapping, i.e. the composite of

$$A[N^\infty](\mathbb{Q}) \hookrightarrow A_{/\mathfrak{o}}(\mathfrak{o}) \to A_{/\mathbb{F}_N}(\mathbb{F}_N)$$

is thus injective.

Take a point $P \in A[N^\infty](\mathbb{Q})^{(i)}$, and consider it as a section of $A_{/K}$ over K. For $\gamma \in \mathrm{Gal}(K/\mathbb{Q}_N)$, we clearly have the commutative square

$$\begin{array}{ccc} A_{/K} & \xrightarrow{[\gamma]} & A_{/K} \\ {\scriptstyle P}\uparrow & & \uparrow{\scriptstyle P} \\ \mathrm{Spec}(K) & \xrightarrow[\mathrm{Spec}(\gamma)]{} & \mathrm{Spec}(K) \end{array}$$

where $[\gamma] = \mathrm{id} \times \mathrm{Spec}(\gamma)$. This diagram uniquely extends to a diagram over $\mathfrak{o}$, replacing K and $A_{/K}$ by $\mathfrak{o}$ and $A_{/\mathfrak{o}}$, respectively. Then passing to the closed fibre, we obtain the commutative square

$$\begin{array}{ccc} A_{/\mathbb{F}_N} & \xrightarrow{[\gamma]_0} & A_{/\mathbb{F}_N} \\ {\scriptstyle P_0}\uparrow & & \uparrow{\scriptstyle P_0} \\ \mathrm{Spec}(\mathbb{F}_N) & \xrightarrow[\mathrm{id}]{} & \mathrm{Spec}(\mathbb{F}_N). \end{array}$$

Here, P_0 is the image of P under the reduction mapping, and $[\gamma]_0$ is the "geometric inertia group action" (which is inverse to the one in [**MW2**]).

We now invoke results due to Mazur and Wiles. Using the notation of [**MW1**, Chapter 3, Section 2], we have an isogeny

$$\sigma : \mathrm{Pic}^0\big(\tilde{\Sigma}_1^{\text{ét}}\big) \times \mathrm{Pic}^0\big(\tilde{\Sigma}_1^{\mu}\big) \to A_{/\mathbb{F}_N}$$

where $\tilde{\Sigma}_1^{\text{ét}}$ and $\tilde{\Sigma}_1^{\mu}$ are isomorphic to the Igusa curve of level N. We have two commutative squares

$$\begin{array}{ccc} \mathrm{Pic}^0(\tilde{\Sigma}_1^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_1^{\mu}) & \xrightarrow{\sigma} & A_{/\mathbb{F}_N} \\ {\scriptstyle \mathrm{id}}\downarrow{\scriptstyle \times\langle a_\gamma\rangle^{-1}} & & \downarrow{\scriptstyle [\gamma]_0} \\ \mathrm{Pic}^0(\tilde{\Sigma}_1^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_1^{\mu}) & \xrightarrow{\sigma} & A_{/\mathbb{F}_N}, \end{array} \qquad \begin{array}{ccc} \mathrm{Pic}^0(\tilde{\Sigma}_1^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_1^{\mu}) & \xrightarrow{\sigma} & A_{/\mathbb{F}_N} \\ {\scriptstyle \mathrm{Frob}}\downarrow{\scriptstyle \times\mathrm{Ver}} & & \downarrow{\scriptstyle T(N)} \\ \mathrm{Pic}^0(\tilde{\Sigma}_1^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_1^{\mu}) & \xrightarrow{\sigma} & A_{/\mathbb{F}_N} \end{array}$$

