TOKYO J. MATH.
VOL. 37, NO. 2, 2014

Eisenstein Ideals and the Rational Torsion Subgroups of Modular Jacobian Varieties II

Masami OHTA

Tokai University

Abstract. We study the rational torsion subgroup of the modular Jacobian variety $J_0(N)$ when N is square-free. We prove that the p-primary part of this group coincides with that of the cuspidal divisor class group for $p \geq 3$ when $3 \nmid N$, and for $p \geq 5$ when $3 \mid N$. We further determine the structure of each eigenspace of such p-primary part with respect to the Atkin-Lehner involutions. This is based on our study of the Eisenstein ideals in the Hecke algebras.

Introduction

In this article, we study the rational torsion subgroup $J_0(N)(\mathbb{Q})_{\text{tors}}$ of the Jacobian variety $J_0(N)$ of the usual modular curve $X_0(N)$ over $\mathbb{Q}$, when N is square-free.

This is a sequel to our previous work [Oh2] in which we studied the same problem for $J_1(N)$ of prime level N. The method here is, basically, similar to that paper, but there are dissimilarities as well, mainly due to the existence of oldforms in the space of cusp forms of weight two with respect to $\Gamma_0(N)$.

Before stating our main result, we briefly recall known facts on $J_0(N)(\mathbb{Q})_{\text{tors}}$. The study of this group began with works of Ogg. Namely, when N (≥ 5) is a prime, he proved that

- the cuspidal divisor class group of $X_0(N)$, the subgroup of $J_0(N)(\mathbb{Q})_{\text{tors}}$ generated by the difference of two cusps of $X_0(N)$, is of order $(N-1)/(N-1, 12)$,

in [Og1], and conjectured that

- this cuspidal divisor class group coincides with $J_0(N)(\mathbb{Q})_{\text{tors}}$,

in [Og2]. In the seminal paper [Ma], Mazur then proved, among others, that this conjecture is valid.

The above result on the cuspidal class number has been extended to other modular curves by many mathematicians, starting in 1970's with a series of papers by Kubert and Lang, cf. [KL]. For our present purpose, Takagi's result [T] on the cuspidal class number of $X_0(N)$ plays an important role.

As for the rational torsion in $J_0(N)$, after Mazur's work, the following were known:

Received June 6, 2013; revised February 4, 2014

Lorenzini [L] proved that the prime-to-6p part of $J_0(p^r)(\mathbb{Q})_{\text{tors}}$ is contained in the cuspidal divisor class group; and also that the same holds for the prime-to-2p part when $p \not\equiv 11 \pmod{12}$, for prime numbers $p \geq 5$. He also determined the structure of the prime-to-2p part in the latter case.

Agashe [A] recently proved that, if E is an elliptic curve over $\mathbb{Q}$ of square-free conductor N (thus there is a morphism $J_0(N) \twoheadrightarrow E$ over $\mathbb{Q}$), and if p is a prime not dividing $6N$ and dividing the order of $E(\mathbb{Q})_{\text{tors}}$, then p is a divisor of the cuspidal divisor class number of $X_0(N)$.

In this paper, we study the same theme as in [A]. Thus we let N be a square-free positive integer, in the rest of this introduction. It is then known that all cusps of $X_0(N)$ are rational over $\mathbb{Q}$. Therefore the cuspidal divisor class group $\mathcal{C}(N)$, i.e. the group generated by the classes of differences of two cusps of $X_0(N)$, is a subgroup of $J_0(N)(\mathbb{Q})_{\text{tors}}$. (By a classical theorem of Manin and Drinfel'd, every element of $\mathcal{C}(N)$ is torsion.) The following is the main result of this paper, in which we indicate by "$[p^\infty]$" the p-primary part:

THEOREM. *Let N be a square-free positive integer, and let $\mathcal{C}(N)$ be as above. Then we have*

$$J_0(N)(\mathbb{Q})_{\text{tors}}[p^\infty] = \mathcal{C}(N)[p^\infty]$$

for all prime numbers $p \geq 3$ when N is not divisible by 3; *and for all prime numbers $p \geq 5$ when N is divisible by* 3.

In the text, this is stated as Theorem (3.6.2), in which we give a finer statement: One can decompose $J_0(N)(\mathbb{Q})_{\text{tors}}[p^\infty] = \mathcal{C}(N)[p^\infty]$ as a direct sum of eigenspaces with respect to the Atkin-Lehner involutions of $J_0(N)$, and we determine the group structure of each direct summand.

To obtain such a result, we need a detailed study of the *Eisenstein ideals* in the *Hecke algebras*. To study these objects, we of course use the theory of modular forms.

As for the modular forms, we consider the following three types of spaces of modular forms (holomorphic at cusps) and subspaces of cusp forms

$$\begin{cases} M_k^{\mathrm{A}}(\Gamma_0(N);\, R) \supseteq S_k^{\mathrm{A}}(\Gamma_0(N);\, R)\,, \\ M_k^{\mathrm{B}}(\Gamma_0(N);\, R) \supseteq S_k^{\mathrm{B}}(\Gamma_0(N);\, R)\,, \\ M_2^{\mathrm{reg}}(\Gamma_0(N);\, R) \supseteq S_2^{\mathrm{reg}}(\Gamma_0(N);\, R) \end{cases}$$

over a ring R, each of which has its own merit. The first (resp. the second) spaces are those of modular forms and cusp forms in the sense of Deligne-Rapoport and Katz (resp. Serre and Swinnerton-Dyer), while the third spaces are those of regular differentials on the modular curve. (The superscript "A" (resp. "B") corresponds to Mazur's notation: Our $M_2^{\mathrm{A}}(\Gamma_0(N);\, R)$ (resp. $M_2^{\mathrm{B}}(\Gamma_0(N);\, R)$) is $\mathrm{A}(R)$ (resp. $\mathrm{B}(R)$) in [Ma, II, 4].) See Section 1 for their definitions, properties and interrelations.

When $R = \mathbb{Q}$ and $k = 2$, the above three kinds of spaces all coincide, and these are acted on by the Hecke operators $T(l)$ (for prime numbers l not dividing N), $U(l)$ (for prime numbers l dividing N) and the Atkin-Lehner involutions w_d (for positive divisors d of N). The Hecke algebras $\boldsymbol{\mathcal{T}}(N;\mathbb{Z})$ and $\mathbf{T}(N;\mathbb{Z})$ considered in this paper are the subalgebras of the endomorphism algebras of these spaces of modular forms and cusp forms generated by all $T(l)$ (l: as above) and w_d over $\mathbb{Z}$, respectively. Thus, when N is a prime, $\mathbf{T}(N;\mathbb{Z})$ is exactly the ring $\mathbf{T}$ considered in [Ma, II, 6]. Although $\mathbf{T}$ coincides with the algebra generated by all $T(l)$ and $U(N)$ in the prime level case, we note that $\mathbf{T}(N;\mathbb{Z})$ definitely differs from this latter type of algebra for general N. We think that these algebras $\boldsymbol{\mathcal{T}}(N;\mathbb{Z})$ and $\mathbf{T}(N;\mathbb{Z})$ are rather suited to control modular forms and cusp forms, especially the Eisenstein series, for our purpose. See Section 2 for our results in this direction.

One can consider $\mathbf{T}(N;\mathbb{Z})$ as a subalgebra of $\mathrm{End}(J_0(N))$ in a natural manner. To study $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$, as initiated by [Ma], an essential role is played by the Eisenstein ideal $I_{\mathbb{Z}}$ of $\mathbf{T}(N;\mathbb{Z})$. By definition, it is the ideal generated by $T(l) - (1+l)$ for all prime numbers l not dividing N. The most important ingredient of the proof of our main theorem is the explicit formula of the index of $I_{\mathbb{Z}}$ in $\mathbf{T}(N;\mathbb{Z})$, up to a power of 2, which turns out to be the order of $\mathcal{C}(N)$ by Takagi's formula, again up to a power of 2. This result is stated as Theorem (3.1.3) in the text, in which we give a more precise description, decomposing $I_{\mathbb{Z}}$ and $\mathbf{T}(N;\mathbb{Z})$ into eigenspaces with respect to the Atkin-Lehner involutions over $\mathbb{Z}[1/2]$. In Section 3, after proving this theorem, we complete the proof of our main theorem.

1. Preliminaries on modular curves and modular forms

1.1. Modular curves. Let N be a positive integer. We first recall known facts on the modular curves attached to the congruence subgroup

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\}. \tag{1.1.1}$$

For more details, see Shimura [Sh], Katz and Mazur [KM] and Deligne and Rapoport [DR]. The group above acts on the complex upper half plane H, and the (open) Riemann surface $\Gamma_0(N)\backslash H$ is compactified by adding cusps $\Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q})$. We denote by $Y_0(N)_{/\mathbb{Q}}$ (resp. $X_0(N)_{/\mathbb{Q}}$), or simply by $Y_0(N)$ (resp. $X_0(N)$) when there is no fear of confusion, Shimura's canonical model of $\Gamma_0(N)\backslash H$ (resp. its compactification $\Gamma_0(N)\backslash(H \cup \mathbb{P}^1(\mathbb{Q}))$) defined over $\mathbb{Q}$.

These curves have natural models over $\mathbb{Z}$. Namely there is the coarse moduli scheme $Y_0(N)_{/\mathbb{Z}}$ classifying the pairs (E, C_N) consisting of

$$\begin{cases} \bullet \text{ an elliptic curve } E \text{ over a scheme } S, \text{ and} \\ \bullet \text{ its } \Gamma_0(N)\text{-structure } C_N \text{ (i.e. a finite flat } S\text{-subgroup scheme of } E[N] \\ \text{which is locally free of rank } N \text{ and cyclic)}. \end{cases} \tag{1.1.2}$$

(Here and henceforth the bracket $[n]$ indicates the kernel of multiplication by n.) When the base schemes are restricted to $\mathbb{Q}$-schemes, the resulting coarse moduli scheme is given by $Y_0(N)$. There is the natural compactification $X_0(N)_{/\mathbb{Z}}$ of $Y_0(N)_{/\mathbb{Z}}$ (i.e. the normalization of the projective j-line via $Y_0(N)_{/\mathbb{Z}} \to Y_0(1)_{/\mathbb{Z}} = \mathrm{Spec}(\mathbb{Z}[j])$). We have

$$\begin{cases} Y_0(N) = Y_0(N)_{/\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}\,, \\ X_0(N) = X_0(N)_{/\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}\,. \end{cases} \tag{1.1.3}$$

For any ring R, we set

$$\begin{cases} Y_0(N)_{/R} := Y_0(N)_{/\mathbb{Z}} \otimes_{\mathbb{Z}} R\,, \\ X_0(N)_{/R} := X_0(N)_{/\mathbb{Z}} \otimes_{\mathbb{Z}} R\,. \end{cases} \tag{1.1.4}$$

$Y_0(N)_{/R}$ and $X_0(N)_{/R}$ are smooth over R and the scheme of cusps $X_0(N)_{/R} - Y_0(N)_{/R}$ is étale over R whenever N is invertible in R.

For a positive divisor d of N such that $(d, N/d) = 1$, any matrix of the form

$$W_d = \begin{bmatrix} dx & y \\ Nz & dw \end{bmatrix} \quad (x, y, z, w \in \mathbb{Z},\ \det W_d = d) \tag{1.1.5}$$

normalizes $\Gamma_0(N)$, and induces involutive automorphisms of $\Gamma_0(N)\backslash H$ and $\Gamma_0(N)\backslash\ (H \cup \mathbb{P}^1(\mathbb{Q}))$ which depend only on d. Further, these induce automorphisms of $Y_0(N)$ and $X_0(N)$ over $\mathbb{Q}$, which we denote by the symbol w_d.

These automorphisms w_d have the following description in terms of moduli: For (E, C_N) over S as above, set

$$w_d(E, C_N) := (E/C_N[d],\ E[d]/C_N[d] \times_S C_N/C_N[d])\,. \tag{1.1.6}$$

The correspondence $(E, C_N) \mapsto w_d(E, C_N)$ induces an involutive automorphism of the coarse moduli scheme $Y_0(N)_{/\mathbb{Z}}$ and extends uniquely to $X_0(N)_{/\mathbb{Z}}$. We then obtain automorphisms of $Y_0(N)_{/R}$ and $X_0(N)_{/R}$ which coincide with the ones described in the classical context when $R = \mathbb{C}$ or $\mathbb{Q}$. All these automorphisms will be denoted by w_d indifferently.

All w_d's commute with each other. If $N = l_1^{e_1} \cdots l_m^{e_m}$ is the prime decomposition and $d = l_{i_1}^{e_{i_1}} \cdots l_{i_k}^{e_{i_k}}$, then we have $w_d = w_{l_{i_1}^{e_{i_1}}} \cdots w_{l_{i_k}^{e_{i_k}}}$, and the group

$$G_{\mathrm{AL}} := \{w_d \mid d > 0,\ d \mid N,\ (d, N/d) = 1\} \subseteq \mathrm{Aut}(Y_0(N)_{/\mathbb{Z}}) \text{ or } \mathrm{Aut}(X_0(N)_{/\mathbb{Z}}) \tag{1.1.7}$$

is an elementary abelian group of type $(2, \ldots, 2)$ of order 2^m generated by $w_{l_i^{e_i}}$ $(i = 1, \ldots, m)$.

Let p be a prime number, and assume that $N = pM$ with M prime to p. We recall the description of $X_0(N)_{/\mathbb{F}_p}$ [DR, VI, 6]: When E is an elliptic curve over an $\mathbb{F}_p$-scheme S, and C_M (resp. C_N) is a $\Gamma_0(M)$-structure (resp. a $\Gamma_0(N)$-structure) on E/S, consider the correspondence:

$(E, C_M) \mapsto (E, C_M \times_S \mathrm{Ker}(\mathrm{Frob}))$
(resp. $(E, C_N) \mapsto (E, C_N[M])$)
where Frob : $E \to E^{(p)}$ is the Frobenius morphism. Now $Y_0(N)_{/\mathbb{F}_p}$ (as well as $Y_0(M)_{/\mathbb{F}_p}$) is the coarse moduli scheme of the same type as above in characteristic p, and this induces a morphism over $\mathbb{F}_p$

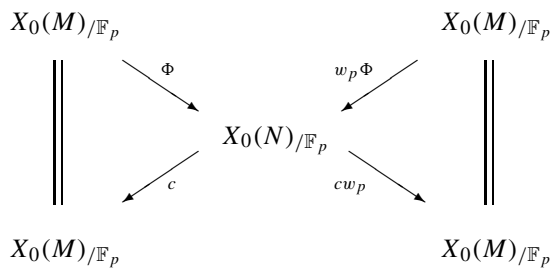
$\Phi : Y_0(M)_{/\mathbb{F}_p} \to Y_0(N)_{/\mathbb{F}_p}$
(resp. $c : Y_0(N)_{/\mathbb{F}_p} \to Y_0(M)_{/\mathbb{F}_p}$).

The morphism $w_p\Phi$ (resp. cw_p) is then induced from the correspondence:

$(E, C_M) \mapsto (E^{(p)}, C_M^{(p)} \times_S \mathrm{Ker}(\mathrm{Ver}))$
(resp. $(E, C_N) \mapsto (E/C_N[p], C_N/C_N[p])$)

where Ver : $E^{(p)} \to E$ is the Verschiebung, and $C_N^{(p)} \subset E^{(p)}$ corresponds to $C_N \subset E$. All these morphisms extend to compactified schemes, which we denote by the same symbols, and we have the following commutative diagram:

(1.1.8)



Here, Φ and $w_p\Phi$ are closed immersions, and $X_0(N)_{/\mathbb{F}_p}$ is the union of the images of Φ and $w_p\Phi$, crossing transversally at the mutually $\mathbb{F}_p$-conjugate supersingular points. The composites $cw_p \circ \Phi$ and $c \circ w_p\Phi$ are the Frobenius morphism of $X_0(M)_{/\mathbb{F}_p}$ to itself.

1.2. Algebraic theory of modular forms. Let N be a positive integer. In this subsection, we recall modular forms of level N in the sense of Deligne and Rapoport [DR] and Katz [K1], [K2]. Since we use this notion only over the base rings in which N is invertible, *we will always assume that R is a $\mathbb{Z}[1/N]$-algebra, in this subsection.*

Aside from the $\Gamma_0(N)$-structure (1.1.2), we will make auxiliary use of the notion of the $\Gamma(N)$-structure ϕ and the $\Gamma_\mu(N)$-structure i for an elliptic curve E over an R-scheme S:

(1.2.1)
$$\begin{cases} \phi : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} E[N] \text{ (an isomorphism of } S\text{-group schemes)}, \\ i : \boldsymbol{\mu}_N \hookrightarrow E[N] \text{ (a closed immersion of } S\text{-group schemes)}. \end{cases}$$

DEFINITION (1.2.2). Let k be a positive integer. A modular form f (not necessarily holomorphic at cusps) of weight k over R with respect to $\Gamma_0(N)$ is a rule which assigns to each pair (E, C_N) as in (1.1.2) over an R-scheme S an element $f(E, C_N) \in H^0(S, \underline{\omega}_{E/S}^{\otimes k})$, where

$\underline{\omega}_{E/S}$ is the direct image of $\Omega^1_{E/S}$ to S, satisfying the following compatibility: If $g : S' \to S$ is a morphism of R-schemes and

$$\begin{array}{ccc} (E, C_N) & \xleftarrow{g'} & (E', C'_N) \\ \downarrow & & \downarrow \\ S & \xleftarrow[g]{} & S' \end{array}$$

is a cartesian square, then we have $f(E', C'_N) = g^* f(E, C_N)$. We denote by $M^{\mathrm{A}}(R, \Gamma_0(N), k)$ the space of all such forms.

Similarly, we define the spaces of modular forms $M^{\mathrm{A}}(R, \Gamma(N), k)$ and $M^{\mathrm{A}}(R, \Gamma_\mu(N), k)$ replacing the above C_N by ϕ and i, respectively.

There is an equivalent way of expressing an element of $M^{\mathrm{A}}(R, \Gamma_0(N), k)$: Consider a triple (E, C_N, ω) over $S = \mathrm{Spec}(B)$ where (E, C_N) is as above, and ω is a B-basis of $H^0(\mathrm{Spec}(B), \underline{\omega}_{E/S})$ (which is supposed to be free over B). Then we may consider an element of $M^{\mathrm{A}}(R, \Gamma_0(N), k)$ as a rule f_0 which assigns to every such triple (E, C_N, ω) an element $f_0(E, C_N, \omega) \in B$ satisfying:

$$(1.2.3) \qquad \begin{cases} \bullet \text{ The formation of } f_0(E, C_N, \omega) \text{ is compatible with cartesian squares} \\ \text{in the same sense as above; and} \\ \bullet \ f_0(E, C_N, \lambda\omega) = \lambda^{-k} f_0(E, C_N, \omega) \text{ for any } \lambda \in B^\times . \end{cases}$$

Indeed, the correspondence $f \leftrightarrow f_0$ with $f(E, C_N) = f_0(E, C_N, \omega)\omega^{\otimes k}$ identifies $M^{\mathrm{A}}(R, \Gamma_0(N), k)$ with the set of all f_0 as above. Similarly for $\Gamma(N)$ and $\Gamma_\mu(N)$ in place of $\Gamma_0(N)$.

Fix a primitive N-th root of unity $\zeta_N \in \overline{\mathbb{Q}}$, and set

$$(1.2.4) \qquad R[\zeta_N] := R \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}[1/N, \zeta_N] .$$

Consider the Tate curve $\mathrm{Tate}(q)$ over $R[\zeta_N]((q^{1/N}))$; [K1, A1.2], [KM, (8.8)]. There is the canonical invariant differential ω_{can} on this curve.

DEFINITION (1.2.5). An element $f \in M^{\mathrm{A}}(R, \Gamma_0(N), k)$ is called holomorphic (at cusps) (resp. a cusp form) if $f_0(\mathrm{Tate}(q), C_N, \omega_{\mathrm{can}}) \in R[\zeta_N]((q^{1/N}))$ belongs to $R[\zeta_N][[q^{1/N}]]$ (resp. $q^{1/N} \cdot R[\zeta_N][[q^{1/N}]]$) for any $\Gamma_0(N)$-structure C_N on $\mathrm{Tate}(q)$. The subspace of such holomorphic forms (resp. cusp forms) is denoted by $M^{\mathrm{A}}_k(\Gamma_0(N); R)$ (resp. $S^{\mathrm{A}}_k(\Gamma_0(N); R)$). Replacing the above C_N by $\Gamma(N)$- or $\Gamma_\mu(N)$-structures, we define the spaces $M^{\mathrm{A}}_k(\Gamma(N); R)$, $S^{\mathrm{A}}_k(\Gamma(N); R)$, $M^{\mathrm{A}}_k(\Gamma_\mu(N); R)$ and $S^{\mathrm{A}}_k(\Gamma_\mu(N); R)$ in the same manner.