([**MW1**, Chapter 3, Section 3, Proposition 2], [**MW2**, Section 3]). In the first diagram, $a_\gamma \in G$ satisfies $\gamma(\zeta_N + \zeta_N^{-1}) = \zeta_N^{a_\gamma} + \zeta_N^{-a_\gamma}$, and $\langle a_\gamma\rangle^{-1}$ on $\mathrm{Pic}^0(\tilde{\Sigma}_1^\mu)$ commutes with $\langle a_\gamma\rangle^{-1}$ on $A_{/\mathbb{F}_N}$ through $\mathrm{Pic}^0(\tilde{\Sigma}_1^\mu) \hookrightarrow \mathrm{Pic}^0(\tilde{\Sigma}_1^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_1^\mu)$ and σ. Moreover, σ induces an isomorphism for the associated N-divisible groups ([**MW1**, Chapter 3, Section 2, Proposition 4]). Therefore, if P_0 corresponds to $(P_1, P_2) \in (\mathrm{Pic}^0(\tilde{\Sigma}_1^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_1^\mu))[N^\infty](\mathbb{F}_N)$, we see from the first diagram above that $P_2 = \omega^{-i}(a_\gamma)P_2$, and hence $P_2 = 0$. The second diagram then shows that $T(N) - 1$ annihilates P_0. This completes the proof. □

LEMMA 3.3.9. (1) $h_2(\Gamma_1(N); \mathbb{Z}_N)^{(-2)}/I_{\infty,\mathbb{Z}_N}^{(-2)} = \{0\}$, *and*
(2) $h_2(\Gamma_1(N); \mathbb{Z}_N)^{(i)}/I_{\infty,\mathbb{Z}_N}^{(i)} \cong \mathbb{Z}_N/B_{2,\omega^i}\mathbb{Z}_N$ *for even* $i \not\equiv 0, -2 \bmod (N-1)$.

PROOF. This is a special(ized) case of the main result of [**Oh1**]. Let $\Lambda_{\mathbb{Z}_N}$ be the Iwasawa algebra over $\mathbb{Z}_N$, i.e. the completed group algebra over $\mathbb{Z}_N$ of the multiplicative group $1 + N\mathbb{Z}_N$. As usual, we fix a topological generator u_0 of $1+N\mathbb{Z}_N$, and identify $\Lambda_{\mathbb{Z}_N}$ with the power series ring $\mathbb{Z}_N[[T]]$ via $u_0 \leftrightarrow 1+T$. Now replacing N and p in [**Oh1**] by 1 and N, and taking $\theta = \omega^i$ with even $i \not\equiv 0 \bmod (N-1)$ and $\psi = \mathbf{1}$, we have the following objects:

- Hida's universal ordinary N-adic Hecke algebras $e\,\mathcal{H}(1; \mathbb{Z}_N)$ and $e\,h(1; \mathbb{Z}_N)$ attached to modular forms and cusp forms, which are finite flat $\Lambda_{\mathbb{Z}_N}$-algebras;
- The Eisenstein ideal $\mathcal{I} = \mathcal{I}(\omega^i, \mathbf{1})$ of $e\,\mathcal{H}(1; \mathbb{Z}_N)$ and its image $I = I(\omega^i, \mathbf{1})$ in $e\,h(1; \mathbb{Z}_N)$;
- The Eisenstein maximal ideal $\mathfrak{M} = \mathfrak{M}(\omega^i, \mathbf{1}) = (\mathcal{I}, N, T)$ of $e\,\mathcal{H}(1; \mathbb{Z}_N)$.

Then, indicating by the subscript "$\mathfrak{m}$" the localization at $\mathfrak{M}$ for any $e\,\mathcal{H}(1; \mathbb{Z}_N)$-module, we have shown in [**Oh1**, (1.5.5) and the remark after (3.2.4)] that

$$e\,h(1; \mathbb{Z}_N)_{\mathfrak{M}}/I_{\mathfrak{M}} \cong \begin{cases} \{0\} \text{ if } i \equiv -2 \bmod (N-1), \\ \Lambda_{\mathbb{Z}_N}/(G(T, \omega^{i+2})) \text{ otherwise} \end{cases}$$

(cf. [**Oh2**, Section 1] for a simplification of the proof). Here, $G(T, \omega^{i+2}) \in \Lambda_{\mathbb{Z}_N}$ satisfies

$$G(u_0^s - 1, \omega^{i+2}) = L_N(-1-s, \omega^{i+2})$$

the right hand side being the Kubota-Leopoldt N-adic L-function.