We let $GL_2(\mathbb{Z}/N\mathbb{Z})$ act on $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ by $GL_2(\mathbb{Z}/N\mathbb{Z}) \ni \gamma : (m, n) \mapsto (m, n)^t\gamma$.

This induces the left action of $GL_2(\mathbb{Z}/N\mathbb{Z})$ on $M^{\mathrm{A}}(R, \Gamma(N), k)$ by:

$$\gamma f(E, \phi) := f(E, \phi \circ {}^t\gamma)$$

which clearly preserves $M_k^{\mathrm{A}}(\Gamma(N); R)$ and $S_k^{\mathrm{A}}(\Gamma(N); R)$.

If n is a positive integer prime to N and invertible in R, and if we define a $\Gamma_0(N) \cap \Gamma(n)$-structure to be a pair of $\Gamma_0(N)$- and $\Gamma(n)$-structures, we can similarly consider $M_k^{\mathrm{A}}(\Gamma_0(N) \cap \Gamma(n); R)$ and $S_k^{\mathrm{A}}(\Gamma_0(N) \cap \Gamma(n); R)$ together with natural action of $GL_2(\mathbb{Z}/n\mathbb{Z})$ on them.

Also $(\mathbb{Z}/N\mathbb{Z})^\times$ naturally acts on the $\Gamma_\mu(N)$-structures by $(\mathbb{Z}/N\mathbb{Z})^\times \ni c : i \mapsto c \cdot i$, and we can let $(\mathbb{Z}/N\mathbb{Z})^\times$ act on $M_k^{\mathrm{A}}(\Gamma_\mu(N); R)$ and $S_k^{\mathrm{A}}(\Gamma_\mu(N); R)$ (which gives the usual diamond operators).

Now we have natural mappings:

$$\begin{cases} M_k^{\mathrm{A}}(\Gamma_0(N); R) \to M_k^{\mathrm{A}}(\Gamma(N); R)\,, \\ M_k^{\mathrm{A}}(\Gamma_0(N); R) \to M_k^{\mathrm{A}}(\Gamma_0(N) \cap \Gamma(n); R)\,, \\ M_k^{\mathrm{A}}(\Gamma_0(N); R) \to M_k^{\mathrm{A}}(\Gamma_\mu(N); R)\,. \end{cases}$$

We describe the first mapping, the others being the evident ones. Given a $\Gamma(N)$-structure ϕ on E, we associate the $\Gamma_0(N)$-structure $C_{N,\phi} := \phi(\mathbb{Z}/N\mathbb{Z} \times \{0\})$. We then send $f \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$ to the rule: $(E, \phi) \mapsto f(E, C_{N,\phi})$.

LEMMA (1.2.6). *The above mappings induce the following canonical isomorphisms*:
(1) *Let B be the upper triangular matrices in $GL_2(\mathbb{Z}/N\mathbb{Z})$. Then we have*

$$M_k^{\mathrm{A}}(\Gamma(N); R)^B = M_k^{\mathrm{A}}(\Gamma_0(N); R)\,.$$

(2) $M_k^{\mathrm{A}}(\Gamma_0(N) \cap \Gamma(n); R)^{GL_2(\mathbb{Z}/n\mathbb{Z})} = M_k^{\mathrm{A}}(\Gamma_0(N); R)\,.$
(3) $M_k^{\mathrm{A}}(\Gamma_\mu(N); R)^{(\mathbb{Z}/N\mathbb{Z})^\times} = M_k^{\mathrm{A}}(\Gamma_0(N); R)\,.$
Similarly for cusp forms.

PROOF. This must be well-known, and in fact can be proved in the same manner as in Edixhoven [E1, 2.1]. The point is that, in the terminology of [KM, (4.2), (4.13)], for a given elliptic curve $E/S/R$, $[\Gamma(N)]_{E/S}$ is an étale B-torsor, $[\Gamma_0(N) \cap \Gamma(n)]_{E/S}$ is an étale $GL_2(\mathbb{Z}/n\mathbb{Z})$-torsor, and $[\Gamma_\mu(N)]_{E/S}$ is an étale $(\mathbb{Z}/N\mathbb{Z})^\times$-torsor over $[\Gamma_0(N)]_{E/S}$, respectively. □

There is a canonical exact sequence

$$0 \to \boldsymbol{\mu}_N \to \mathrm{Tate}(q)[N] \to \mathbb{Z}/N\mathbb{Z} \to 0 \quad \text{for Tate}(q) \text{ over } R((q)) \tag{1.2.7}$$

[KM (8.8)], and hence canonical $\Gamma_\mu(N)$- and $\Gamma_0(N)$-structures on $\mathrm{Tate}(q)$ over the same ring, respectively,

$$\begin{cases} i_{\mathrm{can}} : \boldsymbol{\mu}_N \overset{(1.2.7)}{\hookrightarrow} \mathrm{Tate}(q)[N]\,, \\ C_{N,\mathrm{can}} := \boldsymbol{\mu}_N \subseteq \mathrm{Tate}(q)[N] \end{cases} \tag{1.2.8}$$

from which we obtain the q-expansion mappings (at the cusp infinity):

$$\text{(1.2.9)} \qquad \begin{cases} M_k^{\mathrm{A}}(\Gamma_\mu(N);\, R) \to R[[q]] \text{ by } \ f \mapsto f_0(\mathrm{Tate}(q), i_{\mathrm{can}}, \omega_{\mathrm{can}})\,, \\ M_k^{\mathrm{A}}(\Gamma_0(N);\, R) \to R[[q]] \text{ by } \ f \mapsto f_0(\mathrm{Tate}(q), C_{N,\mathrm{can}}, \omega_{\mathrm{can}})\,. \end{cases}$$

The image of f in the left hand side to $R[[q]]$ will be denoted by $f(q)$. The following is a variant of [K1, Corollary 1.6.2], which is often useful:

PROPOSITION (1.2.10) (The q-expansion principle). *The above mappings are injective. Moreover, if R_0 is a $\mathbb{Z}[1/N]$-subalgebra of R and $f(q)$ lies in $R_0[[q]]$, f belongs to $M_k^{\mathrm{A}}(\Gamma_\mu(N);\, R_0)$ (resp. $M_k^{\mathrm{A}}(\Gamma_0(N);\, R_0)$) in the first (resp. the second) case.*

PROOF. The first case is well-known (cf. Gross [G, Proposition 2.7, §10]), and the second case (which must be also well-known) follows from this and (1.2.6), (3). □

As for base changes, we have:

PROPOSITION (1.2.11). *If R' is a flat R-algebra, the canonical mapping*

$$M_k^{\mathrm{A}}(\Gamma_0(N);\, R) \otimes_R R' \to M_k^{\mathrm{A}}(\Gamma_0(N);\, R')$$

is an isomorphism. Similarly for cusp forms.

PROOF. (Cf. Edixhoven [E2, Section 1]). If $n \geq 3$ is prime to N and R is a $\mathbb{Z}[1/nN]$-algebra, this follows from (1.2.6), (2). The general case follows from this by glueing. □

DEFINITION (1.2.12). Let d be a positive divisor of N such that $(d, N/d) = 1$. For $f \in M_k^{\mathrm{A}}(\Gamma_0(N);\, R)$, we define $\mathbf{w}_d f \in M_k^{\mathrm{A}}(\Gamma_0(N);\, R)$ by

$$(\mathbf{w}_d f)(E, C_N) := \pi^* f(w_d(E, C_N))$$

where $w_d(E, C_N)$ is defined by (1.1.6), $\pi : E \to E/C_N[d]$ is the quotient morphism, and π^* means the pull-back of the section of $\underline{\omega}^{\otimes k}_{(E/C_N[d])/S}$ to that of $\underline{\omega}^{\otimes k}_{E/S}$.

In terms of f_0 as in (1.2.3) corresponding to f, $\mathbf{w}_d f_0$ corresponding to $\mathbf{w}_d f$ can be described as follows: Let $(E, C_N, \omega)/B/R$ be as before. Since the quotient morphism π above is étale, there is a unique differential ω' on $E/C_N[d]$ such that $\pi^*(\omega') = \omega$. We then have

$$\text{(1.2.13)} \qquad (\mathbf{w}_d f_0)(E, C_N, \omega) = f_0(E/C_N[d],\, E[d]/C_N[d] \times_S C_N/C_N[d], \omega')\,.$$

It is easy to see that

$$\text{(1.2.14)} \qquad \mathbf{w}_d(\mathbf{w}_d f) = d^k f \text{ for any } f \in M_k^{\mathrm{A}}(\Gamma_0(N);\, R)\,.$$

1.3. Relation with classical forms. In this subsection, we consider modular forms of Serre and Swinnerton-Dyer type, and the relation with those in the previous subsection. Again let k be a positive integer. For a function $f(z)$ on the complex upper half plane H and $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2^+(\mathbb{R})$, we set

$$(f\,|_k\,\gamma)(z) := \det(\gamma)^{k/2}(cz+d)^{-k} f(\gamma z)\,. \tag{1.3.1}$$

Let $M_k(\Gamma_0(N))$ and $S_k(\Gamma_0(N))$ be the complex vector spaces of modular forms and cusp forms of weight k in the usual sense, respectively. There is a well-known dictionary that identifies these spaces with $M_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{C})$ and $S_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{C})$ (cf. [K2, 2.4] and also [Oh1, 3.6]). The q-expansion (1.2.9) then corresponds to the usual Fourier expansion of classical forms with $q = e^{2\pi i z}$.

Set

$$\begin{cases} M_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}) := \{f \in M_k(\Gamma_0(N)) \mid f(q) \in \mathbb{Z}[[q]]\}\,, \\ S_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}) := \{f \in S_k(\Gamma_0(N)) \mid f(q) \in \mathbb{Z}[[q]]\} \end{cases} \tag{1.3.2}$$

and

$$\begin{cases} M_k^{\mathrm{B}}(\Gamma_0(N);R) := M_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}) \otimes_{\mathbb{Z}} R\,, \\ S_k^{\mathrm{B}}(\Gamma_0(N);R) := S_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}) \otimes_{\mathbb{Z}} R \end{cases} \tag{1.3.3}$$

for any ring R. When $R = \mathbb{Z}[1/N]$, the q-expansion principle (1.2.10) assures us that these spaces coincide with $M_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{Z}[1/N])$ and $S_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{Z}[1/N])$.

The same assertion as (1.2.10) holds for the spaces (1.3.3) with respect to the obvious q-expansion mappings simply because the cokernels of the mappings $M_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}) \hookrightarrow \mathbb{Z}[[q]]$ and $S_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}) \hookrightarrow \mathbb{Z}[[q]]$ are flat over $\mathbb{Z}$. Also, it is obvious from the definition that the formation of $M_k^{\mathrm{B}}(\Gamma_0(N);R)$ and $S_k^{\mathrm{B}}(\Gamma_0(N);R)$ commutes with arbitrary change of base rings.

It thus follows from (1.2.11) that we have canonical isomorphisms

$$\begin{cases} M_k^{\mathrm{A}}(\Gamma_0(N);R) = M_k^{\mathrm{B}}(\Gamma_0(N);R)\,, \\ S_k^{\mathrm{A}}(\Gamma_0(N);R) = S_k^{\mathrm{B}}(\Gamma_0(N);R) \end{cases} \quad \text{for } R \text{ flat over } \mathbb{Z}[1/N]\,. \tag{1.3.4}$$

LEMMA (1.3.5). *For any $\mathbb{Z}[1/N]$-algebra R, we have canonical (q-expansion preserving) injections*:

$$\begin{cases} M_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{Z}[1/N]) \otimes_{\mathbb{Z}[1/N]} R \hookrightarrow M_k^{\mathrm{A}}(\Gamma_0(N);R)\,, \\ M_k^{\mathrm{B}}(\Gamma_0(N);R) \hookrightarrow M_k^{\mathrm{A}}(\Gamma_0(N);R)\,. \end{cases}$$

The same holds for cusp forms.

PROOF. From the above discussions, we have the commutative square

$$\begin{array}{ccc} M_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{Z}[1/N])\otimes_{\mathbb{Z}[1/N]} R & \xrightarrow{\sim} & M_k^{\mathrm{B}}(\Gamma_0(N);R) \\ \downarrow & & \downarrow q\text{-exp.} \\ M_k^{\mathrm{A}}(\Gamma_0(N);R) & \xrightarrow{q\text{-exp.}} & R[[q]] \end{array}$$

with injective q-expansion mappings. Our conclusion follows from this. □

We note that the above mappings are not surjective in general. Indeed, as is well-known, $M_2^{\mathrm{A}}(\Gamma_0(1);\mathbb{Z}) = M_2^{\mathrm{B}}(\Gamma_0(1);\mathbb{Z}) = \{0\}$ and $M_2^{\mathrm{B}}(\Gamma_0(1);\mathbb{Z}/3\mathbb{Z}) = \{0\}$, while $M_2^{\mathrm{A}}(\Gamma_0(1);\mathbb{Z}/3\mathbb{Z})$ is a non-zero space generated by (the form corresponding to) the Hasse invariant. Later in (2.3.9), we will see when this form lifts to $M_2^{\mathrm{B}}(\Gamma_0(N);\mathbb{Q})$.

DEFINITION (1.3.6). Assume that k is even, and let d be a positive divisor of N such that $(d, N/d) = 1$. For any $f \in M_k^{\mathrm{A}}(\Gamma_0(N);R)$ with R a $\mathbb{Z}[1/N]$-algebra, we set

$$f\,|_k\, w_d := d^{-k/2}(\mathbf{w}_d f)$$

the right hand side being defined by (1.2.12).

By (1.2.14), the operator "$|_k\, w_d$" is an involution. This is in fact the Atkin-Lehner involution:

LEMMA (1.3.7). *If $f \in M_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{C}) = M_k(\Gamma_0(N))$, the above $f\,|_k\, w_d$ coincides with $f\,|_k\, W_d$ defined through* (1.3.1) *with a matrix W_d* (1.1.5).

PROOF. This must be also well-known, and indeed can be proved by the same method as [Oh1, (3.6.5)]. (N.B. The differential ω' used there is $d\times$(the differential ω' figuring in (1.2.13)), and a different convention [Oh1, (2.1.1)] was used in place of (1.3.1).) □

COROLLARY (1.3.8). *The subspace $M_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}[1/N])$ of $M_k(\Gamma_0(N))$ is stable under the Atkin-Lehner involutions "$|_k\, w_d$"= "$|_k\, W_d$".* □

By base extension, these involutions induce involutions of $M_k^{\mathrm{B}}(\Gamma_0(N);R)$ whenever R is a $\mathbb{Z}[1/N]$-algebra, for which we use the same symbols "$|_k\, w_d$".

We remark however that the corollary above does not hold when $\mathbb{Z}[1/N]$ is replaced by $\mathbb{Z}$ in general. For example, assume that $p \,\|\, N$ (i.e. $p \mid N$ but $p \nmid (N/p)$), and that f is an element of $M_k^{\mathrm{B}}(\Gamma_0(N/p);\mathbb{Z}) - pM_k^{\mathrm{B}}(\Gamma_0(N/p);\mathbb{Z})$. Then we have

$$f\,|_k\, w_p = f\,|_k \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} = p^{k/2} g$$

with $g(z) = f(pz) \in M_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z})$. Hence we have

$$g\,|_k\, w_p = p^{-k/2} f \notin M_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z})\,.$$

1.4. Regular differentials. For a prime number p, let $\mathbb{Z}_{(p)}$ be the localization of $\mathbb{Z}$ at the prime ideal (p). For the moment, assume that $p \parallel N$. Let R be a $\mathbb{Z}_{(p)}$-algebra. Then the morphism $X_0(N)_{/R} \to \mathrm{Spec}(R)$ is complete intersection, and there is the invertible sheaf $\Omega_{/R}$ of regular differentials on $X_0(N)_{/R}$; cf. [DR, I, 2], [Ma, II, 3] and Mazur and Ribet [MR, 7]. It has the following properties:

(1.4.1) The formation of $\Omega_{/R}$ commutes with arbitrary change of base ($\mathbb{Z}_{(p)}$-) algebras.

(1.4.2) The restriction of $\Omega_{/R}$ to the smooth locus $X_0(N)_{/R}^{\mathrm{smooth}}$ over R is the usual sheaf $\Omega^1_{X_0(N)_{/R}^{\mathrm{smooth}}/R}$ of Kähler differentials.

(1.4.3) Let $R \to k$ be a homomorphism to a field k of characteristic p, and $\pi : \widetilde{X_0(N)}_{/k} \to X_0(N)_{/k}$ the normalization. Then a section of $\Omega_{/k} = \Omega_{/R} \otimes_R k$ on an open subscheme U of $X_0(N)_{/k}$ is a differential ω on $\pi^{-1}(U)$ with at worst simple poles at the inverse image by π of the singular locus of U. If $P \in U(\overline{k})$ is a singular point and $\pi^{-1}(P) = \{P_1, P_2\}$, then $\mathrm{Res}_{P_1}\omega + \mathrm{Res}_{P_2}\omega = 0$.

When N is square-free, there is the sheaf of regular differentials $\Omega_{/\mathbb{Z}}$ on $X_0(N)_{/\mathbb{Z}}$ having similar properties as above. When there is no fear of confusion, we simply write Ω for $\Omega_{/R}$. In each case above, the scheme of cusps of $X_0(N)_{/R}$, denoted "cusps" below, is finite and étale over R by [KM, Theorem 10.10.3, (5)], and we consider it as an effective Cartier divisor in $X_0(N)_{/R}/R$.

LEMMA (1.4.4). *Consider*

(1) $f : X_0(N)_{/\mathbb{Z}_{(p)}} \to \mathrm{Spec}(\mathbb{Z}_{(p)}) = S$ *when* $p \parallel N$, *or*

(2) $f : X_0(N)_{/\mathbb{Z}} \to \mathrm{Spec}(\mathbb{Z}) = S$ *when* N *is square-free.*

Then $R^i f_*(\Omega)$ *and* $R^i f_*(\Omega(\mathrm{cusps}))$ *are locally free* $\mathcal{O}_S$*-modules for all* $i \geq 0$.

PROOF. One can prove this as in [Ma, II, 3] by arguing as [Ma, II, Lemma (3.3)] and then invoking the Grothendieck duality.

Alternatively, one can proceed more directly as follows. When $i \geq 2$, the sheaves in question vanish, and hence we only need to treat the cases $i = 0, 1$. For this, it is enough to show that the functions

$$\begin{cases} S \ni s \mapsto \dim_{\kappa(s)} H^i(X_0(N)_{/\kappa(s)}, \Omega_{/\kappa(s)}), \\ S \ni s \mapsto \dim_{\kappa(s)} H^i(X_0(N)_{/\kappa(s)}, \Omega_{/\kappa(s)}(\mathrm{cusps})) \end{cases}$$

are constant, where $\kappa(s)$ denotes the residue field at s; cf. Mumford [Mu, II, 5, Corollary 2]. But by the invariance of the Euler-Poincaré characteristics [Mu, II, 5, Corollary, (b)], it is enough to prove this for one of the values $i = 0$ or 1.

Let us check this for $i = 0$. We may replace s by a geometric point $\overline{s}$ above s. First $\dim_{\kappa(\overline{s})} H^0(X_0(N)_{/\kappa(\overline{s})}, \Omega_{/\kappa(\overline{s})})$ is always equal to the genus of $X_0(N)$. This is obvious when $X_0(N)_{/\kappa(\overline{s})}$ is smooth. Otherwise, the description of the bad fiber given in 1.1 and (1.4.3) implies that the above dimension is equal to $2 \cdot \mathrm{genus}(X_0(N/p)) +$

#(supersingular points on $X_0(N/p)_{/\kappa(\overline{s})}) - 1$. It is well-known, and easy to prove using 1.1, that this is equal to the genus of $X_0(N)$.

Also, we see using (1.4.3) that $\dim_{\kappa(\overline{s})} H^0(X_0(N)_{/\kappa(\overline{s})}, \Omega_{/\kappa(\overline{s})}(\text{cusps}))$ is equal to $\dim_{\kappa(\overline{s})} H^0(X_0(N)_{/\kappa(\overline{s})}, \Omega_{/\kappa(\overline{s})}) + \#(\text{cusps on } X_0(N)_{/\kappa(\overline{s})}) - 1$ for all $\overline{s}$. Our claim then follows since the scheme of cusps is étale over R. □

From this and the property (1.4.3), we obtain:

COROLLARY (1.4.5). (1) *The canonical mappings*

$$\begin{cases} H^0(X_0(N)_{/\mathbb{Z}_{(p)}}, \Omega) \otimes_{\mathbb{Z}_{(p)}} R \to H^0(X_0(N)_{/R}, \Omega)\,, \\ H^0(X_0(N)_{/\mathbb{Z}_{(p)}}, \Omega(\text{cusps})) \otimes_{\mathbb{Z}_{(p)}} R \to H^0(X_0(N)_{/R}, \Omega(\text{cusps})) \end{cases}$$

are isomorphisms of free R-modules of finite rank for any $\mathbb{Z}_{(p)}$-algebra R when $p \parallel N$.