Let M be the maximal ideal of $H_2(\Gamma_1(N); \mathbb{Z}_N)^{(i)}$ generated by $T(l) - (1 + l\omega^i(l))$ $(l \neq N)$, $T(N) - 1$ and N. Then, via the specialization to weight 2, we

have a canonical isomorphism $e\,h(1;\mathbb{Z}_N)_{\mathfrak{M}}/T\cdot e\,h(1;\mathbb{Z}_N)_{\mathfrak{M}} \cong h_2(\Gamma_1(N);\mathbb{Z}_N)^{(i)}_M$, and the image of $I_{\mathfrak{M}}$ to the ring in the right hand side is $(I^{(i)}_{\infty,\mathbb{Z}_N})_M$. Consequently, we have

$$h_2(\Gamma_1(N);\mathbb{Z}_N)^{(i)}_M/(I^{(i)}_{\infty,\mathbb{Z}_N})_M \cong \begin{cases} 0 \text{ if } i \equiv -2 \bmod\ (N-1), \\ \mathbb{Z}_N/B_{2,\omega^i}\mathbb{Z}_N \text{ otherwise.} \end{cases}$$

If $I^{(i)}_{\infty,\mathbb{Z}_N} = h_2(\Gamma_1(N);\mathbb{Z}_N)^{(i)}$, our conclusion is obvious. Otherwise, the image of M in $h_2(\Gamma_1(N);\mathbb{Z}_N)^{(i)}$ is the unique maximal ideal containing $I^{(i)}_{\infty,\mathbb{Z}_N}$, and hence the left hand side above coincides with $h_2(\Gamma_1(N);\mathbb{Z}_N)^{(i)}/I^{(i)}_{\infty,\mathbb{Z}_N}$. □

The following corollary is in accordance with the fact that $NB_{2,\omega^{-2}} \in \mathbb{Z}_N^{\times}$.

Corollary 3.3.10. *$A[N^\infty](\mathbb{Q})^{(-2)}$ is trivial.*

Proof. This follows from Proposition 3.3.8 and Lemma 3.3.9 immediately. □

One can also decompose $\mathcal{C}_0[N^\infty] \subseteq J_1(N)[N^\infty](\mathbb{Q})$ in the same manner as (3.3.7),

$$\mathcal{C}_0[N^\infty] = \oplus_{i=0}^{N-3}\mathcal{C}_0[N^\infty]^{(i)}. \tag{3.3.11}$$

Kubert and Lang [**KL**, Chapter 6, Theorem 2.1] have shown that

$$\mathcal{C}_0[N^\infty]^{(i)} \cong \mathbb{Z}_N/B_{2,\omega^i}\mathbb{Z}_N \quad \text{for } i \not\equiv 0, -2 \bmod\ (N-1). \tag{3.3.12}$$

The quotient homomorphism $J_1(N) \to A$ is injective on $\mathcal{C}_0[N^\infty]^{(i)}$ for $i \not\equiv 0 \bmod (N-1)$, and we use the symbol $\mathcal{C}_0[N^\infty]^{(i)}_A$ to denote its image. Let $\mathcal{C}_0[N^\infty]^{(i)}_{A/\mathfrak{o}}$ be the schematic closure of $\mathcal{C}_0[N^\infty]^{(i)}_A$ in $A_{/\mathfrak{o}}$, which is a constant group scheme. Let $\mathcal{C}_0[N^\infty]^{(i)}_{A/\mathbb{F}_N}$ be its closed fibre.

Theorem 3.3.13 (cf. [**Wi**, Theorem 7.2], [**Kam2**, Proposition 2.4]). *We have*

$$\mathcal{C}_0[N^\infty]^{(i)}_{A/\mathbb{F}_N} = (A_{/\mathbb{F}_N}[N^\infty]^{(i)})^{\text{ét}}\big[I^{(i)}_{\infty,\mathbb{Z}_N}\big]$$

for even $i \not\equiv 0 \bmod\ (N-1)$.