(2) *Similarly*,

$$\begin{cases} H^0(X_0(N)_{/\mathbb{Z}}, \Omega) \otimes_{\mathbb{Z}} R \to H^0(X_0(N)_{/R}, \Omega)\,, \\ H^0(X_0(N)_{/\mathbb{Z}}, \Omega(\text{cusps})) \otimes_{\mathbb{Z}} R \to H^0(X_0(N)_{/R}, \Omega(\text{cusps})) \end{cases}$$

are always isomorphisms of free R-modules of finite rank when N is square-free. □

DEFINITION (1.4.6). We set

$$\begin{cases} S_2^{\mathrm{reg}}(\Gamma_0(N); R) := H^0(X_0(N)_{/R}, \Omega)\,, \\ M_2^{\mathrm{reg}}(\Gamma_0(N); R) := H^0(X_0(N)_{/R}, \Omega(\text{cusps})) \end{cases}$$

in the respective cases considered above.

Thus these are free R-modules of finite rank, and the formation of these spaces commutes with change of base rings considered in (1.4.5). Also, for R as in (1.4.5), there is a morphism: $\mathrm{Spec}(R((q))) \to X_0(N)_{/R}$ corresponding to the cusp at infinity. The pull-back of $\omega \in M_2^{\mathrm{reg}}(\Gamma_0(N); R)$ to $\mathrm{Spec}(R((q)))$ is of the form $f_\omega(q) \cdot dq/q$, and we have the q-expansion mappings

$$\begin{cases} M_2^{\mathrm{reg}}(\Gamma_0(N); R) \to R[[q]]\,, \\ S_2^{\mathrm{reg}}(\Gamma_0(N); R) \to qR[[q]] \end{cases} \quad \text{by } \omega \mapsto f_\omega(q)\,. \tag{1.4.7}$$

PROPOSITION (1.4.8). *Let R be as in* (1.4.5). *In each case, there exist q-expansion preserving mappings*:

$$\begin{cases} S_2^{\mathrm{reg}}(\Gamma_0(N); R) \to S_2^{\mathrm{B}}(\Gamma_0(N); R)\,, \\ M_2^{\mathrm{reg}}(\Gamma_0(N); R) \to M_2^{\mathrm{B}}(\Gamma_0(N); R)\,. \end{cases}$$

These are injections when R is flat over $\mathbb{Z}_{(p)}$ (resp. $\mathbb{Z}$) in the case (1) (*resp. in the case* (2)).

PROOF. Set $R_0 := \mathbb{Z}_{(p)}$ (resp. $\mathbb{Z}$) in the case (1) (resp. in the case (2)).

Since $M_2^{\mathrm{reg}}(\Gamma_0(N); R_0)$ is a free R_0-module, we have

$$M_2^{\mathrm{reg}}(\Gamma_0(N); R_0) \hookrightarrow M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Q}) \overset{(1.4.2)}{=} H^0(X_0(N)_{/\mathbb{Q}}, \Omega^1_{X_0(N)_{/\mathbb{Q}}/\mathbb{Q}}(\mathrm{cusps}))\,.$$

The right hand side is canonically isomorphic to $M_2^{\mathrm{B}}(\Gamma_0(N); \mathbb{Q})$, and hence we have the q-expansion preserving injection

$$M_2^{\mathrm{reg}}(\Gamma_0(N); R_0) \hookrightarrow M_2^{\mathrm{B}}(\Gamma_0(N); \mathbb{Q})\,.$$

From the definitions (1.3.2) and (1.3.3), this gives us an injection

$$M_2^{\mathrm{reg}}(\Gamma_0(N); R_0) \hookrightarrow M_2^{\mathrm{B}}(\Gamma_0(N); R_0)$$

and similarly for cusp forms. Our conclusion follows by base extensions. □

In the case (1), each automorphism $w_d \in G_{\mathrm{AL}}$ (1.1.7) of $X_0(N)_{/\mathbb{Z}_{(p)}}$ induces an involution of $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})$ and $S_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})$

$$\omega \mapsto w_d^*(\omega) =: \omega\,|_2\, w_d$$

by the functoriality of $\Omega_{/\mathbb{Z}_{(p)}}$, which is the unique invertible sheaf on $X_0(N)_{/\mathbb{Z}_{(p)}}$ satisfying (1.4.2) since $X_0(N)_{/\mathbb{Z}_{(p)}}$ is Cohen-Macaulay. Similarly in the case (2), the group G_{AL} acts on $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z})$ and $S_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z})$ by the same rule. It is easy to see that this action is compatible with the action (1.3.8) on classical forms. The involutions obtained from these by base extensions will be also denoted by the same symbols.

PROPOSITION (1.4.9). (1) *When $p \parallel N$, the image of $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})$ in $M_2^{\mathrm{B}}(\Gamma_0(N); \mathbb{Z}_{(p)})$ is the following set*:

$$\{f \in M_2^{\mathrm{B}}(\Gamma_0(N); \mathbb{Z}_{(p)}) \mid (f\,|_2\, w_p)(q) \in \mathbb{Z}_{(p)}[[q]]\}\,.$$

(2) *When N is square-free, the image of $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z})$ in $M_2^{\mathrm{B}}(\Gamma_0(N); \mathbb{Z})$ is the set*:

$$\{f \in M_2^{\mathrm{B}}(\Gamma_0(N); \mathbb{Z}) \mid (f\,|_2\, w_d)(q) \in \mathbb{Z}[[q]] \text{ for all } w_d \in G_{\mathrm{AL}}\}\,.$$

The same statements hold for cusp forms.

PROOF. We give the proof for the second statement; the other cases are similar. It is clear from the argument above that the image is contained in the given set.

To show the reverse inclusion, we follow the argument of [Ma, II, 4] and [G, Proposition 8.4]: Let f be in the given set. We may consider the differential ω_f corresponding to f as a meromorphic section of $\Omega^1_{X_0(N)^{\mathrm{smooth}}_{/\mathbb{Z}}/\mathbb{Z}}$. Since $X_0(N)^{\mathrm{smooth}}_{/\mathbb{Z}}$ is a regular scheme, we can consider the divisor of poles of this section. It is clear that it is disjoint from the generic

fibre. On the other hand, $w_l \in G_{\mathrm{AL}}$ interchanges two irreducible components of $X_0(N)_{/\mathbb{F}_l}$ when $l \mid N$, and hence our hypothesis implies that the polar divisor of ω_f does not contain any irreducible component of the closed fibres. We thus see that ω_f is a holomorphic section of $\Omega^1_{X_0(N)^{\mathrm{smooth}}_{/\mathbb{Z}}/\mathbb{Z}}$. Finally, this section uniquely extends to a section of the invertible sheaf $\Omega_{/\mathbb{Z}}(\mathrm{cusps})$ since $X_0(N)_{/\mathbb{Z}}$ is Cohen-Macaulay, which completes the proof. □

COROLLARY (1.4.10). *Let N be square-free, and let R be a $\mathbb{Z}[1/N]$-algebra. Then the canonical mappings in* (1.4.8) *are isomorphisms.*

PROOF. We may assume that $R = \mathbb{Z}[1/N]$. In this case, the assertion follows from (1.3.8) and the above proposition. (This also follows from the same argument as in the proof of (1.4.9).) □

When N is a prime (≥ 5), Mazur proved that the above assertion is valid for any ring R [Ma, II, Lemma (4.6)]. However, this is not true for general N; cf. the remark at the end of 1.3.

We next consider $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)$ when $p \parallel N$. Set $M = N/p$. In general, there are two "degeneracy" morphisms

$$\text{(1.4.11)} \qquad \begin{cases} \alpha : X_0(N)_{/\mathbb{Z}[1/M]} \to X_0(M)_{/\mathbb{Z}[1/M]}, \\ \beta : X_0(N)_{/\mathbb{Z}[1/M]} \to X_0(M)_{/\mathbb{Z}[1/M]} \end{cases}$$

corresponding to $(E, C_N) \mapsto (E, C_N[M])$ and $(E, C_N) \mapsto (E/C_N[p], C_N/C_N[p])$ for pairs as in (1.1.2), respectively. Recall that there are two irreducible components $Z_\infty :=$ (the image of Φ), and $Z_0 :=$ (the image of $w_p\Phi$) on $X_0(N)_{/\mathbb{F}_p}$, in the notation of (1.1.8). We identify these components with $X_0(M)_{/\mathbb{F}_p}$ via Φ and $w_p\Phi$, respectively. Then we see that

$$\text{(1.4.12)} \qquad \begin{cases} \alpha = \mathrm{id} \text{ on } Z_\infty, \text{ and } \alpha = \mathrm{Frob} \text{ on } Z_0, \\ \beta = \mathrm{Frob} \text{ on } Z_\infty, \text{ and } \beta = \mathrm{id} \text{ on } Z_0, \\ w_p \text{ induces the identity morphism between } Z_\infty \text{ and } Z_0. \end{cases}$$

By (1.4.3), there is a natural injection

$$\text{(1.4.13)} \quad M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p) \hookrightarrow H^0(Z_\infty, \Omega^1_{Z_\infty/\mathbb{F}_p}(\mathrm{cusps}, \mathrm{ss})) \oplus H^0(Z_0, \Omega^1_{Z_0/\mathbb{F}_p}(\mathrm{cusps}, \mathrm{ss}))$$
$$= \bigoplus^2 H^0(X_0(M)_{/\mathbb{F}_p}, \Omega^1_{X_0(M)_{/\mathbb{F}_p}/\mathbb{F}_p}(\mathrm{cusps}, \mathrm{ss}))$$

where "ss" means the reduced divisor supported at the supersingular points. Identifying the

regular differentials with the pairs of differentials on $X_0(M)_{/\mathbb{F}_p}$, we have

(1.4.14)
$$\begin{cases} \alpha^*(\omega) = (\omega, 0) \text{ for } \omega \in H^0(X_0(M)_{/\mathbb{F}_p}, \Omega^1_{X_0(M)_{/\mathbb{F}_p}/\mathbb{F}_p}(\text{cusps})) \cong M_2^{\mathrm{B}}(\Gamma_0(M); \mathbb{F}_p)\,, \\ \beta^*(\omega) = (0, \omega) \text{ for } \omega \in H^0(X_0(M)_{/\mathbb{F}_p}, \Omega^1_{X_0(M)_{/\mathbb{F}_p}/\mathbb{F}_p}(\text{cusps})) \cong M_2^{\mathrm{B}}(\Gamma_0(M); \mathbb{F}_p)\,, \\ w_p^*(\omega_1, \omega_2) = (\omega_2, \omega_1) \text{ for } (\omega_1, \omega_2) \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)\,. \end{cases}$$

From these considerations, we deduce:

LEMMA (1.4.15). *For each sign $\varepsilon = \pm 1$, the q-expansion mapping is injective on the subspace* $\{\omega \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p) \mid \omega\,|_2\, w_p = \varepsilon\omega\}$.

PROOF. In the above notation, an element in this space is of the form $(\omega', \varepsilon\omega')$ with $\omega' \in H^0(X_0(M)_{/\mathbb{F}_p}, \Omega^1_{X_0(M)_{/\mathbb{F}_p}/\mathbb{F}_p}(\text{cusps, ss}))$. Thus, if the q-expansion of this element (at the cusp infinity) vanishes, we have that ω' in the first component is zero. □

CONVENTION (1.4.16). Under the same situation as in (1.4.8), when R is flat over $\mathbb{Z}_{(p)}$ or $\mathbb{Z}$ respectively, we identify $S_2^{\mathrm{reg}}(\Gamma_0(N); R)$ (resp. $M_2^{\mathrm{reg}}(\Gamma_0(N); R)$) with its image in $S_2^{\mathrm{B}}(\Gamma_0(N); R)$ (resp. $M_2^{\mathrm{B}}(\Gamma_0(N); R)$), and use the notation "$f \in M_2^{\mathrm{reg}}(\Gamma_0(N); R)$" by which we mean that $f \in M_2^{\mathrm{B}}(\Gamma_0(N); R)$ and it lies in the image of $M_2^{\mathrm{reg}}(\Gamma_0(N); R)$, especially when we consider the q-expansions. By further abuse of notation, we sometimes express an element of $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p) = M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)}) \otimes_{\mathbb{Z}_{(p)}} \mathbb{F}_p$ by the symbol f and denote its q-expansion by $f(q)$. The same convention applies to cusp forms.

1.5. Hecke operators. Let R be a $\mathbb{Z}[1/N]$-algebra. In [G, §3 and §10], Gross discussed Hecke operators $T(l)$ for prime numbers $l \nmid N$, $U(l)$ for prime numbers $l \mid N$, and the diamond operators $\langle a \rangle$ for $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, acting on $M_k^{\mathrm{A}}(\Gamma_\mu(N); R)$. They all commute, and hence $T(l)$ and $U(l)$ induce endomorphisms of $M_k^{\mathrm{A}}(\Gamma_0(N); R)$ by (1.2.6), (3), for which we use the same symbols. The effect of these operators on q-expansions are given by the usual formulas: Let $f \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$ have the q-expansion $f(q) = \sum_{n=0}^\infty a_n q^n$. Then we have

$$\begin{cases} (f\,|_k\, T(l))(q) = \sum_{n=0}^\infty a_{nl} q^n + l^{k-1} \sum_{n=0}^\infty a_n q^{nl}\,, \\ (f\,|_k\, U(l))(q) = \sum_{n=0}^\infty a_{nl} q^n\,. \end{cases} \tag{1.5.1}$$

These operators on $M_k^{\mathrm{B}}(\Gamma_0(N); \mathbb{Z}[1/N]) = M_k^{\mathrm{A}}(\Gamma_0(N); \mathbb{Z}[1/N])$ are of course the classical Hecke operators, and they preserve $M_k^{\mathrm{B}}(\Gamma_0(N); \mathbb{Z})$. By base extension, we obtain $T(l)$ and $U(l)$ on $M_k^{\mathrm{B}}(\Gamma_0(N); R)$ for arbitrary ring R.

When $l \nmid N$ and R is a $\mathbb{Z}[1/Nl]$- algebra, we may consider $U(l)$ as giving

$$U(l) : M_k^{\mathrm{A}}(\Gamma_0(N); R) \to M_k^{\mathrm{A}}(\Gamma_0(Nl); R)\,. \tag{1.5.2}$$

We have the same operator for arbitrary ring R for "M_k^{B}".

From now on, we assume that k is even, and recall that $M_k^{\mathrm{A}}(\Gamma_0(N); R)$ and $M_k^{\mathrm{B}}(\Gamma_0(N); R)$ are stable under the operators w_d (i.e. "$|_k\, w_d$"; (1.3.6)) for any $\mathbb{Z}[1/N]$-algebra R. The following fact is well-known for $M_k^{\mathrm{B}}(\Gamma_0(N); R)$.

LEMMA (1.5.3). *Under the same situation as above, $T(l)$ and w_d commute on $M_k^{\mathrm{A}}(\Gamma_0(N); R)$.*

PROOF. This must be also more or less well-known, and we will be brief.

Since we need a base changing property of modular forms, which fails to hold for $M_k^{\mathrm{A}}(\Gamma_0(N); R)$, we first work with $M_k^{\mathrm{A}}(\Gamma_\mu(N); R)$. Fix a primitive d-th root of unity ζ_d. Let R be a $\mathbb{Z}[1/N, \zeta_d]$-algebra, and take $f \in M_k^{\mathrm{A}}(\Gamma_\mu(N); R)$. For an elliptic curve $E/S/R$ and a $\Gamma_\mu(N)$-structure i (1.2.1), we view i as $i_d \times i_{N/d}$ with $i_d : \boldsymbol{\mu}_d \hookrightarrow E[d]$ and $i_{N/d} : \boldsymbol{\mu}_{N/d} \hookrightarrow E[N/d]$. We can define $\mathbf{w}_d f \in M_k^{\mathrm{A}}(\Gamma_\mu(N); R)$ by setting

$$\mathbf{w}_d f(E, i_d \times i_{N/d}) := \pi^* f(E', i'_d \times i'_{N/d})$$

where

$$\begin{cases} E' := E/\mathrm{Im}(i_d)\,, \\ \pi : E \to E' \text{: the quotient morphism,} \\ i'_{N/d} : \text{the composite of } \boldsymbol{\mu}_{N/d} \overset{i_{N/d}}{\hookrightarrow} E \overset{\pi}{\to} E'\,, \\ i'_d(\zeta_d) := \pi(t) \text{ with a section } t \text{ of } E[d] \text{ such that } e_d(i_d(\zeta_d), t) = \zeta_d\,. \end{cases}$$

Here, e_d is the e_d-pairing on E.

We claim that, when R is a $\mathbb{Z}[1/Nl, \zeta_d]$-algebra,

$$(\mathbf{w}_d f) |_k\, T(l) = (\mathbf{w}_d (f |_k\, T(l))) |_k\, \langle l \rangle_d$$

where $\langle l \rangle_d$ changes i_d to $l \cdot i_d$ and leaves $i_{N/d}$ unchanged. To see that the both sides take the same value at (E, i) over an R-scheme S, we may replace (E, i) with its base change $(E_{/T}, i_{/T})$ by a faithfully flat morphism $T \to S$, since the canonical mapping $H^0(S, \underline{\omega}_{E/S}^{\otimes k}) \to H^0(T, \underline{\omega}_{E_{/T}/T}^{\otimes k})$ is injective. Further restricting to each connected component of T, we are reduced to the case where S is connected and E admits a $\Gamma(l)$-structure (1.2.1) over S. In this case, the Hecke operator $T(l)$ is given by:

$$f |_k\, T(l)(E, i_d \times i_{N/d}) = \frac{1}{l} \sum_{C_l} p^* f(E/C_l, \tilde{i}_d \times \tilde{i}_{N/d})$$

where the sum is over $(l+1)$ cyclic subgroup schemes of $E[l]$ of order l, $p : E \to E/C_l$ is the quotient morphism, and $\tilde{i}_d := p \circ i_d$ and $\tilde{i}_{N/d} := p \circ i_{N/d}$, [G, (3.3)], [K1, 1.11]. The verification of the desired relation is then direct.

This relation especially holds on $M_k^{\mathrm{A}}(\Gamma_\mu(N); \mathbb{Z}[1/Nl, \zeta_d])$, and hence on its subspace $M_k^{\mathrm{A}}(\Gamma_\mu(N); \mathbb{Z}[1/N, \zeta_d])$ also. Now if $N = 1$, there is nothing to prove. If $N \geq 2$, the

formation of $M_k^{\mathrm{A}}(\Gamma_\mu(N); R)$ commutes with arbitrary base changes of $\mathbb{Z}[1/N, \zeta_d]$-algebras, [G, Proposition 2.5, §10]. (This is why we consider the forms of this type.) We therefore conclude that the above relation holds on $M_k^{\mathrm{A}}(\Gamma_\mu(N); R)$ for any $\mathbb{Z}[1/N, \zeta_d]$-algebra R.

Returning to $f \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$, we deduce from this and (1.2.6), (3) that

$$(\mathbf{w}_d f) \mid_k T(l) = \mathbf{w}_d (f \mid_k T(l))$$

whenever R is a $\mathbb{Z}[1/N, \zeta_d]$-algebra, where $\mathbf{w}_d$ here is defined by (1.2.12). It then follows that the same holds for arbitrary $\mathbb{Z}[1/N]$-algebras R. □

We will also need another operator $B(l)$: Let l be a prime number which may or may not divide N. When $f \in M_k(\Gamma_0(N))$, it is given by $f \mid_k B(l) := l^{-k/2} f \mid_k \begin{bmatrix} l & 0 \\ 0 & 1 \end{bmatrix}$. It is clear that, if $f(q) = \sum_{n=0}^{\infty} a_n q^n$, we have $(f \mid_k B(l))(q) = \sum_{n=0}^{\infty} a_n q^{nl} = f(q^l)$, and that this operator induces a mapping

$$B(l) : M_k^{\mathrm{B}}(\Gamma_0(N); R) \to M_k^{\mathrm{B}}(\Gamma_0(Nl); R) \tag{1.5.4}$$

for any ring R.

As for $M_k^{\mathrm{A}}(\Gamma_0(N); R)$, we proceed as follows. Let R be a $\mathbb{Z}[1/Nl]$-algebra. For $f \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$, we define $f \mid_k B(l)$ by

$$(f \mid_k B(l))(E, C_{Nl}) := l^{-k} \pi^* f(E/C_{Nl}[l], C_{Nl}/C_{Nl}[l]) \tag{1.5.5}$$

for elliptic curves $E/S/\mathbb{Z}[1/Nl]$ and its $\Gamma_0(Nl)$-structure C_{Nl}, $\pi : E \to E/C_{Nl}[l]$ being the quotient morphism.