PROOF. For $i \equiv -2 \bmod (N-1)$, this follows from Lemma 3.3.9, (1). Assume that $i \not\equiv 0, -2 \bmod (N-1)$. By Lemma 3.3.9, (2) and (3.3.12), it is sufficient to show that $(A_{/\mathbb{F}_N}[N^\infty]^{(i)})^{\text{ét}}[I^{(i)}_{\infty,\mathbb{Z}_N}](\overline{\mathbb{F}}_N)$ is a cyclic group, or equivalently that $A_{/\mathbb{F}_N}[N](\overline{\mathbb{F}}_N)^{(i)}[I^{(i)}_{\infty,\mathbb{Z}_N}]$ is cyclic. By [**MW1**, Chapter 3, Section 2, Proposition 4], which we have already quoted in the proof of Proposition 3.3.8, this is in turn equivalent to the cyclicity of $(\mathrm{Pic}^0(\tilde{\Sigma}_1^{\text{ét}}) \times \mathrm{Pic}^0(\tilde{\Sigma}_1^{\mu}))[N](\overline{\mathbb{F}}_N)^{(i)}[I^{(i)}_{\infty,\mathbb{Z}_N}]$. This is a special case of [**MW1**, Chapter 3, Section 3, Proposition 4′]. □

We can now complete the proof of Theorem I in the introduction. For the p-torsion part with $p \neq 2, N$, it was already done in 3.2. As for the N-torsion part, we know that $J_1(N)(\mathbb{Q})[N^\infty]^{(0)} = \mathcal{C}_0[N^\infty]^{(0)} = \{0\}$, and hence it remains to show that $J_1(N)(\mathbb{Q})[N^\infty]^{(i)} = A[N^\infty]^{(i)}(\mathbb{Q}) = \mathcal{C}_0[N^\infty]^{(i)}$ when $i \not\equiv 0 \bmod (N-1)$. In this case, by Proposition 3.3.8, the reduction modulo N mapping considered in its proof gives us an injection

$$A[N^\infty]^{(i)}(\mathbb{Q}) \hookrightarrow (A_{/\mathbb{F}_N}[N^\infty]^{(i)})^{\text{ét}}\big[I^{(i)}_{\infty,\mathbb{Z}_N}\big](\mathbb{F}_N)$$

and hence our conclusion follows from Theorem 3.3.13.

Theorem II in the introduction is also plain from our preceding arguments. For $p \neq 2, N$, it was established in Theorems 2.4.2 and 3.1.2. For $p = N$, the index $|h_2(\Gamma_1(N); \mathbb{Z}_N) : I_{\infty,\mathbb{Z}_N}|$ is the product of $|h_2(\Gamma_1(N); \mathbb{Z}_N)^{(i)} : I^{(i)}_{\infty,\mathbb{Z}_N}| =: \mathrm{Ind}^{(i)}$ for even i in the range $0 \leq i \leq N-3$. If $i = 0$, the image of τ in $I^{(0)}_{\infty,\mathbb{Z}_N}$ is $(N-1)/2 \in \mathbb{Z}_N^\times$, and hence $\mathrm{Ind}^{(0)} = 1$. If $i = N-3$, we have seen in Lemma 3.3.9, (1) that $\mathrm{Ind}^{(N-3)} = 1 = |\mathbb{Z}_N : NB_{2,\omega^{N-3}}\mathbb{Z}_N|$. For other i, we have $\mathrm{Ind}^{(i)} = |\mathbb{Z}_N : B_{2,\omega^i}\mathbb{Z}_N|$ by Lemma 3.3.9, (2). Combining these, we obtain the first part. Since $J_1(N)(\mathbb{Q})[N^\infty]^{(0)} = \{0\}$, the second part follows from Proposition 3.3.8. This completes the proof of Theorem II. For the same reason as Proposition 3.2.7, we also see that $I_{\infty,\mathbb{Z}_N}$ is the annihilator ideal of $\mathcal{C}_0[N^\infty]$ in $h_2(\Gamma_1(N); \mathbb{Z}_N)$.