LEMMA (1.5.6). *Let R be a $\mathbb{Z}[1/Nl]$-algebra. Then the formula* (1.5.5) *defines mappings*

$$\begin{cases} B(l) : M_k^{\mathrm{A}}(\Gamma_0(N); R) \to M_k^{\mathrm{A}}(\Gamma_0(Nl); R), \\ B(l) : S_k^{\mathrm{A}}(\Gamma_0(N); R) \to S_k^{\mathrm{A}}(\Gamma_0(Nl); R). \end{cases}$$

If f is in the left hand sides, we have

$$(f \mid_k B(l))(q) = f(q^l).$$

PROOF. The first assertion is clear. As for the second, consider the Tate curve $\mathrm{Tate}(q)$ over $R((q))$ with the canonical $\Gamma_0(Nl)$-structure $C_{Nl,\mathrm{can}}$ (1.2.8), and the canonical invariant differential ω_{can}. Then we see that $\mathrm{Tate}(q)/C_{Nl}[l] \cong \mathrm{Tate}(q^l)$ through which $C_{Nl,\mathrm{can}}/C_{Nl,\mathrm{can}}[l] \cong C_{N,\mathrm{can}}$. Moreover if π is the composite of $\mathrm{Tate}(q) \to \mathrm{Tate}(q)/C_{Nl}[l] \xrightarrow{\sim} \mathrm{Tate}(q^l)$, the pull-back of the canonical invariant differential ω'_{can} on $\mathrm{Tate}(q^l)$ by π is $l\omega_{\mathrm{can}}$ (see [K1, 1.11] for these). We therefore have

$$l^k (f \mid_k B(l))(q) \omega_{\mathrm{can}}^{\otimes k} = l^k (f \mid_k B(l))(\mathrm{Tate}(q), C_{Nl,\mathrm{can}})$$

$$= \pi^*(f_0(\mathrm{Tate}(q^l), C_{N,\mathrm{can}}, \omega'^{\otimes k}_{\mathrm{can}})\omega'^{\otimes k}_{\mathrm{can}}) = l^k f(q^l)\omega^{\otimes k}_{\mathrm{can}}$$

which completes the proof. □

LEMMA (1.5.7). *Let d be a positive divisor of N such that $(d, N/d) = 1$, and l a prime number not dividing d. Consider the mappings*

$$\begin{cases} U(l) : M_k^{\mathrm{A}}(\Gamma_0(N); R) \to M_k^{\mathrm{A}}(\Gamma_0(N); R) \text{ for a } \mathbb{Z}[1/N]\text{-algebra } R \text{ when } l \mid N, \\ U(l) : M_k^{\mathrm{A}}(\Gamma_0(N); R) \to M_k^{\mathrm{A}}(\Gamma_0(Nl); R) \text{ for a } \mathbb{Z}[1/Nl]\text{-algebra } R \text{ when } l \nmid N, \\ B(l) : M_k^{\mathrm{A}}(\Gamma_0(N); R) \to M_k^{\mathrm{A}}(\Gamma_0(Nl); R) \text{ for a } \mathbb{Z}[1/Nl]\text{-algebra } R. \end{cases}$$

In each case, the operator w_d on the left hand side commutes with w_d on the right hand side.

PROOF. The proof is easier than that of (1.5.3) because l is invertible in R in each case. The assertions can be checked directly by using the explicit formula of $U(l)$, $B(l)$ and w_d given in [G, (3.6)], (1.5.5) and (1.2.12), respectively. □

Finally, we have the following

PROPOSITION (1.5.8) (cf. [G, Proposition 8.7]). *Let the situation be as in* (1.4.9).

(1) *When $p \parallel N$, $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})$ is stable under all $T(l)$ and $U(l)$.*

(2) *When N is square-free, $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z})$ is stable under all $T(l)$ and $U(l)$.*

Consequently, we can consider these operators on $M_2^{\mathrm{reg}}(\Gamma_0(N); R)$ for any $\mathbb{Z}_{(p)}$-algebra R in the case (1), *and for any ring R in the case* (2).

PROOF. We give the proof for the part (2); the other part is similar. Let p be a prime factor of N.

When $p \neq l$, $T(l)$ or $U(l)$ and w_p commute on $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Q})$ (by (1.5.3) and (1.5.7); or rather, by the well-known such commutativity for classical forms). Thus if $f \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z})$, $(f\,|_2\,T(l))\,|_2 w_p$ and $(f\,|_2\,U(l))\,|_2 w_p$ have integral q-expansions by (1.4.9). When $p = l$, set $U(p)' = w_p U(p) w_p$. By [G, Proposition 6.10], $f\,|_2\,U(p)'$ also has integral q-expansion, and hence $(f\,|_2\,U(p))\,|_2\,w_p = (f\,|_2\,w_p)\,|_2\,U(p)'$ has the same property.

Our claim now follows from (1.4.9). □

2. Results on modular forms

2.1. Results of Atkin-Lehner type. From now on, we assume that the weight k is an even positive integer.

LEMMA (2.1.1). *Let l be a prime number such that $l \parallel N$, and R a $\mathbb{Z}[1/N]$-algebra. Let f be an element of $M_k^{\mathrm{A}}(\Gamma_0(N); R)$ whose q-expansion $f(q)$ is a power series in q^l. Then*

there is a $g \in M_k^{\mathrm{A}}(\Gamma_0(N/l); R)$ *such that*

$$\begin{cases} f = l^{-k/2} g \mid_k w_l = l^{-k}(\mathbf{w}_l g) \ \ (cf.\ (1.3.6)), \\ f(q) = g(q^l). \end{cases}$$

PROOF. When $R = \mathbb{C}$, this is Atkin and Lehner [AL, Lemma 16]. The assertion was proved by Mazur when $N = l\ (\geq 5)$ [Ma, II, Lemma (5.9)], and Agashe [A, Lemma 3.4] remarked that the same proof applies in general (at least when $k = 2$ and N is square-free).

One can also argue as in [Oh2, Lemma (1.3.4)]. Since this lemma is of fundamental importance to what follows, we outline the proof. First, we may assume that R is a $\mathbb{Z}[1/N, \zeta_N]$-algebra, ζ_N being a primitive N-th root of unity. Then the exact sequence (1.2.7) canonically splits over $R((q^{1/N}))$, identifying $\mathrm{Tate}(q)[N]$ with $\{\zeta_N^a q^{b/N} \mid 0 \leq a, b \leq N-1\}$. We thus have the canonical $\Gamma(N)$-structure

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

by $\phi_{\mathrm{can}}(a, b) = \zeta_N^a q^{b/N}$.

Recall that we may identify $h \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$ with an element of $M_k^{\mathrm{A}}(\Gamma(N); R)$ by setting $h(E, \phi) := h(E, C_{N,\phi})$ as described before (1.2.6). Then $\mathbf{w}_l f \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$ is invariant under the action of the upper triangular matrices in $GL_2(\mathbb{Z}/N\mathbb{Z}) = GL_2(\mathbb{Z}/N'\mathbb{Z}) \times GL_2(\mathbb{Z}/l\mathbb{Z})$, where $N' := N/l$ (cf. (1.2.6), (1)), and we want to show that this is invariant under $GL_2(\mathbb{Z}/l\mathbb{Z})$ (cf. (1.2.6), (2)), equivalently that it is invariant under the lower triangular unipotent matrices in $GL_2(\mathbb{Z}/l\mathbb{Z})$.

To see this, we note that

$$\left(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}_l \mathbf{w}_l f\right)(q) = f(q^{1/l})$$

where $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}_l \in SL_2(\mathbb{Z}/l\mathbb{Z})$, and the left hand side is the q-expansion of the form at the cusp infinity, i.e. the evaluation at $(\mathrm{Tate}(q), \phi_{\mathrm{can}}, \omega_{\mathrm{can}}^{\otimes k})$. Indeed, this can be proved in the same manner as [Oh2, Lemma (1.3.4)].

Now it follows from our hypothesis that $f(q^{1/l})$ is a power series in q, which implies that $\left(\begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix}_l \mathbf{w}_l f\right)(q) = (\mathbf{w}_l f)(q)$ for any $\begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix}_l \in SL_2(\mathbb{Z}/l\mathbb{Z})$ (loc. cit.). Since $\mathbf{w}_l f$ is a priori invariant under any $\begin{bmatrix} c & 0 \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z})$, we have that the same holds for $\begin{bmatrix} c & 0 \\ 0 & 1 \end{bmatrix} \mathbf{w}_l f = \mathbf{w}_l f$ trivially. We can therefore apply the q-expansion principle [K1, Theorem 1.6.1, Corollary 1.9.1] to conclude that $\begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix}_l \mathbf{w}_l f = \mathbf{w}_l f$ for any $\begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix}_l \in SL_2(\mathbb{Z}/l\mathbb{Z})$. We have that $g := \mathbf{w}_l f$ belongs to $M_k^{\mathrm{A}}(\Gamma_0(N/l); R)$, and the first relation in our claim holds.

Finally, in general, we have $l^{-k}(\mathbf{w}_l g)(q) = g(q^l)$ when $g \in M_k^{\mathrm{A}}(\Gamma_0(N/l); R)$. Indeed,

$g(E, C_N)$ depends only on the $\Gamma_0(N/l)$-structure underlying C_N, and hence we have

$$l^{-k}(\mathbf{w}_l g)(E, C_N) = l^{-k}\pi^* g(E/C_N[l], C_N/C_N[l]) = (g \mid_k B(l))(E, C_N)$$

with $\pi : E \to E/C_N[l]$ the quotient morphism (cf. (1.5.5)). Our claim follows from (1.5.6). □

The following is a weaker version of [AL, Theorem 1]:

PROPOSITION (2.1.2). *Let $l_1, \dots, l_s$ be primes dividing N, and R a $\mathbb{Z}[1/N]$-algebra. Assume that $f \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$ has the q-expansion $f(q) = \sum_{n=0}^{\infty} a_n q^n$ such that $a_n = 0$ unless n is divisible by some l_i, $1 \le i \le s$. If $l_s \parallel N$ and $f \mid_k w_{l_s} = \pm f$, we have that*

$$\begin{cases} a_n = 0 \text{ unless } n \text{ is divisible by some } l_i,\ 1 \le i \le s-1, \text{ when } s \ge 2\,, \\ f(q) \text{ is a constant when } s = 1\,. \end{cases}$$

PROOF. First assume that $s \ge 2$. In general, if $g \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$ and $g(q) = \sum_{n=0}^{\infty} b_n q^n$, we see from (1.5.1) and (1.5.6) that

$$(g \mid_k (1 - U(l_i)B(l_i)))(q) = \sum_{\substack{n=0 \\ l_i \nmid n}}^{\infty} b_n q^n$$

with $g \mid_k (1 - U(l_i)B(l_i)) \in M_k^{\mathrm{A}}(\Gamma_0(Nl_i); R)$. From the above form of the q-expansion, we see that the operators $1 - U(l_i)B(l_i)$ commute each other.

Set $h := f \mid_k \prod_{i=1}^{s-1}(1 - U(l_i)B(l_i)) \in M_k^{\mathrm{A}}(\Gamma_0(Nl_1 \cdots l_{s-1}); R)$. Then $h(q)$ is a power series in q^{l_s}, and hence the previous lemma implies that there is an $h' \in M_k^{\mathrm{A}}(\Gamma_0(Nl_1 \cdots l_{s-1}/l_s); R)$ such that $h = l_s^{-k/2} h' \mid_k w_{l_s}$, or equivalently, $h \mid_k w_{l_s} = l_s^{-k/2} h'$, and $h(q) = h'(q^{l_s})$.

By (1.5.7), $1 - U(l_i)B(l_i)$ $(1 \le i \le s-1)$ and w_{l_s} commute, and hence we have $h \mid_k w_{l_s} = \pm h$ by the assumption. We therefore have $\pm h = l_s^{-k/2} h'$, which implies that $h(q)$ must be a constant. We have thus shown that $a_n = 0$ unless n is divisible by one of $l_1, \dots, l_{s-1}$.

When $s = 1$, we can repeat the same argument as above for $f = h$. □

DEFINITION (2.1.3). We use the following terminology when $N = l_1 \cdots l_m > 1$ is square-free with prime numbers $l_1, \dots, l_m$: We set $\boldsymbol{E} := \{\pm 1\}^m$. If R is a $\mathbb{Z}[1/2]$-algebra and M is an $R[G_{\mathrm{AL}}]$-module (cf. (1.1.7)), for each $\boldsymbol{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_m) \in \boldsymbol{E}$, we let $M^{\boldsymbol{\varepsilon}}$ be the maximum direct summand of M on which w_{l_i} acts as multiplication by ε_i $(1 \le i \le m)$, so that

$$M = \bigoplus_{\boldsymbol{\varepsilon} \in \boldsymbol{E}} M^{\boldsymbol{\varepsilon}}\,.$$

We remind of us that when R is a $\mathbb{Z}[1/N]$-algebra, $M_k^{\mathrm{A}}(\Gamma_0(N); R)$ and $M_k^{\mathrm{B}}(\Gamma_0(N); R)$ are G_{AL}-modules by $w_d : f \mapsto f|_k w_d$ for arbitrary N; cf. 1.3. When N is square-free, $M_2^{\mathrm{reg}}(\Gamma_0(N); R)$ is a G_{AL}-module for arbitrary R by the same rule; cf. 1.4. We immediately obtain from (2.1.2) the following

COROLLARY (2.1.4). *Let $N = l_1 \cdots l_m > 1$ be square-free, and R a $\mathbb{Z}[1/2N]$-algebra. If f is an element of $M_k^{\mathrm{A}}(\Gamma_0(N); R)^{\varepsilon}$ having the q-expansion $f(q) = \sum_{n=0}^{\infty} a_n q^n$ such that $a_n = 0$ unless $(n, N) > 1$, then $f(q)$ is a constant.* □

2.2. Regular differentials in characteristic p. For the moment, until (2.2.6) below, we assume that p is an odd prime, and $N = pM$ with M not divisible by p. We are going to follow the argument of Serre [Se2, §3].

It is easy to see that we have a disjoint decomposition

$$\Gamma_0(M) = \Gamma_0(N) \coprod \left(\coprod_{i=0}^{p-1} \Gamma_0(N) \frac{1}{p} W_p \begin{bmatrix} 1 & i \\ 0 & p \end{bmatrix} \right) \tag{2.2.1}$$

where W_p is a matrix of the form (1.1.5). For $f \in M_k(\Gamma_0(N))$, we set

$$\mathrm{Tr}_M^N(f) := f + \sum_{i=0}^{p-1} f|_k \frac{1}{p} W_p \begin{bmatrix} 1 & i \\ 0 & p \end{bmatrix} \in M_k(\Gamma_0(M)) . \tag{2.2.2}$$

It easily follows that

$$\begin{cases} \mathrm{Tr}_M^N(f) = f + p^{1-k/2}(f|_k w_p)|_k U(p) , \\ \mathrm{Tr}_M^N(f|_k w_p) = f|_k w_p + p^{1-k/2} f|_k U(p) \end{cases} \tag{2.2.3}$$

(cf. [Se2, §3, Lemme 7]).

PROPOSITION (2.2.4). *Let $N = pM$ be as above. Then there is a q-expansion preserving $\mathbb{F}_p$-linear mapping*

$$\varphi_p : M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p) \to M_{p+1}^{\mathrm{A}}(\Gamma_0(M); \mathbb{F}_p)$$

such that

$$\varphi_p(f|_2 w_d) = \left(\frac{d}{p}\right) \varphi_p(f)|_{p+1} w_d$$

for any positive divisor d of M satisfying $(d, M/d) = 1$ (hence $(d, N/d) = 1$), where $\left(\frac{*}{p}\right)$ is the Legendre symbol.

PROOF. First we give the proof when $p \geq 5$, in which case the mapping φ_p actually

takes values in $M^{\mathrm{B}}_{p+1}(\Gamma_0(M);\mathbb{F}_p)$. Let

$$E_{p-1} = 1 - \frac{2(p-1)}{B_{p-1}} \sum_{n=1}^{\infty} \Big(\sum_{0<t|n} t^{p-2} \Big) q^n$$

($q = e^{2\pi i z}$) be the Eisenstein series of weight $p-1$ and level 1. Here, B_{p-1} is the $(p-1)$st Bernoulli number, and it is well-known that $2(p-1)/B_{p-1}$ is divisible by p so that $E_{p-1} \equiv 1 \pmod{p}$. (Here and below, the congruences mean the ones for the corresponding q-expansions considered in $\mathbb{Z}_{(p)}[[q]]$.) Set

$$g := E_{p-1} - p^{(p-1)/2} E_{p-1} \mid_{p-1} w_p = E_{p-1} - p^{p-1} E_{p-1} \mid_{p-1} B(p)\,.$$

This form belongs to $M^{\mathrm{B}}_{p-1}(\Gamma_0(p);\mathbb{Z}_{(p)})$ and we clearly have $g \equiv 1 \pmod{p}$. Since $g \mid_{p-1} w_p = p^{(p-1)/2}(E_{p-1} \mid_{p-1} B(p) - E_{p-1})$, we see that $g \mid_{p-1} w_p \equiv 0 \pmod{p^{(p+1)/2}}$.

Let F be an element of $M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})$, and recall that this space is stable under G_{AL}; cf. 1.4. We have

$$\begin{cases} \mathrm{Tr}^N_M(Fg) \in M^{\mathrm{B}}_{p+1}(\Gamma_0(M);\mathbb{Z}_{(p)})\,, & \text{and} \\ \mathrm{Tr}^N_M(Fg) \equiv F \pmod{p}\,. \end{cases}$$

Indeed, we have $\mathrm{Tr}^N_M(Fg) - Fg = p^{1-(p+1)/2}((Fg) \mid_{p+1} w_p \mid_{p+1} U(p))$ by (2.2.3). Since $(Fg) \mid_{p+1} w_p = (F \mid_2 w_p)(g \mid_{p-1} w_p)$, we see from the above that $\mathrm{Tr}^N_M(Fg) - Fg \in M^{\mathrm{B}}_{p+1}(\Gamma_0(M);\mathbb{Z}_{(p)})$ and it is congruent to 0 (mod p).

We now define $\varphi_p : M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{F}_p) \to M^{\mathrm{B}}_{p+1}(\Gamma_0(M);\mathbb{F}_p)$ as follows: For f in the left hand side, take $F \in M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})$ such that $f = F \pmod{p}$; cf. (1.4.5), (1). We put

$$\varphi_p(f) := \mathrm{Tr}^N_M(Fg) \pmod{p}\,.$$

It is easy to see that this is well-defined, and φ_p preserves q-expansions.

We next show that φ_p has the desired compatibility with w_d. To see this, we first note that, for d as in our proposition, $W_d = \begin{bmatrix} dx & y \\ Nz & dw \end{bmatrix}$ normalizes both $\Gamma_0(M)$ and $\Gamma_0(N)$, and hence

$$\varphi_p(f) \mid_{p+1} w_d = \mathrm{Tr}^N_M((Fg) \mid_{p+1} w_d) \pmod{p}$$

$$= \mathrm{Tr}^N_M((F \mid_2 w_d)(g \mid_{p-1} w_d)) \pmod{p}\,.$$

Here, we have $(g \mid_{p-1} w_d)\mid_{p-1} w_p = (g \mid_{p-1} w_p)\mid_{p-1} w_d = (g \mid_{p-1} w_p)\mid_{p-1} \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix} \equiv 0 \pmod{p^{(p+1)/2}}$. It follows again from (2.2.3) that

$$\varphi_p(f) \mid_{p+1} w_d = (F \mid_2 w_d)(g \mid_{p-1} w_d) \pmod{p}\,.$$

On the other hand, it follows from $g\,|_{p-1}\,w_d = g\,|_{p-1}\begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix}$ that $g\,|_{p-1}\,w_d \equiv d^{(p-1)/2} \equiv \left(\frac{d}{p}\right) \pmod{p}$. Consequently, we obtain

$$(F\,|_2\,w_d)(g\,|_{p-1}\,w_d) \equiv \left(\frac{d}{p}\right) F\,|_2\,w_d \equiv \left(\frac{d}{p}\right) \mathrm{Tr}_M^N((F\,|_2\,w_d)g) \pmod{p}$$

which completes the proof when $p \geq 5$.

We next turn to the case $p = 3$. Take a prime $l \equiv 2 \pmod 3$ which does not divide N. Then we have the Eisenstein series

$$E_{2,l} = 1 + \frac{24}{l-1}\sum_{n=1}^{\infty}\Bigg(\sum_{\substack{0<t|n \\ l\nmid t}} t\Bigg)q^n$$

which belongs to $M_2^{\mathrm{B}}(\Gamma_0(l); \mathbb{Z}_{(3)})$. This is congruent to 1 (mod 3) by our assumption on l. Then using $g_l := E_{2,l} - 3E_{2,l}\,|_2\,w_3$ instead of g, we obtain

$$\varphi_{3,l} : M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_3) \to M_4^{\mathrm{B}}(\Gamma_0(Ml); \mathbb{F}_3)$$

by $\varphi_{3,l}(f) := \mathrm{Tr}_{Ml}^{Nl}(Fg_l) \pmod 3$, where as before $F \in M_2^{\mathrm{reg}}(\Gamma_0(N), \mathbb{Z}_{(3)})$ satisfies $F \pmod 3 = f$. This mapping has the same compatibility for the action of w_d as above.

Take another prime $l' \equiv 2 \pmod 3$, which does not divide Nl, and consider also $\varphi_{3,l'} : M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_3) \to M_4^{\mathrm{B}}(\Gamma_0(Ml'); \mathbb{F}_3)$. Then the composite of $\varphi_{3,l}$ with the natural mappings $M_4^{\mathrm{B}}(\Gamma_0(Ml); \mathbb{F}_3) \hookrightarrow M_4^{\mathrm{A}}(\Gamma_0(Ml); \mathbb{F}_3) \hookrightarrow M_4^{\mathrm{A}}(\Gamma_0(Mll'); \mathbb{F}_3)$ and the similar one for $\varphi_{3,l'}$ coincide by the q-expansion principle. On the other hand, we see that the commutative diagram with natural injections

$$\begin{array}{ccc} M_4^{\mathrm{A}}(\Gamma_0(M); \mathbb{F}_3) & \longrightarrow & M_4^{\mathrm{A}}(\Gamma_0(Ml); \mathbb{F}_3) \\ \downarrow & & \downarrow \\ M_4^{\mathrm{A}}(\Gamma_0(Ml'); \mathbb{F}_3) & \longrightarrow & M_4^{\mathrm{A}}(\Gamma_0(Mll'); \mathbb{F}_3) \end{array}$$

is cartesian. This follows from the fact that, for example, the image of the upper horizontal mapping consists of those $f \in M_4^{\mathrm{A}}(\Gamma_0(Ml); \mathbb{F}_3)$ such that the values $f(E, C_{Ml})$ depend only on $(E, C_{Ml}[M])$, and likewise for other mappings (cf. (1.2.6), (2)). We therefore obtain from $\varphi_{3,l}$ and $\varphi_{3,l'}$ the desired mapping φ_3. □

Sometimes, the following weaker version suffices for our purposes, and is in fact convenient for notational reasons, since we do not have to take care of the change of signs.

VARIANT (2.2.5). *Let $N = pM$ be as above. Then there is a q-expansion preserving $\mathbb{F}_p$-linear mapping*

$$\varphi'_p : M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p) \to M_{2p}^{\mathrm{B}}(\Gamma_0(M); \mathbb{F}_p)$$

which commutes with the operators w_d for positive divisors d of M such that $(d, M/d) = 1$.

PROOF. Apply the same argument as in the above proof in the case $p \geq 5$, using

$$E_{2(p-1)} = 1 - \frac{4(p-1)}{B_{2(p-1)}} \sum_{n=1}^{\infty} \Big(\sum_{0<t|n} t^{2p-3} \Big) q^n . \qquad \square$$

We now list some consequences of the above results.

PROPOSITION (2.2.6). *Let $N = pM$ be as above. Let f be an element of $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)$ with the q-expansion $f(q) = \sum_{n=0}^{\infty} a_n q^n$.*

(1) If $f(q)$ is a power series in q^p, then $f(q)$ is a constant. We moreover have $f(q) = 0$ when $p \geq 5$.

(2) If $M > 1$ and $a_n = 0$ unless $(n, N) > 1$, then we have $a_n = 0$ unless $(n, M) > 1$.

PROOF. By (2.2.4), $f' := \varphi_p(f) \in M_{p+1}^{\mathrm{A}}(\Gamma_0(M); \mathbb{F}_p)$ has the same q-expansion as f.

We first prove the part (1). There is a q-expansion preserving injection $M_{p+1}^{\mathrm{A}}(\Gamma_0(M); \mathbb{F}_p) \hookrightarrow M_{p+1}^{\mathrm{A}}(\Gamma_\mu(M'); \mathbb{F}_p)$ for any positive multiple M' of M prime to p. Thus fixing such an $M' \geq 4$, it is enough to show the same assertion as in (1) for $g \in M_{p+1}^{\mathrm{A}}(\Gamma_\mu(M'); \mathbb{F}_p)$ in place of f. To do this, we use the filtration theory of modular forms (mod p) developed by Serre, Katz and Gross.

When $h \in M_k^{\mathrm{A}}(\Gamma_\mu(M'); \mathbb{F}_p)$, we denote by $w(h)$ its filtration: If $h = 0$, we set $w(h) = -\infty$, and if $h \neq 0$, $w(h)$ is the least non-negative integer such that there exists an $h' \in M_{w(h)}^{\mathrm{A}}(\Gamma_\mu(M'); \mathbb{F}_p)$ satisfying $h(q) = h'(q)$, in which case $w(h)$ is congruent to k modulo $p-1$, cf. [G, page 459]. On the other hand, there is the Serre-Katz operator $\theta : M_k^{\mathrm{A}}(\Gamma_\mu(M'); \mathbb{F}_p) \to M_{k+p+1}^{\mathrm{A}}(\Gamma_\mu(M'); \mathbb{F}_p)$ whose effect on q-expansions is $q(d/dq)$.

Now if the q-expansion of $g \in M_{p+1}^{\mathrm{A}}(\Gamma_\mu(M'); \mathbb{F}_p)$ is a power series in q^p, it is annihilated by θ so that $w(g)$ must be divisible by p by [G, Proposition 4.10, a)]. If $g \neq 0$, i.e. $w(g) \neq -\infty$, we have $w(g) \equiv p+1 \pmod{p-1}$, which is impossible when $p \geq 5$. When $p = 3$, we have either $w(g) = 0$ or $-\infty$, i.e. $g(q)$ is a constant.

As for (2), let $l_1, \ldots, l_t$ be all the prime factors of M. Using the same notation as in the proof of (2.1.2), set

$$f'' := f' \,|_{p+1} \prod_{i=1}^{t} (1 - U(l_i)B(l_i)) \in M_{p+1}^{\mathrm{A}}(\Gamma_0(Ml_1 \cdots l_t); \mathbb{F}_p) .$$

Then $f''(q)$ is a power series in q^p. We have seen in the course of the proof of (1) that $f''(q)$ is a constant, and hence our conclusion follows. $\square$

Note that, as is well-known, the assertion (2.2.6), (1) holds for $f \in M_2^{\mathrm{A}}(\Gamma_0(N); \mathbb{F}_p)$ when p does not divide N (for the same reason as above).

In the rest of this subsection, p need not divide N.

PROPOSITION (2.2.7). *Let $N = l_1 \cdots l_m > 1$ be square-free, and p an odd prime. Let $f \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)$ have the q-expansion $f(q) = \sum_{n=0}^{\infty} a_n q^n$. Assume that there are prime factors $l_1, \ldots, l_s$ of N different from p such that $a_n = 0$ unless n is divisible by some l_i, $1 \le i \le s$. If $f \mid_2 w_{l_s} = \pm f$, we have that*

$$\begin{cases} a_n = 0 \text{ unless } n \text{ is divisible by some } l_i,\ 1 \le i \le s-1 \text{ when } s \ge 2\,, \\ f(q) \text{ is a constant when } s = 1\,. \end{cases}$$

PROOF. If p does not divide N, this follows immediately from (2.1.2). When p divides N, we can apply (2.1.2) to $\varphi_p(f) \in M_{p+1}^{\mathrm{A}}(\Gamma_0(N/p); \mathbb{F}_p)$ (or $\varphi_p'(f) \in M_{2p}^{\mathrm{B}}(\Gamma_0(N/p); \mathbb{F}_p)$). □

COROLLARY (2.2.8). *Let N and p be as in* (2.2.7). *Assume that $f \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)^{\boldsymbol{\varepsilon}}$ with some $\boldsymbol{\varepsilon} \in \boldsymbol{E}$ (cf.* (2.1.3)) *has the q-expansion $f(q) = \sum_{n=0}^{\infty} a_n q^n$ such that $a_n = 0$ unless $(n, N) > 1$. Then $f(q)$ is a constant. If $p \ge 5$, we have $f(q) = 0$.*

PROOF. This follows from (2.2.6) and (2.2.7). □

2.3. Eisenstein series. From now on, we fix a square-free level $N > 1$ whose prime decomposition is $N = l_1 \cdots l_m$. We are going to describe the Eisenstein series in $M_2(\Gamma_0(N))$.

For this, recall Hecke's non-holomorphic Eisenstein series [H, §2]:

$$G_2(z; 0, 0, 1) = -\frac{\pi}{y} + \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \Big(\sum_{0<t\mid n} t \Big) q^n \tag{2.3.1}$$

where $z = x + yi$ is the variable on H. It is invariant under the action (1.3.1) of any $\gamma \in SL_2(\mathbb{Z})$ with $k = 2$.

Set $K(z) := -(8\pi^2)^{-1} G_2(z; 0, 0, 1)$ so that

$$K(z) = \frac{1}{8\pi y} - \frac{1}{24} + \sum_{n=1}^{\infty} \Big(\sum_{0<t\mid n} t \Big) q^n\,. \tag{2.3.2}$$

One can define $K \mid_2 W_d$ for W_d as in (1.1.5), and it is clear that this depends only on d, and we write it $K \mid_2 w_d$, as before.

In what follows, we sometimes have to distinguish the sign

$$\boldsymbol{\varepsilon}_+ := (+1, \ldots, +1) \in \boldsymbol{E} \tag{2.3.3}$$

from others.

LEMMA (2.3.4). *For each $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_m) \in \boldsymbol{E}$ different from $\boldsymbol{\varepsilon}_+$, set*

$$E_{\boldsymbol{\varepsilon}} := K \mid_2 \prod_{i=1}^{m} (1 + \varepsilon_i w_{l_i})\,.$$

This belongs to $M_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}}$. *It has the* q*-expansion of the form*

$$E_{\boldsymbol{\varepsilon}}(q) = \pm\frac{1}{24}\prod_{i=1}^{m}(l_i + \varepsilon_i) + \sum_{n=1}^{\infty} a_n q^n$$

with $a_n \in \mathbb{Z}$, *and* $a_n = \sum_{0<t|n} t$ *when* $(n, N) = 1$ (*especially* $a_1 = 1$). *These* $2^m - 1$ *forms constitute a basis of the space of Eisenstein series in* $M_2(\Gamma_0(N))$.

PROOF. The operator "$|_2 \prod_{i=1}^{m}(1 + \varepsilon_i w_{l_i})$" does not depend on the order of the product. Since $\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+$, some ε_i is equal to -1. Then the non-holomorphic term of $K\,|_2\,(1 - w_{l_i})$ vanishes, and it is equal to

$$E'_{2,l_i} = \frac{l_i - 1}{24} + \sum_{n=1}^{\infty}\Bigg(\sum_{\substack{0<t|n \\ l_i \nmid t}} t\Bigg)q^n$$

which is the constant multiple of the Eisenstein series $E_{2,l_i} \in M_2(\Gamma_0(l_i))$ appeared in the proof of (2.2.4).

Starting from this, each time one applies "$|_2\,(1+\varepsilon_j w_{l_j})$", the constant term is multiplied by $\varepsilon_j l_j + 1$, while the coefficients of q^n $(n > 0)$ remain integral and unchanged whenever $l_j \nmid n$. Therefore $E_{\boldsymbol{\varepsilon}}$ belongs to $M_2(\Gamma_0(N))$ and it has the q-expansion of the form as stated above.

From the definition, it is clear that $E_{\boldsymbol{\varepsilon}}\,|_2\,w_{l_k} = \varepsilon_k E_{\boldsymbol{\varepsilon}}$, and hence $E_{\boldsymbol{\varepsilon}} \in M_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}}$. It then follows that the forms $E_{\boldsymbol{\varepsilon}}$ $(\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+)$ are linearly independent over $\mathbb{C}$. Since the dimension of the space of Eisenstein series in $M_2(\Gamma_0(N))$ is equal to #(the cusps of $X_0(N)$)$-1 = 2^m - 1$, our conclusion follows. □

COROLLARY (2.3.5). *We have*

$$\begin{cases} M_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}_+} = S_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}_+}, \\ M_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}} = S_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}} \oplus \mathbb{C}E_{\boldsymbol{\varepsilon}} \text{ when } \boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+. \end{cases}$$

□

We next consider when there is an element of $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)^{\boldsymbol{\varepsilon}}$ whose q-expansion is a non-zero constant. We have seen in the previous subsection (cf. (2.2.6) and the remark after it) that there is no such an element when $p \geq 5$. On the other hand, when $p = 3$, there is an $H \in M_2^{\mathrm{A}}(\Gamma_0(1); \mathbb{F}_3)$ such that $H(q) = 1$, which is given by the Hasse invariants of elliptic curves. When 3 does not divide N, the argument in the final part of the proof of (2.1.1) shows:

$$(H\,|_2\,w_{l_i})(q) = l_i = \left(\frac{l_i}{3}\right) \quad (i = 1, \ldots, m)\,. \tag{2.3.6}$$

We therefore set

$$\boldsymbol{\varepsilon}_H := \left(\left(\frac{l_1}{3}\right), \ldots, \left(\frac{l_m}{3}\right)\right) \text{ when } 3 \nmid N\,. \tag{2.3.7}$$

When $3 \mid N$, we may assume that $l_1 = 3$, and set

$$\text{(2.3.8)} \qquad \begin{cases} \boldsymbol{\varepsilon}_H^+ := \left(+1, \left(\frac{l_2}{3}\right), \ldots, \left(\frac{l_m}{3}\right)\right), \\ \boldsymbol{\varepsilon}_H^- := \left(-1, \left(\frac{l_2}{3}\right), \ldots, \left(\frac{l_m}{3}\right)\right) \end{cases} \quad \text{when} \quad l_1 = 3 \mid N\,.$$

Using (1.4.9), (1) if $p \mid N$, we see that $E_{\boldsymbol{\varepsilon}}$ ($\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}^+$) belongs to $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$ except for the case where $p = 3$ and $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H$ or $\boldsymbol{\varepsilon}_H^{\pm}$. In this exceptional case, $3E_{\boldsymbol{\varepsilon}}$ belongs to $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(3)})^{\boldsymbol{\varepsilon}}$, and the q-expansion of its reduction modulo 3 is a non-zero constant.

PROPOSITION (2.3.9). (1) *When $3 \nmid N$, there is an element of $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_3)^{\boldsymbol{\varepsilon}}$ whose q-expansion is a non-zero constant if and only if $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H$ and $\boldsymbol{\varepsilon}_H \neq \boldsymbol{\varepsilon}_+$.*

(2) *When $3 \mid N$, the same holds if and only if either $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H^+$ and $\boldsymbol{\varepsilon}_H^+ \neq \boldsymbol{\varepsilon}_+$, or $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H^-$.*

PROOF. We prove the second assertion. The first one is similar and simpler. By (2.2.5), for each $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_m) \in \boldsymbol{E}$ ($l_1 = 3$), there is a q-expansion preserving mapping

$$M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_3)^{\boldsymbol{\varepsilon}} \to M_6^{\mathrm{B}}(\Gamma_0(N/3); \mathbb{F}_3)^{\boldsymbol{\varepsilon}'}$$

with $\boldsymbol{\varepsilon}' = (\varepsilon_2, \ldots, \varepsilon_m)$. (Read $\boldsymbol{\varepsilon}' = \phi$ if $N = 3$.) In $M_6^{\mathrm{A}}(\Gamma_0(N/3); \mathbb{F}_3)$, H^3 is the unique element having the q-expansion 1, which belongs to the sign $\boldsymbol{\varepsilon}' = \left(\left(\frac{l_2}{3}\right), \ldots, \left(\frac{l_m}{3}\right)\right)$. Thus if there is an element whose q-expansion is a non-zero constant in the left hand side, we must have $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H^{\pm}$. If $\boldsymbol{\varepsilon}_H^+ = \boldsymbol{\varepsilon}_+$, there is no such an element by (2.3.5).

Conversely, if $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H^+ \neq \boldsymbol{\varepsilon}_+$ or $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H^-$, we have seen above that the q-expansion of $3E_{\boldsymbol{\varepsilon}}$ (mod 3) is a non-zero constant. □

2.4. Hecke algebras. We keep the notation in the previous subsection.

DEFINITION (2.4.1). For any ring R, we let

$$\begin{cases} \boldsymbol{T}(N; R) \subseteq \mathrm{End}_R(M_2^{\mathrm{reg}}(\Gamma_0(N); R))\,, \\ \mathbf{T}(N; R) \subseteq \mathrm{End}_R(S_2^{\mathrm{reg}}(\Gamma_0(N); R)) \end{cases}$$

be the (commutative) subalgebras generated over R by the Hecke operators $T(l)$ with prime numbers l not dividing N, and the Atkin-Lehner operators w_{l_i} ($i = 1, \ldots, m$). (Here and henceforth, we understand that $\mathrm{End}_R(\{0\}) = \{0\}$.)

When N is a prime (≥ 5), $\mathbf{T}(N; \mathbb{Z})$ is exactly the ring $\mathbf{T}$ considered by Mazur [Ma, II, 6]. In this case, this ring coincides with the one generated by $T(l)$ as above and $U(N)$ (loc. cit.). However, in general, $\mathbf{T}(N; \mathbb{Z})$ is different from the ring generated by $T(l)$ and $U(l_i)$, as w_N and $U(l_i)$ do not commute, cf. [Sh, Remark 3.59].

In what follows, for $f \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$, $M_k^{\mathrm{B}}(\Gamma_0(N); R)$ or $M_2^{\mathrm{reg}}(\Gamma_0(N); R)$, we set

$$\text{(2.4.2)} \qquad a(n; f) := (\text{the coefficient of } q^n \text{ in } f(q))\,.$$

One can define the operators $T(n)$ for positive integers n prime to N by the usual formulas from $T(l)$, and we have

$$a(1;\, f\,|_k\, T(n)) = a(n;\, f)\,. \tag{2.4.3}$$

On the other hand, $\boldsymbol{\mathcal{T}}(N;\, R)$ and $\mathbf{T}(N;\, R)$ are algebras over $R[G_{\mathrm{AL}}]$. We can thus decompose them as direct sums of rings when 2 is invertible in R:

$$\begin{cases} \boldsymbol{\mathcal{T}}(N;\, R) = \oplus_{\boldsymbol{\varepsilon}\in \boldsymbol{E}} \boldsymbol{\mathcal{T}}(N;\, R)^{\boldsymbol{\varepsilon}}\,, \\ \mathbf{T}(N;\, R) = \oplus_{\boldsymbol{\varepsilon}\in \boldsymbol{E}} \mathbf{T}(N;\, R)^{\boldsymbol{\varepsilon}} \end{cases} \tag{2.4.4}$$

(cf. (2.1.3)). We will use the same symbol $T(n)$ to denote the image of $T(n)$ in the above direct summands. Then $\boldsymbol{\mathcal{T}}(N;\, R)^{\boldsymbol{\varepsilon}}$ (resp. $\mathbf{T}(N;\, R)^{\boldsymbol{\varepsilon}}$) is the subring of $\mathrm{End}_R(M_2^{\mathrm{reg}}(\Gamma_0(N);\, R)^{\boldsymbol{\varepsilon}})$ (resp. $\mathrm{End}_R(S_2^{\mathrm{reg}}(\Gamma_0(N);\, R)^{\boldsymbol{\varepsilon}})$) generated by $T(l)$'s over R.

LEMMA (2.4.5). *Fix $\boldsymbol{\varepsilon} \in \boldsymbol{E}$. Let the pairings*

$$\begin{cases} M_2^{\mathrm{reg}}(\Gamma_0(N);\, \mathbb{Q})^{\boldsymbol{\varepsilon}} \times \boldsymbol{\mathcal{T}}(N;\, \mathbb{Q})^{\boldsymbol{\varepsilon}} \xrightarrow{(\ ,\ )} \mathbb{Q}\,, \\ S_2^{\mathrm{reg}}(\Gamma_0(N);\, \mathbb{Q})^{\boldsymbol{\varepsilon}} \times \mathbf{T}(N;\, \mathbb{Q})^{\boldsymbol{\varepsilon}} \xrightarrow{(\ ,\ )} \mathbb{Q} \end{cases}$$

be defined by $(f, t) = a(1;\, f\,|_2\, t)$. Then these two pairings are perfect.

PROOF. We remind of us that $M_2^{\mathrm{reg}}(\Gamma_0(N);\, \mathbb{Q}) = M_2^{\mathrm{B}}(\Gamma_0(N);\, \mathbb{Q})$ and similarly for cusp forms by (1.4.10).

Consider the mapping

$$M_2^{\mathrm{reg}}(\Gamma_0(N);\, \mathbb{Q})^{\boldsymbol{\varepsilon}} \to \mathrm{Hom}(\boldsymbol{\mathcal{T}}(N;\, \mathbb{Q})^{\boldsymbol{\varepsilon}}, \mathbb{Q})$$

induced by the first pairing. If $f \in M_2^{\mathrm{reg}}(\Gamma_0(N);\, \mathbb{Q})^{\boldsymbol{\varepsilon}}$ is mapped to zero, we have $a(1;\, f\,|_2\, T(n)) = a(n;\, f) = 0$ for all n prime to N. Then by (2.1.4), $f(q)$ is a constant and hence it is zero. This shows that the above mapping is injective.