3.4. Related remarks.

We consider here the modular curve $X_\mu(N)_{/\mathbb{Q}}$ and its Jacobian variety $J_\mu(N)_{/\mathbb{Q}} = J_\mu(N)$ defined over $\mathbb{Q}$ as in Section 1. The ∞-cusps of $X_\mu(N)_{/\mathbb{Q}}$ are rational over $\mathbb{Q}$, and we can consider the subgroup $\mathcal{C}_\infty \subseteq J_\mu(N)(\mathbb{Q})$, the classes of divisors of degree zero supported at these cusps. Its order is $c(N)$ since the automorphism w_ζ of $X_\mu(N)_{/\mathbb{Q}(\zeta)}$ interchanges 0-cusps and ∞-cusps (cf. (1.2.9)). The following theorem is a simple consequence of this fact and Theorem I.

THEOREM 3.4.1. *For any odd prime p, we have*

$$J_\mu(N)(\mathbb{Q})[p^\infty] = \mathcal{C}_\infty[p^\infty].$$

PROOF. As a curve over $\mathbb{Q}$, $X_\mu(N)_{/\mathbb{Q}}$ is isomorphic to $X_1(N)_{/\mathbb{Q}}$ (cf. [**G**, p. 465]; the isomorphism in fact interchanges 0-cusps and ∞-cusps). Therefore the abelian varieties $J_\mu(N)$ and $J_1(N)$ are isomorphic over $\mathbb{Q}$, and their rational torsion subgroups have the same order. □

We finally consider the Eisenstein ideal related to $J_\mu(N)(\mathbb{Q})_{\mathrm{tors}}$. Recall that the correspondence $t \mapsto w_\zeta^{-1} \circ t \circ w_\zeta =: t^*$ gives an involutive automorphism of $\mathrm{End}(J_\mu(N)_{/\mathbb{Q}(\zeta)^+})$. When $t \in h_2(\Gamma_1(N); \mathbb{Z})$, t^* coincides with the image of t under the Rosati involution, and is defined over $\mathbb{Q}$. Let $h_2^*(\Gamma_1(N); \mathbb{Z})$ and $I_{\infty,\mathbb{Z}}^*$ be the images of $h_2(\Gamma_1(N); \mathbb{Z})$ and $I_{\infty,\mathbb{Z}}$ under this involution, respectively. Thus $I_{\infty,\mathbb{Z}}^*$ is the ideal generated by $T(l)^* - (1 + l\langle l\rangle^*) (= (T(l) - (l + \langle l\rangle)) \circ \langle l\rangle^{-1}$; cf. (1.2.7)) with prime numbers $l \neq N$, $T(N)^* - 1$ and $\tau^* = \tau$. Set

$$\begin{cases} h_2^*(\Gamma_1(N); \mathbb{Z}_p) := h_2^*(\Gamma_1(N); \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p, \\ I_{\infty,\mathbb{Z}_p}^* := I_{\infty,\mathbb{Z}}^* \cdot h_2^*(\Gamma_1(N); \mathbb{Z}_p). \end{cases} \tag{3.4.2}$$

The following theorem corresponds to Theorem II.

THEOREM 3.4.3. *With the same notation as above, let p be an odd prime number.*

(1) $|h_2^*(\Gamma_1(N); \mathbb{Z}_p) : I_{\infty,\mathbb{Z}_p}^*| = |\mathbb{Z}_p : c(N)\mathbb{Z}_p|$.

(2) $I_{\infty,\mathbb{Z}_p}^*$ *annihilates* $J_\mu(N)(\mathbb{Q})[p^\infty]$.

PROOF. The first assertion follows immediately from Theorem II, (1). The second assertion follows from Theorem 3.4.1 simply because $I_{\infty,\mathbb{Z}_p}^*$ annihilates $\mathcal{C}_\infty[p^\infty]$. □

References

[CES] B. Conrad, B. Edixhoven and W. Stein, $J_1(p)$ has connected fibers, Doc. Math., **8** (2003), 331–408.