Conversely, if $t \in \boldsymbol{\mathcal{T}}(N;\, \mathbb{Q})^{\boldsymbol{\varepsilon}}$ is mapped to zero under the mapping

$$\boldsymbol{\mathcal{T}}(N;\, \mathbb{Q})^{\boldsymbol{\varepsilon}} \to \mathrm{Hom}(M_2^{\mathrm{reg}}(\Gamma_0(N);\, \mathbb{Q})^{\boldsymbol{\varepsilon}}, \mathbb{Q})$$

induced by the first pairing, we have $a(1;\, f\,|_2\, T(n)\,|_2\, t) = a(n;\, f\,|_2\, t) = 0$ when $(n, N) = 1$ for any $f \in M_2^{\mathrm{reg}}(\Gamma_0(N);\, \mathbb{Q})^{\boldsymbol{\varepsilon}}$. Then for the same reason as above, we see that $f\,|_2\, t = 0$, which shows that $t = 0$, and this mapping is also injective.

This proves that the first pairing is perfect, and the same proof works for cusp forms. □

THEOREM (2.4.6). *Let p be an odd prime, and fix $\boldsymbol{\varepsilon} \in \boldsymbol{E}$. Consider the pairings between free $\mathbb{Z}_{(p)}$-modules of finite rank*

$$\begin{cases} M_2^{\mathrm{reg}}(\Gamma_0(N);\, \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \times \boldsymbol{\mathcal{T}}(N;\, \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \xrightarrow{(\ ,\ )} \mathbb{Z}_{(p)}\,, \\ S_2^{\mathrm{reg}}(\Gamma_0(N);\, \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \times \mathbf{T}(N;\, \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \xrightarrow{(\ ,\ )} \mathbb{Z}_{(p)} \end{cases}$$

defined by the same formula as in (2.4.5). *Then the first pairing is perfect unless* $p = 3$ *and* $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H$ (*when* $3 \nmid N$) *or* $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H^{\pm}$ (*when* $3 \mid N$). *The second pairing is always perfect.*

PROOF. For the first one, we need to show that the induced mapping

$$M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \to \mathrm{Hom}(\boldsymbol{T}(N; \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}, \mathbb{Z}_{(p)})$$

is an isomorphism. We have already seen above that this is injective.

Let φ be an element in the right hand side. By the previous lemma, there is an $f \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Q})^{\boldsymbol{\varepsilon}}$ such that $\varphi(t) = a(1; f|_2 t)$ for all $t \in \boldsymbol{T}(N; \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$. We want to show that f belongs to $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$, i.e. $a(n; f) \in \mathbb{Z}_{(p)}$ for all $n \geq 0$; cf. (1.4.10) when $p \nmid N$, and (1.4.9), (1) when $p \mid N$. We first see that $\varphi(T(n)) = a(n; f) \in \mathbb{Z}_{(p)}$ for n prime to N.

Now assume that $f \notin M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$. Then there is an integer $c \geq 1$ such that $p^c f \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$ and $g := p^c f \pmod p \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)^{\boldsymbol{\varepsilon}}$ is a non-zero element. It follows from (1.4.15) that the q-expansion $g(q)$ is also non-zero. From the above observation, g satisfies the condition in (2.2.8), and we necessarily have that $p = 3$ and $g(q)$ is a non-zero constant. Finally, (2.3.9) implies that g cannot exist under our hypothesis. This shows that $f \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$, and hence completes the proof for the first pairing.

The assertion for the second pairing is also clear from the above argument. □

COROLLARY (2.4.7). *Let* R *be a* $\mathbb{Z}_{(p)}$*-algebra. Except for the case where* $p = 3$ *and* $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H, \boldsymbol{\varepsilon}_H^{\pm}$ *in the first case below, the canonical mappings*

$$\begin{cases} \boldsymbol{T}(N; \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \otimes_{\mathbb{Z}_{(p)}} R \to \boldsymbol{T}(N; R)^{\boldsymbol{\varepsilon}}, \\ \mathbf{T}(N; \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \otimes_{\mathbb{Z}_{(p)}} R \to \mathbf{T}(N; R)^{\boldsymbol{\varepsilon}} \end{cases}$$

are isomorphisms, and the pairings above induce perfect pairings

$$\begin{cases} M_2^{\mathrm{reg}}(\Gamma_0(N); R)^{\boldsymbol{\varepsilon}} \times \boldsymbol{T}(N; R)^{\boldsymbol{\varepsilon}} \xrightarrow{(\ ,\ )} R, \\ S_2^{\mathrm{reg}}(\Gamma_0(N); R)^{\boldsymbol{\varepsilon}} \times \mathbf{T}(N; R)^{\boldsymbol{\varepsilon}} \xrightarrow{(\ ,\ )} R. \end{cases}$$

PROOF. This follows easily from (2.4.6); cf. e.g. [Oh2, (1.3.5), (1.3.6)]. □

REMARK (2.4.8). We obtain from (2.4.7) an isomorphism

$$M_2^{\mathrm{reg}}(\Gamma_0(N); R)^{\boldsymbol{\varepsilon}} \cong \mathrm{Hom}_R(\boldsymbol{T}(N; R)^{\boldsymbol{\varepsilon}}, R).$$

Let φ in the right hand side be an *R-algebra homomorphism*, and let f in the left hand side correspond to φ. Then it is clear that

$$a(1; f) = 1.$$

On the other hand, take a positive integer n prime to N, and let φ' correspond to $f|_2 T(n)$. For any $t \in \boldsymbol{T}(N; R)^{\boldsymbol{\varepsilon}}$, we have $\varphi'(t) = a(1; f|_2 T(n)t) = \varphi(T(n))\varphi(t)$ and hence $\varphi' =$

$a(n;\, f)\varphi$. It follows that f is an eigenform of $T(n)$:

$$f\,|_2T(n) = a(n;\, f)f\,.$$

The same holds for cusp forms.

3. Eisenstein ideals and the rational torsion in $J_0(N)$

3.1. Eisenstein ideals. Throughout this section, as before, we assume that $N = l_1 \cdots l_m > 1$ is square-free with prime numbers l_i $(i = 1, \ldots, m)$.

DEFINITION (3.1.1). We define the *Eisenstein ideals* of the Hecke algebras by

$$\begin{cases} \mathcal{I}_R := (T(l) - (1+l)\ (l : \text{prime numbers},\ l \nmid N)) \subseteq \boldsymbol{T}(N;\, R)\,, \\ I_R := (T(l) - (1+l)\ (l : \text{prime numbers},\ l \nmid N)) \subseteq \mathbf{T}(N;\, R)\,. \end{cases}$$

When 2 is invertible in R, according to the direct sum decomposition (2.4.4), we have

$$\begin{cases} \mathcal{I}_R = \oplus_{\boldsymbol{\varepsilon} \in \boldsymbol{E}} \mathcal{I}_R^{\boldsymbol{\varepsilon}}\,, \\ I_R = \oplus_{\boldsymbol{\varepsilon} \in \boldsymbol{E}} I_R^{\boldsymbol{\varepsilon}}\,. \end{cases}$$

Thus $\mathcal{I}_R^{\boldsymbol{\varepsilon}}$ and $I_R^{\boldsymbol{\varepsilon}}$ are the ideals of $\boldsymbol{T}(N;\, R)^{\boldsymbol{\varepsilon}}$ and $\mathbf{T}(N;\, R)^{\boldsymbol{\varepsilon}}$ generated by all $T(l) - (1+l)$ with prime numbers $l \nmid N$, respectively.

Our present purpose is to determine the structure of $\mathbf{T}(N;\, \mathbb{Z}[1/2])/I_{\mathbb{Z}[1/2]} \cong \oplus_{\boldsymbol{\varepsilon} \in \boldsymbol{E}} \mathbf{T}(N;\, \mathbb{Z}[1/2])^{\boldsymbol{\varepsilon}}/I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}[1/2]}$. To state our result, for each $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_m) \in \boldsymbol{E}$, we set

$$(3.1.2)\quad c(N;\, \boldsymbol{\varepsilon}) := \begin{cases} 1 \text{ if } \boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_+ \text{ (cf. (2.3.3))}\,, \\ \frac{1}{8}\prod_{i=1}^m (l_i + \varepsilon_i) \text{ if } \boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+ \text{ and } \boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H \text{ or } \boldsymbol{\varepsilon}_H^{\pm} \text{ (cf. (2.3.7), (2.3.8))}\,, \\ \frac{1}{24}\prod_{i=1}^m (l_i + \varepsilon_i) \text{ if } \boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+, \boldsymbol{\varepsilon}_H, \boldsymbol{\varepsilon}_H^{\pm}\,. \end{cases}$$

Actually the powers of 2 in these numbers will play no role in this paper; but note that the third number is exactly the constant term of the Eisenstein series $E_{\boldsymbol{\varepsilon}}$ in (2.3.4) up to sign, and the second one is the same number multiplied by ± 3 (while there is no Eisenstein series in $M_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}_+}$). By the definitions of $\boldsymbol{\varepsilon}_H$ and $\boldsymbol{\varepsilon}_H^{\pm}$, we see that $c(N;\, \boldsymbol{\varepsilon})$ always belongs to $\mathbb{Z}[1/2]$.

Mazur proved that $\mathbf{T}(N;\, \mathbb{Z})/(I_{\mathbb{Z}},\, 1 + w_N) \cong \mathbb{Z}/n\mathbb{Z}$ with $n =$ (the numerator of $(N-1)/12$) [Ma, II, Proposition (9.7)], and also that $\mathbf{T}(N;\, \mathbb{Z}[1/2])^{\boldsymbol{\varepsilon}_+} = I^{\boldsymbol{\varepsilon}_+}_{\mathbb{Z}[1/2]}$ [Ma, II, the proof of Proposition (14.1)], when N is a prime (≥ 5). The following theorem is a partial generalization of his result, whose proof will be completed in the subsection 3.4 below.

THEOREM (3.1.3). *Let the notation be as above. Then for each $\boldsymbol{\varepsilon} \in \boldsymbol{E}$, we have*

$$\mathbf{T}(N;\, \mathbb{Z}[1/2])^{\boldsymbol{\varepsilon}}/I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}[1/2]} \cong \mathbb{Z}[1/2]/c(N;\, \boldsymbol{\varepsilon})\mathbb{Z}[1/2]$$

equivalently,

$$\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}/I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}} \cong \mathbb{Z}_{(p)}/c(N;\boldsymbol{\varepsilon})\mathbb{Z}_{(p)}$$

for all odd prime numbers p.

We first note the following

LEMMA (3.1.4). *If $c(N;\boldsymbol{\varepsilon})$ is not a unit in $\mathbb{Z}[1/2]$, then $S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Q})^{\boldsymbol{\varepsilon}} \neq \{0\}$.*

PROOF. Under our assumption, $\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+$ and there is an odd prime p dividing $c(N;\boldsymbol{\varepsilon})$. Since $c(N;\boldsymbol{\varepsilon}_H)$ and $c(N;\boldsymbol{\varepsilon}_H^{\pm})$ are not divisible by 3, we see that p divides $\frac{1}{24}\prod_{i=1}^{m}(l_i+\varepsilon_i)$ even in the case $p=3$. Then $E_{\boldsymbol{\varepsilon}} \in M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$ and its reduction modulo p is a non-zero element of $M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{F}_p)^{\boldsymbol{\varepsilon}}$ as $a(1;E_{\boldsymbol{\varepsilon}})=1$ by (2.3.4). This, considered as a section of $\Omega_{/\mathbb{F}_p}$(cusps) on $X_0(N)_{/\mathbb{F}_p}$ (cf. our convention (1.4.16)), is holomorphic at the cusp infinity by our assumption. Since G_{AL} acts transitively on the cusp sections of $X_0(N)_{/\mathbb{Z}}$, we see that this differential is in fact a section of $\Omega_{/\mathbb{F}_p}$, that is, $E_{\boldsymbol{\varepsilon}} \pmod p$ belongs to $S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{F}_p)^{\boldsymbol{\varepsilon}}$. Hence $S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$ is also non-zero by (1.4.5). □

This lemma shows that (3.1.3) holds trivially when $S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Q})^{\boldsymbol{\varepsilon}} = \{0\}$ (i.e. $\{0\}/\{0\} \cong \{0\}$). Thus in the argument of 3.2–3.4, we will always assume that $S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Q})^{\boldsymbol{\varepsilon}} \neq \{0\}$, and hence $\mathbf{T}(N;\mathbb{Q})^{\boldsymbol{\varepsilon}}$ is not a zero ring.

3.2. Proof of (3.1.3) in the "general" case. By the "general" case, we mean the case where

$$\begin{cases} \boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+, \text{ and} \\ \boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_H, \boldsymbol{\varepsilon}_H^{\pm} \text{ when } p=3\,. \end{cases}$$

In this subsection, we prove the second statement of (3.1.3) under this condition. The remaining "special" cases will be treated in the subsequent subsections. In the present case, the proof goes along the same line as in our previous work [Oh2, 2.2–2.4], and it is in fact simpler.

Let $\mathcal{C}_N$ be the set of cusps of $X_0(N)$. For a ring R, let $R[\mathcal{C}_N]$ be the free R-module on this set, and $R[\mathcal{C}_N]^0$ its degree-0 part. We define

$$\mathbf{Res} : M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Q}) \to \mathbb{Q}[\mathcal{C}_N]^0 \text{ by } \mathbf{Res}(f) := \sum_{c\in\mathcal{C}_N} (\mathrm{Res}_c\,\omega_f)\cdot c \tag{3.2.1}$$

where Res_c means the residue at c, and ω_f is the differential corresponding to f. Since G_{AL} acts on $\mathcal{C}_N$ simply transitively and $\omega_f \circ w = \omega_{f|_2 w}$ for $w \in G_{\mathrm{AL}}$, we see that

$$\mathbf{Res}(f) = \sum_{w\in G_{\mathrm{AL}}} (\mathrm{Res}_\infty\,\omega_{f|_2 w})\cdot(w\infty) = \sum_{w\in G_{\mathrm{AL}}} a(0;f|_2 w)\cdot(w\infty)\,. \tag{3.2.2}$$

When $f \in M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z})$, we have $a(0;f|_2 w) \in \mathbb{Z}$ by (1.4.9), (2), and hence **Res** sends $M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z})$ to $\mathbb{Z}[\mathcal{C}_N]^0$.

LEMMA (3.2.3). *We have the exact sequence*

$$0 \to S_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}) \to M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}) \overset{\mathbf{Res}}{\to} \mathbb{Z}[\mathcal{C}_N]^0 \to 0\,.$$

PROOF. Since $\dim_{\mathbb{Q}} M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Q}) = \dim_{\mathbb{Q}} S_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Q}) + (2^m - 1)$, the above sequence tensored with $\mathbb{Q}$ is exact. To prove our claim, in view of (1.4.9), (2), we only need to show the surjectivity of **Res**. For this, it is enough to show that the above sequence tensored with $\mathbb{F}_p$ is exact for every prime number p. But by (1.4.5), it becomes

$$0 \to S_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p) \to M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p) \overset{\mathbf{Res}}{\to} \mathbb{F}_p[\mathcal{C}_N]^0 \to 0$$

where **Res** is defined by (3.2.2) in characteristic p. This sequence is then left exact, and again comparing the dimensions, we see that it is exact. □

It is easy to see that $\mathbf{Res}(f\,|_2\, w) = w^{-1}\mathbf{Res}(f) = w\mathbf{Res}(f)$ for $f \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Q})$ and $w \in G_{\mathrm{AL}}$. Thus for an odd prime p and $\boldsymbol{\varepsilon} \in \boldsymbol{E}$, we obtain the exact sequence

$$0 \to S_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \overset{i}{\to} M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \overset{\mathbf{Res}}{\to} (\mathbb{Z}_{(p)}[\mathcal{C}_N]^0)^{\boldsymbol{\varepsilon}} \to 0 \tag{3.2.4}$$

from the previous lemma. We consider this as an exact sequence of $\boldsymbol{T}(N; \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$-modules by endowing $(\mathbb{Z}_{(p)}[\mathcal{C}_N]^0)^{\boldsymbol{\varepsilon}}$ the quotient module structure of $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$.

LEMMA (3.2.5). *When tensored with* $\mathbb{Q}$, *the sequence* (3.2.4) *uniquely splits as modules over* $\boldsymbol{T}(N; \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$. *The associated congruence module* (*cf.* [Oh2, 2.3]) *is isomorphic to* $\mathbb{Z}_{(p)}/c(N; \boldsymbol{\varepsilon})\mathbb{Z}_{(p)}$.

PROOF. We first note that, since $\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+$, $(\mathbb{Z}_{(p)}[\mathcal{C}_N]^0)^{\boldsymbol{\varepsilon}}$ is a free $\mathbb{Z}_{(p)}$-module of rank one generated by $(\prod_{i=1}^m (w_{l_i} + \varepsilon_i)) \cdot \infty$.

Also, since $\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_H, \boldsymbol{\varepsilon}_H^{\pm}$ when $p = 3$, $E_{\boldsymbol{\varepsilon}}$ belongs to $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$, which is an eigenform of $T(l)$ (with the eigenvalue $1 + l$) for all $l \nmid N$. $\mathbb{Q}E_{\boldsymbol{\varepsilon}}$ is mapped isomorphically to $(\mathbb{Q}[\mathcal{C}_N]^0)^{\boldsymbol{\varepsilon}}$ under **Res**, so that this gives a splitting of (3.2.4) over $\mathbb{Q}$.

If $\mathbb{Q}f$ is another splitting image of $(\mathbb{Q}[\mathcal{C}_N]^0)^{\boldsymbol{\varepsilon}}$, f is an eigenform of all $T(l)$ $(l \nmid N)$ with the same system of eigenvalues as $E_{\boldsymbol{\varepsilon}}$. If $a(1; f) = 0$, the relation (2.4.3) shows that $a(n; f) = 0$ for all n prime to N, which implies that $f = 0$ by (2.1.4). Therefore we have $a(1; f) \neq 0$, and we may assume that $a(1; f) = 1$. In this case, $a(n; f - E_{\boldsymbol{\varepsilon}}) = 0$ when $(n, N) = 1$, and hence (2.1.4) again shows that $f = E_{\boldsymbol{\varepsilon}}$. This proves the uniqueness of the splitting.

Now it follows from our first remark that **Res** is given as the composite of

$$r_\infty : M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \to \mathbb{Z}_{(p)};\ \ f \mapsto \left(\prod_{i=1}^m \varepsilon_i\right)\mathrm{Res}_\infty(\omega_f)$$

and the isomorphism $\mathbb{Z}_{(p)} \overset{\sim}{\to} (\mathbb{Z}_{(p)}[\mathcal{C}_N]^0)^{\boldsymbol{\varepsilon}}$ $(a \mapsto a(\prod_{i=1}^m (w_{l_i} + \varepsilon_i)) \cdot \infty)$. By (2.3.4) we have $\mathbb{Q}E_{\boldsymbol{\varepsilon}} \cap M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} = \mathbb{Z}_{(p)}E_{\boldsymbol{\varepsilon}}$, and the congruence module in question is isomorphic

to

$$\mathbb{Z}_{(p)}/r_\infty(E_{\boldsymbol{\varepsilon}})\mathbb{Z}_{(p)} = \mathbb{Z}_{(p)}/a(0;E_{\boldsymbol{\varepsilon}})\mathbb{Z}_{(p)} = \mathbb{Z}_{(p)}/c(N;\boldsymbol{\varepsilon})\mathbb{Z}_{(p)}\,. \qquad \square$$

We now prove (3.1.3) in the case under consideration. Take the $\mathbb{Z}_{(p)}$-dual (which we indicate by the superscript "$\vee$") of the exact sequence (3.2.4). Then by the duality (2.4.6), we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longleftarrow & S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}\vee} & \xleftarrow{i^\vee} & M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}\vee} & \xleftarrow{\mathbf{Res}^\vee} & (\mathbb{Z}_{(p)}[\mathcal{C}_N]^0)^{\boldsymbol{\varepsilon}\vee} & \longleftarrow & 0 \\ & & \downarrow{\scriptstyle (2.4.6)}\wr & & \downarrow\wr{\scriptstyle (2.4.6)} & & & & \\ 0 & \longleftarrow & \mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} & \xleftarrow[j]{} & \boldsymbol{\mathcal{T}}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} & & & & \end{array} \tag{3.2.6}$$

where the mapping j is the natural surjection sending $T(l)$ to $T(l)$. When tensored with $\mathbb{Q}$, the upper horizontal sequence splits uniquely as modules over $\boldsymbol{\mathcal{T}}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$, and the splitting image of $S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Q})^{\boldsymbol{\varepsilon}\vee}$ in $M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Q})^{\boldsymbol{\varepsilon}\vee}$ corresponds to the annihilator of $\mathbb{Q}E_{\boldsymbol{\varepsilon}}$ in $\boldsymbol{\mathcal{T}}(N;\mathbb{Q})^{\boldsymbol{\varepsilon}}$ with respect to the pairing in (2.4.5). Call this annihilator $\mathfrak{J}$. Then an element t of $\boldsymbol{\mathcal{T}}(N;\mathbb{Q})^{\boldsymbol{\varepsilon}}$ belongs to $\mathfrak{J}$ if and only if $a(1;E_{\boldsymbol{\varepsilon}}\,|_2\,t)=0$ by definition, and this is equivalent to that $a(1;E_{\boldsymbol{\varepsilon}}\,|_2\,T(n)\,|_2\,t) = a(1;E_{\boldsymbol{\varepsilon}}\,|_2\,t\,|_2\,T(n)) = a(n;E_{\boldsymbol{\varepsilon}}\,|_2\,t) = 0$ for all n prime to N. By (2.1.4), this condition is equivalent to that $E_{\boldsymbol{\varepsilon}}\,|_2\,t = 0$. Therefore we see that $\mathcal{J} := \boldsymbol{\mathcal{T}}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \cap \mathfrak{J}$ is nothing but the annihilator ideal of $E_{\boldsymbol{\varepsilon}}$ in $\boldsymbol{\mathcal{T}}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$, and the congruence module attached to the upper sequence in (3.2.6) is isomorphic to $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}/j(\mathcal{J})$. By [Oh2, (2.3.4)], this is isomorphic to the congruence module considered in (3.2.5). Thus our proof will be complete with the following

LEMMA (3.2.7). *$\mathcal{I}^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}$ is the annihilator ideal of $E_{\boldsymbol{\varepsilon}}$ in $\boldsymbol{\mathcal{T}}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$: $\mathcal{I}^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}} = \mathcal{J}$.*

PROOF. Clearly $\mathcal{J}$ contains $\mathcal{I}^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}$. But we have the sequence of natural $\mathbb{Z}_{(p)}$-algebra homomorphisms

$$\mathbb{Z}_{(p)} \twoheadrightarrow \boldsymbol{\mathcal{T}}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}/\mathcal{I}^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}} \twoheadrightarrow \boldsymbol{\mathcal{T}}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}/\mathcal{J} \twoheadrightarrow \mathbb{Z}_{(p)} = \mathrm{End}_{\mathbb{Z}_{(p)}}(\mathbb{Z}_{(p)}E_{\boldsymbol{\varepsilon}})$$

the right arrow being induced by the action of Hecke operators on $E_{\boldsymbol{\varepsilon}}$. Therefore the middle arrow must be an isomorphism. $\square$

3.3. Proof of (3.1.3) in the case $p = 3$ and $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H, \boldsymbol{\varepsilon}_H^{\pm}$. To prove the proposition (3.3.3) below, we need some preliminary consideration. In general, let L be a positive integer, and take an auxiliary prime $l \geq 3$ not dividing L. Then there is the fine moduli scheme $M(L;l)$ classifying elliptic curves with $\Gamma_0(L)\cap\Gamma(l)$-structure (i.e. a pair of $\Gamma_0(L)$- and $\Gamma(l)$-structures; cf. 1.2) over $\mathbb{Z}[1/Ll]$-schemes. Let $\overline{M}(L;l)$ be its canonical compactification. There is the usual invertible sheaf $\underline{\omega}$ on this scheme such that

$$M_k^{\mathrm{A}}(\Gamma_0(L)\cap\Gamma(l);R) = H^0(\overline{M}(L;l),\underline{\omega}^{\otimes k}\otimes_{\mathbb{Z}[1/Ll]}R)$$

for $\mathbb{Z}[1/Ll]$-algebras R. For any $\mathbb{Z}[1/Ll]$-module K, we set

$$M_k^{\mathrm{A}}(\Gamma_0(L);K) := H^0(\overline{M}(L;l),\underline{\omega}^{\otimes k}\otimes_{\mathbb{Z}[1/Ll]}K)^{GL_2(\mathbb{Z}/l\mathbb{Z})} \tag{3.3.1}$$

(cf. [K1, 1.6]). This is independent of the choice of l in the sense that if $l' \geq 3$ is another prime not dividing Ll and K is a $\mathbb{Z}[1/Lll']$-module, then the right hand side of (3.3.1) is canonically isomorphic to the one defined by using l' in place of l. The left hand side of (3.3.1) agrees with the previous terminology when K is a $\mathbb{Z}[1/Ll]$-algebra; cf. (1.2.6), (2). Also, there is the q-expansion mapping $M_k^{\mathrm{A}}(\Gamma_0(L);K) \hookrightarrow K[[q]]$ (loc. cit.).

LEMMA (3.3.2) (cf. [Ma, page 86]). *Let a and b be positive integers prime to L. Then there is the following commutative diagram*

$$\begin{array}{ccccc} M_k^{\mathrm{A}}(\Gamma_0(L);\mathbb{Z}/b\mathbb{Z}) & \xrightarrow[\sim]{\text{“}\times a\text{”}} & M_k^{\mathrm{A}}(\Gamma_0(L);a(\mathbb{Z}/ab\mathbb{Z})) & \xrightarrow{\subseteq} & M_k^{\mathrm{A}}(\Gamma_0(L);\mathbb{Z}/ab\mathbb{Z}) \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{Z}/b\mathbb{Z}[[q]] & \xrightarrow{\sim} & a(\mathbb{Z}/ab\mathbb{Z})[[q]] & \longrightarrow & \mathbb{Z}/ab\mathbb{Z}[[q]] \end{array}$$

where the vertical arrows are the q-expansion mappings, the lower left horizontal arrow is induced by the mapping $c \pmod b \mapsto ac \pmod{ab}$, and the lower right horizontal arrow is the inclusion. The right square is cartesian.

For any positive divisor d of L such that $(d, L/d) = 1$, the operators w_d on the upper left and the upper right spaces commute, and the upper middle space is stable under w_d.

PROOF Let $l \geq 3$ be a prime not dividing Lab. Then with the terminology above, from $\mathbb{Z}/b\mathbb{Z} \xrightarrow{\sim} a(\mathbb{Z}/ab\mathbb{Z}) \hookrightarrow \mathbb{Z}/ab\mathbb{Z}$, we obtain

$$H^0(\overline{M}(L;l),\underline{\omega}^{\otimes k}\otimes_{\mathbb{Z}[1/Ll]}\mathbb{Z}/b\mathbb{Z}) \xrightarrow{\sim} H^0(\overline{M}(L;l),\underline{\omega}^{\otimes k}\otimes_{\mathbb{Z}[1/Ll]}a(\mathbb{Z}/ab\mathbb{Z}))$$

$$\hookrightarrow H^0(\overline{M}(L;l),\underline{\omega}^{\otimes k}\otimes_{\mathbb{Z}[1/Ll]}\mathbb{Z}/ab\mathbb{Z})\,.$$

The upper horizontal line in the lemma is the one obtained from this by taking the invariants under $GL_2(\mathbb{Z}/l\mathbb{Z})$. It is then clear that the diagram commutes, and the right square is cartesian.

Let $\mathcal{E} = (E, C_L, \phi)$ be the universal elliptic curve E with $\Gamma_0(L)$- (resp. $\Gamma(l)$-) structure C_L (resp. ϕ) over $M(L;l)$. Set $w_d\mathcal{E} := (E/C_L[d], E[d]/C_L[d] \times_{M(L;l)} C_L/C_L[d], \phi')$ with ϕ' the natural $\Gamma(l)$-structure induced by ϕ. Then there is an automorphism φ of $M(L;l)$ such that the base change of $\mathcal{E}$ by φ is $w_d\mathcal{E}$. Letting $\pi : E \to E/C_L[d]$ be the quotient morphism, we can define an automorphism of $H^0(M(L;l),\underline{\omega}^{\otimes k}\otimes_{\mathbb{Z}[1/Ll]}K)$ by $s \mapsto \pi^*\varphi^*(s)$, the meaning of π^* being the same as in (1.2.12). This automorphism induces the unique automorphism, which we denote by $\mathbf{w}_d$, of $H^0(\overline{M}(L;l),\underline{\omega}^{\otimes k}\otimes_{\mathbb{Z}[1/Ll]}K)$ in view of the description of $\underline{\omega}$ on $\overline{M}(L;l)$ around the cusps given in [K1, 1.5]. It is clear that this $\mathbf{w}_d$ is functorial with respect to K, and especially the mappings considered above are compatible

with $\mathbf{w}_d$ on the three modules. It is also clear that $\mathbf{w}_d$ on the two extreme modules induce the previous automorphisms $\mathbf{w}_d$ (1.2.12) on the corresponding modules in the upper line in our lemma, and the conclusion follows. □

Returning to the situation considered in the previous subsections, we obtain the following

PROPOSITION (3.3.3) *Assume that* $p = 3$, *and* $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H$ *when* $3 \nmid N$ *or* $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H^{\pm}$ *when* $3 \mid N$. *Then we have*

$$I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(3)}} = \mathbf{T}(N; \mathbb{Z}_{(3)})^{\boldsymbol{\varepsilon}}$$

i.e. (3.1.3) *holds in this case.*

PROOF First we consider the case $3 \mid N = l_1 \cdots l_m$ with $l_1 = 3$. Since $\mathbf{T}(3; \mathbb{Z}_{(3)}) = \{0\}$, we only need to consider the case $N > 3$ and hence $m \geq 2$. Assume to the contrary that $I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(3)}}$ is not the unit ideal for $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H^{+}$ or $\boldsymbol{\varepsilon}_H^{-}$. Then there is a homomorphism

$$\mathbf{T}(N; \mathbb{Z}_{(3)})^{\boldsymbol{\varepsilon}} \twoheadrightarrow \mathbf{T}(N; \mathbb{Z}_{(3)})^{\boldsymbol{\varepsilon}}/I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(3)}} \twoheadrightarrow \mathbb{F}_3$$

which factors through $\mathbf{T}(N; \mathbb{F}_3)^{\boldsymbol{\varepsilon}}$. We thus obtain an algebra homomorphism $\mathbf{T}(N; \mathbb{F}_3)^{\boldsymbol{\varepsilon}} \twoheadrightarrow \mathbb{F}_3$ which sends $T(l)$ to $1 + l$ for each prime number $l \nmid N$. By the duality (2.4.7), there corresponds an element $f \in S_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_3)$ such that

$$\begin{cases} f(q) = \sum_{n=1}^{\infty} a_n q^n \text{ with } a_n = \sigma(n) := \sum_{0<t|n} t \text{ if } (n, N) = 1\,, \\ f \mid_2 w_{l_i} = \left(\frac{l_i}{3}\right) f, \quad i = 2, \ldots, m\,. \end{cases}$$

Set $M := l_2 \cdots l_m$. By (2.2.4), $\varphi_p(f) =: F \in M_4^{\mathrm{A}}(\Gamma_0(M); \mathbb{F}_3)$ satisfies

$$\begin{cases} f(q) = F(q), \\ F \mid_4 w_{l_i} = F, \quad i = 2, \ldots, m\,. \end{cases}$$

We are going to show that the existence of such a form implies that there is a $G \in M_4^{\mathrm{A}}(\Gamma_0(1); \mathbb{Z}/9\mathbb{Z})$ whose q-expansion is 1. To see this, let

$$E_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \in M_4^{\mathrm{B}}(\Gamma_0(1); \mathbb{Z}); \quad \sigma_3(n) = \sum_{0<t|n} t^3$$

be the usual Eisenstein series, and set

$$E_4' := E_4 \mid_4 \prod_{i=2}^{m} (w_{l_i} + 1)\,.$$

Clearly, this belongs to $M_4^{\mathrm{B}}(\Gamma_0(M); \mathbb{Z})$ and satisfies $E_4' \mid_4 w_{l_i} = E_4'$ for $i = 2, \cdots, m$. Also,

for the same reason as (2.3.4), we have

$$E_4' = \prod_{i=2}^{m}(l_i^2+1) + 240\sum_{n=1}^{\infty} b_n q^n$$

with $b_n \in \mathbb{Z}$ and $b_n = \sigma_3(n)$ when $(n, M) = 1$, and note that the constant term is a 3-adic unit. Let $F' :=$"$\times 3$"$F \in M_4^{\mathrm{A}}(\Gamma_0(M); \mathbb{Z}/9\mathbb{Z})$ in the terminology of the previous lemma, and set

$$G' := E_4' - 80F' \in M_4^{\mathrm{A}}(\Gamma_0(M); \mathbb{Z}/9\mathbb{Z})$$

where we used the same symbol E_4' to denote its reduction modulo 9. We have $G' \mid_4 w_{l_i} = G'$ $(i = 2, \dots, m)$, and if $G'(q) = \sum_{n=0}^{\infty} c_n q^n$, then $c_0 \in (\mathbb{Z}/9\mathbb{Z})^\times$ and $c_n = 0$ if $(n, N) = 1$. Further set $G'' := G' \mid_4 \prod_{i=2}^{m}(1 - U(l_i)B(l_i)) \in M_4^{\mathrm{A}}(\Gamma_0(M^2); \mathbb{Z}/9\mathbb{Z})$. Since $m \geq 2$, the constant term of $G''(q)$ vanishes, and $G''(q)$ is of the form $240\times$(a power series in q^3). By the previous lemma, there is a $g \in M_4^{\mathrm{A}}(\Gamma_0(M^2); \mathbb{F}_3)$ such that $G'' =$"$\times 3$"g. Since $\theta g = 0$, the filtration of g is divisible by 3, and we have $g = 0$. This shows that $c_n = 0$ whenever $(n, M) = 1$. We conclude by (2.1.4) that $G'(q) = c_0 \in (\mathbb{Z}/9\mathbb{Z})^\times$. Repeated use of (2.1.1) then assures us that there is an element of $M_4^{\mathrm{A}}(\Gamma_0(1); \mathbb{Z}/9\mathbb{Z})$ whose q-expansion is a unit in $\mathbb{Z}/9\mathbb{Z}$, and hence the existence of the desired G.

Now we have that the q-expansion of $E_4 - G \in M_4^{\mathrm{A}}(\Gamma_0(1); \mathbb{Z}/9\mathbb{Z})$ is equal to $240\sum_{n=1}^{\infty}\sigma_3(n)q^n$. Again by the previous lemma, there is an element of $M_4^{\mathrm{A}}(\Gamma_0(1); \mathbb{F}_3)$ with the q-expansion $\sum_{n=1}^{\infty}\sigma_3(n)q^n$. However by Deligne [D, Proposition 6.2], $M_4^{\mathrm{A}}(\Gamma_0(1); \mathbb{F}_3)$ is a one-dimensional space spanned by the square of the Hasse invariant form $H \in M_2^{\mathrm{A}}(\Gamma_0(1); \mathbb{F}_3)$. Therefore such a form cannot exist, and this completes the proof when $3 \mid N$.

Next we treat the (simpler) case $3 \nmid N$. If $I^{\boldsymbol{\varepsilon}H}_{\mathbb{Z}_{(3)}} \neq \mathbf{T}(N; \mathbb{Z}_{(3)})^{\boldsymbol{\varepsilon}H}$, there exists an $f \in S_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_3)$ such that

$$\begin{cases} f(q) = \sum_{n=1}^{\infty} a_n q^n \text{ with } a_n = \sigma(n) \text{ if } (n, N) = 1\,, \\ f \mid_2 w_{l_i} = \left(\frac{l_i}{3}\right) f, \quad i = 1, \dots, m\,. \end{cases}$$

This time we set $F := fH \in S_4^{\mathrm{A}}(\Gamma_0(N); \mathbb{F}_3)$. It has the same q-expansion as f, and $F \mid_4 w_{l_i} = F$ for $i = 1, \dots, m$ by (2.3.6). With this F, we can repeat the same argument as in the first case (but without worrying about the prime factor 3 in N) to get G as above. □

3.4. Proof of (3.1.3) in the case $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_+$. To prove (3.1.3) in the remaining case, we need the following purely algebraic description of the trace mapping considered in 2.2.

LEMMA (3.4.1) *Let M be a positive integer, and p a prime number not dividing M. Set $L := pM$. For any $\mathbb{Z}[1/L]$-algebra R, there is the* (*necessarily unique*) *mapping*

$$\mathrm{Tr}_M^L : M_k^{\mathrm{A}}(\Gamma_0(L); R) \to M_k^{\mathrm{A}}(\Gamma_0(M); R)$$

satisfying (2.2.3).

PROOF We first construct the mapping Tr^L_M, and then show that it satisfies (2.2.3). Let E be an elliptic curve over an R-scheme S. The functor $(\mathrm{Sch}/S) \to (\mathrm{Sets})$ defined by $T \mapsto$ (the set of $\Gamma(p)$-structures on $E_{/T} = E \times_S T$ over T) is represented by an étale $GL_2(\mathbb{Z}/p\mathbb{Z})$-torsor $\widetilde{S}$ over S. (This is $[\Gamma(p)]_{E/S}$ in the terminology of [KM, (4.2), (4.13)].) We have the tautological $\Gamma(p)$-structure $\phi_{\widetilde{S}} : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} E_{/\widetilde{S}}[p]$ over $\widetilde{S}$. There are $p+1$ cyclic subgroups of order p of the abstract group $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, which give rise to constant subgroup schemes of $E_{/\widetilde{S}}[p]$ via $\phi_{\widetilde{S}}$. Call them H_j $(1 \le j \le p+1)$.

Now let $f \in M^{\mathrm{A}}_k(\Gamma_0(L); R)$. When E is an elliptic curve with a $\Gamma_0(M)$-structure C_M over an R-scheme S, consider

$$\sum_{j=1}^{p+1} f(E_{/\widetilde{S}}, C_{M/\widetilde{S}} \times_{\widetilde{S}} H_j) \in H^0(\widetilde{S}, \underline{\omega}^{\otimes k}_{E_{/\widetilde{S}}/\widetilde{S}}) .$$

This section is invariant under the action of $GL_2(\mathbb{Z}/p\mathbb{Z})$, and hence it uniquely descends to an element of $H^0(S, \underline{\omega}^{\otimes k}_{E/S})$, which we denote by $\mathrm{Tr}^L_M(f)(E, C_M)$. One easily checks that:

i) The rule $(E, C_M) \mapsto \mathrm{Tr}^L_M(f)(E, C_M)$ is compatible with cartesian squares in the sense of (1.2.2), and hence $\mathrm{Tr}^L_M(f)$ belongs to $M^{\mathrm{A}}_k(\Gamma_0(M); R)$.

ii) When S is connected and E admits a $\Gamma(p)$-structure over S,

$$\mathrm{Tr}^L_M(f)(E, C_M) = \sum_{C_p} f(E, C_M \times_S C_p)$$

where the sum ranges over all cyclic subgroup schemes of order p of the constant group scheme $E[p]$.

We next prove that $\mathrm{Tr}^L_M(f)$ satisfies (2.2.3). It is enough to show the second relation, i.e. that

$$\mathrm{Tr}^L_M(f \mid_k w_p)(E, C_L) = \mathrm{Tr}^L_M(f \mid_k w_p)(E, C_L[M])$$

$$= (f \mid_k w_p)(E, C_L) + p^{1-k/2}(f \mid_k U(p))(E, C_L)$$

for each $(E, C_L)/S/R$. For this, after a faithfully flat base extension and restricting to connected components as in the proof of (1.5.3), we are reduced to the case considered in ii). In this case, we have

$$\mathrm{Tr}^L_M(f \mid_k w_p)(E, C_L) \overset{(1.3.6)}{=} p^{-k/2} \sum_{C_p} (\mathbf{w}_p f)(E, C_L[M] \times_S C_p) .$$

By (1.1.6) and (1.2.12), this is the sum of $p^{-k/2}(\mathbf{w}_p f)(E, C_L[M] \times_S C_L[p]) = (f \mid_k w_p)(E, C_L)$ and $p^{-k/2} \sum_{C_p \neq C_L[p]} \pi^*_{C_p} f(E/C_p, \pi_{C_p}(C_L[M]) \times_S E[p]/C_p)$ where

$\pi_{C_p} : E \to E/C_p$ is the quotient homomorphism. In this second term, $E[p]/C_p = \pi_{C_p}(C_L[p])$, so that this is equal to $p^{1-k/2}(f|_k U(p))(E, C_L)$ (cf. [G, (3.6)]). This completes the proof. □

We are now ready to prove the following

PROPOSITION (3.4.2) *For any odd prime p, we have*

$$I^{\boldsymbol{\varepsilon}_+}_{\mathbb{Z}_{(p)}} = \mathbf{T}(N; \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}_+}$$

and hence (3.1.3) *holds for $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_+$.*

PROOF We first give the proof under the assumption $p \nmid N$. Assume that $I^{\boldsymbol{\varepsilon}_+}_{\mathbb{Z}_{(p)}} \neq \mathbf{T}(N; \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}_+}$. Then for the same reason as (3.3.3), there is an $f \in S_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p) \subseteq M_2^{\mathrm{A}}(\Gamma_0(N); \mathbb{F}_p)$ such that

$$(*) \qquad \begin{cases} f(q) = \sum_{n=0}^{\infty} a_n q^n \text{ with } a_n = \sigma(n) \text{ if } (n, N) = 1\,, \\ f|_2 w_{l_i} = f \text{ for all prime factors } l_i \text{ of } N\,. \end{cases}$$

Assume for the moment that $m \geq 2$, and set $\boldsymbol{\varepsilon} := (-1, +1, \ldots, +1)$. We may and do assume that $\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_H$ when $p = 3$, changing the order of the prime factors of N if necessary. Under these conditions, we are going to prove the following

CLAIM *Assume that there is an $f \in M_2^{\mathrm{A}}(\Gamma_0(N); \mathbb{F}_p)$ satisfying $(*)$. Then there is a $g \in M_2^{\mathrm{A}}(\Gamma_0(N/l_1); \mathbb{F}_p)$ satisfying $(*)$ with N replaced by N/l_1.*

We note that this inductive step was inspired by the similar argument of Agashe [A, Proposition 3.5], while he attributes this idea to Mazur.