[DR] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques, In: Modular Functions of One Variable, II, Antwerp, 1972, (eds. P. Deligne and W. Kuyk), Lecture Notes in Math., **349**, Springer-Verlag, Berline, 1973, pp. 143–316.

[DI] F. Diamond and J. Im, Modular forms and modular curves, In: Seminar on Fermat's Last Theorem, (ed. V. Kumar Murty), CMS Conf. Proc., **17**, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133.

[G] B. H. Gross, A tameness criterion for Galois representations associated to modular forms (mod p), Duke Math. J., **61** (1990), 445–517.

[EGAIII] A. Grothendieck, Éléments de géométrie algébrique. III, rédigés avec la collaboration de J. Dieudonné, Inst. Hautes Études Sci. Publ. Math., **11** (1961).

[Kam1] S. Kamienny, Rational points on modular curves and abelian varieties, J. Reine

Angew. Math., **359** (1985), 174–187.
[Kam2] S. Kamienny, On $J_1(p)$ and the kernel of the Eisenstein ideal, J. Reine Angew. Math., **404** (1990), 203–208.
[Kam3] S. Kamienny, On torsion in $J_1(N)$, Acta Arith., **120** (2005), 185–190.
[Kat1] N. M. Katz, p-adic properties of modular schemes and modular forms, In: Modular Functions of One Variable, III, Antwerp, 1972, (eds. W. Kuyk and J.-P. Serre), Lecture Notes in Math., **350**, Springer-Verlag, Berline, 1973, pp. 69–190.
[Kat2] N. M. Katz, p-adic interpolation of real analytic Eisenstein series, Ann. of Math. (2), **104** (1976), 459–571.
[KM] N. M. Katz and B. Mazur, Arithmetic moduli of elliptic curves, Ann. of Math. Stud., **108** (1985).
[KL] D. S. Kubert and S. Lang, Modular Units, Grundlehren math. Wiss., **244**, Springer-Verlag, Berlin, 1981.
[Ma] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math., **47** (1977), 33–186.
[MW1] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbf{Q}$, Invent. Math., **76** (1984), 179–330.
[MW2] B. Mazur and A. Wiles, On p-adic analytic families of Galois representations, Compositio Math., **59** (1986), 231–264.
[Mu] D. Mumford, Abelian Varieties, Tata Inst. Fund. Res. Stud. Math., **5**, Oxford University Press, London, 1970.
[Og1] A. P. Ogg, Rational points on certain elliptic modular curves, Proc. Sympos. Pure Math., **24** (1973), 221–231.
[Og2] A. P. Ogg, Diophantine equations and modular forms, Bull. Amer. Math. Soc., **81** (1975), 14–27.
[Oh1] M. Ohta, Congruence modules related to Eisenstein series, Ann. Sci. École Norm. Sup. (4), **36** (2003), 225–269.
[Oh2] M. Ohta, Companion forms and the structure of p-adic Hecke algebras, J. Reine Angew. Math., **585** (2005), 141–172.
[Ra] M. Raynaud, Schémas en groupes de type $(p, \dots, p)$, Bull. Soc. Math. France, **102** (1974), 241–280.
[Ri] K. A. Ribet, A modular construction of unramified p-extension of $\mathbf{Q}(\mu_p)$, Invent. Math., **34** (1976), 151–162.
[Se] J.-P. Serre, Sur la topologie des variétés algébriques en caractéristique p, Symp. Int. Top. Alg., Mexico (1958), 24–53 (Œuvre I, No. 38).
[Sh] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Publ. Math. Soc. Japan, **11**, Iwanami Shoten and Princeton University Press, 1971.
[Wa] L. C. Washington, Introduction to cyclotomic fields (second edition), Grad. Texts in Math., **83** (1997).
[Wi] A. Wiles, Modular curves and the class group of $\mathbf{Q}(\zeta_p)$, Invent. Math., **58** (1980), 1–35.

Masami Ohta
Professor Emeritus
Tokai University
Hiratsuka
Kanagawa 259-1292, Japan
E-mail: ohta@tokai-u.jp