Consider the reduction modulo p of the Eisenstein series $E_{\boldsymbol{\varepsilon}}$ for which we use the same symbol, and set $h := f - E_{\boldsymbol{\varepsilon}} \in M_2^{\mathrm{A}}(\Gamma_0(N); \mathbb{F}_p)$. Then it follows from our assumption that $a(n; h) = 0$ unless $(n, N) \neq 1$, and $h|_2 w_{l_i} = h$ for $i = 2, \ldots, m$. (2.1.2) implies that $h(q)$ is a power series in q^{l_1}. So by (2.1.1), there is a $g' \in M_2^{\mathrm{A}}(\Gamma_0(N/l_1); \mathbb{F}_p)$ such that $h = l_1^{-1} g'|_2 w_{l_1}$ and $h(q) = g'(q^{l_1})$. Since $g' = l_1 h|_2 w_{l_1}$, we have $g'|_2 w_{l_i} = g'$ for $i = 2, \ldots, m$, and $g'|_2 T(l) = (1 + l)g'$ for primes $l \nmid N$. Here we used that $f|_2 T(l) = (1 + l)f$ (and also that $E_{\boldsymbol{\varepsilon}}|_2 T(l) = (1 + l)E_{\boldsymbol{\varepsilon}}$) which follows easily from $(*)$ and (2.1.4). To complete the proof, it remains to show that $a(1; g') \neq 0$ and $g'|_2 T(l_1) = (1 + l_1)g'$ for then $g = a(1; g')^{-1} g'$ satisfies $(*)$.

First $g' = l_1(f - E_{\boldsymbol{\varepsilon}})|_2 w_{l_1} = l_1(f + E_{\boldsymbol{\varepsilon}})$, and hence $a(1; g') = 2l_1 \neq 0$. On the other hand, we obtain from the relations $l_1^{-1} g' = f + E_{\boldsymbol{\varepsilon}}$ and $h = f - E_{\boldsymbol{\varepsilon}} = l_1^{-1} g'|_2 w_{l_1}$ that

$$2E_{\boldsymbol{\varepsilon}} = l_1^{-1}(g' - g'|_2 w_{l_1})\,.$$

We now apply Tr^N_{N/l_1} to this equality. By (3.4.1),

$$\mathrm{Tr}^N_{N/l_1}(E_{\boldsymbol{\varepsilon}}) = E_{\boldsymbol{\varepsilon}} + E_{\boldsymbol{\varepsilon}} \mid_2 w_{l_1} \mid_2 U(l_1) = E_{\boldsymbol{\varepsilon}} - E_{\boldsymbol{\varepsilon}} \mid_2 U(l_1)\,.$$

But since $E_{\boldsymbol{\varepsilon}} = E'_{2,l_1} \mid_2 \prod_{i=2}^m (1 + w_{l_i})$ in the terminology of the proof of (2.3.4) and $E'_{2,l_1} \mid_2 U(l_1) = E'_{2,l_1}$, we have $E_{\boldsymbol{\varepsilon}} \mid_2 U(l_1) = E_{\boldsymbol{\varepsilon}}$ and hence $\mathrm{Tr}^N_{N/l_1}(E_{\boldsymbol{\varepsilon}}) = 0$. Consequently,

$$\mathrm{Tr}^N_{N/l_1}(g') = \mathrm{Tr}^N_{N/l_1}(g' \mid_2 w_{l_1}) = g' \mid_2 w_{l_1} + g' \mid_2 U(l_1)\,.$$

Since $g' \in M_2^{\mathrm{A}}(\Gamma_0(N/l_1); \mathbb{F}_p)$, it follows from the construction of the trace mapping given in the proof of (3.4.1) that $\mathrm{Tr}^N_{N/l_1}(g') = (1 + l_1)g'$. Also we have $(g' \mid_2 w_{l_1})(q) = l_1 g'(q^{l_1})$. Therefore the right hand side is $g' \mid_2 T(l_1)$. This finishes the proof of our claim.

Our assumption therefore implies the existence of $f_l \in M_2^{\mathrm{A}}(\Gamma_0(l); \mathbb{F}_p)$ with a prime number l different from p satisfying

$$\begin{cases} f_l(q) = \sum_{n=0}^{\infty} b_n q^n \text{ with } b_n = \sigma(n) \text{ whenever } l \nmid n\,, \\ f_l \mid_2 w_l = f_l\,. \end{cases}$$

We wish to show that such a form cannot exist. Except for the case $p = 3$ and $l \equiv 2 \pmod 3$, we can repeat the above procedure once more. Namely let $E'_{2,l}$ be the Eisenstein series as above. Then there is an $f'_l \in M_2^{\mathrm{A}}(\Gamma_0(1); \mathbb{F}_p)$ such that $f_l - E'_{2,l} = l^{-1} f'_l \mid_2 w_l$. This satisfies $a(1; f'_l) \neq 0$. If $p \geq 5$, this contradicts [Ma, II, (5.6), (a)]. If $p = 3$ it contradicts [D, Proposition 6.2] which we already quoted in the proof of (3.3.3). Finally assume that $p = 3$ and $l \equiv 2 \pmod 3$. In this case, using the notation in (3.3.2), we consider $24E'_{2,l} - 8 \times$"$\times 3$"$f_l \in M_2^{\mathrm{A}}(\Gamma_0(l); \mathbb{Z}/9\mathbb{Z})$. Its q-expansion is a power series in q^l so that we obtain by (2.1.1) an element of $M_2^{\mathrm{A}}(\Gamma_0(1); \mathbb{Z}/9\mathbb{Z})$ whose constant term of the q-expansion is a unit in $\mathbb{Z}/9\mathbb{Z}$. This contradicts [Ma, II, (5.6), (c)]. We have thus completed the proof of (3.4.2) in the case $p \nmid N$.

We next turn to the proof in the case $p \mid N$. Assume that our conclusion does not hold so that there is an $f \in S_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)^{\boldsymbol{\varepsilon}+}$ such that $f(q) = \sum_{n=1}^{\infty} c_n q^n$ with $c_n = \sigma(n)$ for $(n, N) = 1$. When $N = p$ it is easy to see that such a form does not exist: The (trivial) case $p = 3$ was already excluded. If $p \geq 5$, the q-expansion of $f - E'_{2,p} \in M_2^{\mathrm{reg}}(\Gamma_0(p); \mathbb{F}_p)$ is a power series in q^p whose constant term belongs to $\mathbb{F}_p^{\times}$. By (2.2.6), (1), this is impossible.

We may therefore assume that $N > p$, and we are going to reduce the problem to the case $p \nmid N$ considered above. Set $M := N/p$. We may take $l_1 = p$ so that $M = l_2 \cdots l_m > 1$. The case where $p = 3$ and $\boldsymbol{\varepsilon}_+ = \boldsymbol{\varepsilon}_H^+$ is already settled by (3.3.3), and thus we assume otherwise in the following. Then $\boldsymbol{\varepsilon} := (-1, +1, \ldots, +1)$ is not $\boldsymbol{\varepsilon}_H^-$ when $p = 3$, and so, as before, we can consider the reduction modulo p of the Eisenstein series $E_{\boldsymbol{\varepsilon}} \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)$.

We again consider $h := f - E_{\boldsymbol{\varepsilon}} \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)$. This time, (2.2.6), (2) and (2.2.7) imply that $h(q)$ is a constant, and in fact $h(q) = 0$ when $p \geq 5$ by (2.2.6), (1). Let us

show that $h(q) = 0$ also when $p = 3$. Indeed, if $h(q) \neq 0$, it follows from (2.2.5) that $\varphi_3'(h) \in M_6^{\mathrm{B}}(\Gamma_0(M); \mathbb{F}_3)$ has the same non-zero constant as its q-expansion, and satisfies $\varphi_3'(h)\,|_6\, w_{l_i} = \varphi_3'(h)$ for $i = 2, \ldots, m$. On the other hand, the q-expansion of $\varphi_3'(3E_{\boldsymbol{\varepsilon}_H^-}) \in M_6^{\mathrm{B}}(\Gamma_0(M); \mathbb{F}_3)$ is also a non-zero constant, and we have $\varphi_3'(3E_{\boldsymbol{\varepsilon}_H^-})\,|_6\, w_{l_i} = \left(\frac{l_i}{3}\right)\varphi_3'(3E_{\boldsymbol{\varepsilon}_H^-})$ for $i = 2, \ldots, m$. Since we assumed that $\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_H^-$, this contradicts the q-expansion principle, showing that $h(q) = 0$ as required.

We now use the terminology of 1.4, and identify an element of $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)$ with a pair of (meromorphic) differentials on $X_0(M)_{/\mathbb{F}_p}$ by (1.4.13). From the third relation in (1.4.14), we see that to f (resp. $E_{\boldsymbol{\varepsilon}}$) corresponds a pair of differentials of the form (ω, ω) (resp. $(\omega', -\omega')$). Then $(\omega - \omega', \omega + \omega')$ corresponds to h. But we have shown that $h(q) = 0$, i.e. $\omega = \omega'$. This implies that $(0, 2\omega)$ is a regular differential on $X_0(N)_{/\mathbb{F}_p}$, and hence ω is holomorphic at the supersingular points by (1.4.3). It follows that $\omega \in H^0(X_0(M)_{/\mathbb{F}_p}, \Omega^1_{X_0(M)_{/\mathbb{F}_p}/\mathbb{F}_p})$ because f is a cusp form. The first relation in (1.4.14) shows that $\alpha^*(\omega)$ corresponds to $(1/2)(f + E_{\boldsymbol{\varepsilon}})$. This means that $(1/2)(f + E_{\boldsymbol{\varepsilon}}) =: f'$ belongs to $S_2^{\mathrm{B}}(\Gamma_0(M); \mathbb{F}_p)(\hookrightarrow M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p))$. It is clear that $f'\,|_2\, T(l) = (1 + l)f'$ for primes $l \nmid N$, and $f'\,|_2\, w_{l_i} = f'$ for $i = 2, \ldots, m$. Further we have $f'\,|_2\, T(p) = (1 + p)f' = f'$. Indeed, since $T(p)$ and $U(p)$ have the same effect on q-expansions in characteristic p and $f'(q) = f(q) = E_{\boldsymbol{\varepsilon}}(q)$, it is enough to show that $E_{\boldsymbol{\varepsilon}}\,|_2\, U(p) = E_{\boldsymbol{\varepsilon}}$. This follows from the same argument as the equality "$E_{\boldsymbol{\varepsilon}}\,|_2\, U(l_1) = E_{\boldsymbol{\varepsilon}}$" given in the first step. We conclude that f' satisfies $(*)$ with N replaced by M, and we already know that such an f' does not exist. □

We have thus completed the proof of Theorem (3.1.3).

3.5. Kernels of Eisenstein ideals in $J_0(N)$ in characteristic p. Let $J_0(N)$ be the Jacobian variety of $X_0(N)$ defined over $\mathbb{Q}$. We denote by $J_0(N)_{/\mathbb{Z}}$ and $J_0(N)_{/\mathbb{Z}_{(p)}}$ its Néron models over $\mathbb{Z}$ or $\mathbb{Z}_{(p)}$, respectively, and by $J_0(N)_{/\mathbb{F}_p}$ their fibre at p.

The Hecke algebra $\mathbf{T}(N; \mathbb{Z})$ acts on $J_0(N)$, and we may consider it as a subring of $\mathrm{End}_{\mathbb{Q}}(J_0(N))$ or $\mathrm{End}_{\mathbb{Z}}(J_0(N)_{/\mathbb{Z}})$ etc. (As is well-known the covariant and the contravariant actions of $T(l)$ on $J_0(N)$ coincide, and the same holds for w_{l_i} since $w_{l_i}^2 = 1$. Thus we need not distinguish these two actions.)

Let p be an odd prime and set

$$\mathcal{G}_p(N) := J_0(N)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty]\,. \tag{3.5.1}$$

This is a module over $\mathbf{T}(N; \mathbb{Z}_{(p)})$ and hence we have the direct sum decomposition (2.1.3):

$$\mathcal{G}_p(N) = \oplus_{\boldsymbol{\varepsilon} \in \boldsymbol{E}} \mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}\,. \tag{3.5.2}$$

Each direct summand is a module over $\mathbf{T}(N; \mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$. In the following, we set

$$\mathfrak{P}_p^{\boldsymbol{\varepsilon}} := (I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}, p)\,. \tag{3.5.3}$$

This is the unique maximal ideal of $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$ containing $I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}$ when $I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}$ is a proper ideal of $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$.

PROPOSITION (3.5.4) (cf. [Ma, pages 118-119]). *Assume that $p \nmid N$, and that $I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}$ is a proper ideal. Then the dimension of $\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[\mathfrak{P}^{\boldsymbol{\varepsilon}}_p]$ over $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}/\mathfrak{P}^{\boldsymbol{\varepsilon}}_p \cong \mathbb{F}_p$ is at most one.*

PROOF We follow Mazur's argument. There is the well-known isomorphism due to Cartier and Serre [Se1, Proposition 10]:

$$\mathcal{G}_p(N)[p] \cong H^0(X_0(N)_{/\overline{\mathbb{F}}_p}, \Omega^1_{X_0(N)_{/\overline{\mathbb{F}}_p}/\overline{\mathbb{F}}_p})^{\mathcal{C}}$$

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

$$\mathcal{G}_p(N)[p] \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p \hookrightarrow H^0(X_0(N)_{/\overline{\mathbb{F}}_p}, \Omega^1_{X_0(N)_{/\overline{\mathbb{F}}_p}/\overline{\mathbb{F}}_p}) \cong S_2^{\mathrm{B}}(\Gamma_0(N);\overline{\mathbb{F}}_p)\,.$$

All these mappings commute with the action of $\mathbf{T}(N;\mathbb{Z}_{(p)})$. Therefore it is enough to show that $S_2^{\mathrm{B}}(\Gamma_0(N);\mathbb{F}_p)^{\boldsymbol{\varepsilon}}[\mathfrak{P}^{\boldsymbol{\varepsilon}}_p]$ is of dimension one over $\mathbb{F}_p$. But the duality (2.4.7) implies that this space is $\mathbb{F}_p$-dual to $\mathbf{T}(N;\mathbb{F}_p)^{\boldsymbol{\varepsilon}}/\mathfrak{P}^{\boldsymbol{\varepsilon}}_p$, and our claim follows. □

We now want to extend the above proposition to the case $p \mid N$. For this we need some lemmas. In the following, we let M be a square-free positive integer. When $M > 1$, we consider the set $\boldsymbol{E}'$ of signs (2.1.3) with respect to M. To distinguish from the signs with respect to N, we will always put the prime for elements of $\boldsymbol{E}'$ (and likewise for the Eisenstein ideals of level M). We especially set $\boldsymbol{\varepsilon}'_+ := (+1,\ldots,+1) \in \boldsymbol{E}'$.

LEMMA (3.5.5) *Let $M > 1$ be as above, and p a prime not dividing M. Assume that $p \geq 5$.*

(1) *For each $\boldsymbol{\varepsilon}' \in \boldsymbol{E}'$, $\boldsymbol{T}(M;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}'}$ is generated over $\mathbb{Z}_{(p)}$ by $T(l)$ with prime numbers l not dividing pM.*

(2) *Assume that $\boldsymbol{\varepsilon}' \neq \boldsymbol{\varepsilon}'_+$. The Eisenstein ideal $\mathcal{I}'^{\boldsymbol{\varepsilon}'}_{\mathbb{Z}_{(p)}}$ of $\boldsymbol{T}(M;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}'}$ is generated by $T(l) - (1+l)$ with prime numbers l not dividing pM.*

Consequently, the same assertions with $\boldsymbol{T}(M;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}'}$ (resp. $\mathcal{I}'^{\boldsymbol{\varepsilon}'}_{\mathbb{Z}_{(p)}}$) replaced by $\mathbf{T}(M;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}'}$ (resp. its Eisenstein ideal $I'^{\boldsymbol{\varepsilon}'}_{\mathbb{Z}_{(p)}}$) also hold.

PROOF (1) By (2.4.7), it is enough to show that $\boldsymbol{T}(M;\mathbb{F}_p)^{\boldsymbol{\varepsilon}'}$ is generated by $T(l)$ with l not dividing pM. Assume otherwise. Then again by (2.4.7), there is a non-zero $f \in M_2^{\mathrm{reg}}(\Gamma_0(M);\mathbb{F}_p)^{\boldsymbol{\varepsilon}'}$ such that $a(1;\, f\,|_2\, T(n)) = a(n;\, f) = 0$ for all n prime to pM. Since there is a natural injection $M_2^{\mathrm{reg}}(\Gamma_0(M);\mathbb{F}_p) \hookrightarrow M_2^{\mathrm{reg}}(\Gamma_0(pM);\mathbb{F}_p)$, it follows from (2.2.6), (2) that $a(n;\, f) = 0$ whenever $(n, M) = 1$. Then (2.2.7) implies that $f(q)$ is a constant, and we in fact have $f(q) = 0$ by (2.2.6), (1). This shows that $f = 0$, which is a contradiction.

(2) Let $\mathcal{I}'$ be the ideal generated by $T(l) - (1 + l)$ with prime numbers $l \nmid pM$. Since $\varepsilon' \neq \varepsilon'_+$, there certainly exists the Eisenstein series $E_{\varepsilon'} \in M_2^{\mathrm{reg}}(\Gamma_0(M); \mathbb{Z}_{(p)})^{\varepsilon'}$. We have the sequence of $\mathbb{Z}_{(p)}$-algebra homomorphisms

$$\mathbb{Z}_{(p)} \to \boldsymbol{T}(M; \mathbb{Z}_{(p)})^{\varepsilon'}/\mathcal{I}' \twoheadrightarrow \boldsymbol{T}(M; \mathbb{Z}_{(p)})^{\varepsilon'}/\mathcal{I}'^{\varepsilon'}_{\mathbb{Z}_{(p)}} \twoheadrightarrow \mathbb{Z}_{(p)} = \mathrm{End}_{\mathbb{Z}_{(p)}}(\mathbb{Z}_{(p)} E_{\varepsilon'})$$

where the right arrow is given by the action on $E_{\varepsilon'}$. By the first assertion, the left arrow is surjective, and hence the middle arrow is an isomorphism. □

When $\varepsilon' = \varepsilon'_+$, we have the following

LEMMA (3.5.6) *Let M and p be as in the previous lemma. Let I' be the ideal of $\mathbf{T}(M; \mathbb{Z}_{(p)})^{\varepsilon'_+}$ generated by $T(l) - (1 + l)$ with $l \nmid pM$. Then we have $I' = \mathbf{T}(M; \mathbb{Z}_{(p)})^{\varepsilon'_+}$.*

PROOF Assume otherwise. Since there is a surjection $\mathbb{Z}_{(p)} \twoheadrightarrow \mathbf{T}(M; \mathbb{Z}_{(p)})^{\varepsilon'_+}/I'$ by the previous lemma, we see that $\mathbf{T}(M; \mathbb{Z}_{(p)})^{\varepsilon'_+}/(p, I') \cong \mathbb{F}_p$. Thus we have a non-zero $f \in S_2^{\mathrm{reg}}(\Gamma_0(M); \mathbb{F}_p)^{\varepsilon'_+}$ such that $a(n; f) = \sigma(n)$ for $(n, pM) = 1$.

Let $\varepsilon = (-1, \varepsilon'_+)$ be the sign with respect to pM, and consider $E_\varepsilon \in M_2^{\mathrm{reg}}(\Gamma_0(pM); \mathbb{Z}_{(p)})^{\varepsilon}$. Then $g = f - E_\varepsilon \in M_2^{\mathrm{reg}}(\Gamma_0(pM); \mathbb{F}_p)$ satisfies $a(n; g) = 0$ for $(n, pM) = 0$. As in the proof of (3.5.5), (1) above, it follows from (2.2.6) and (2.2.7) that $g(q) = 0$ and hence $f(q) = E_\varepsilon(q)$. For the same reason as in the final part of the proof of (3.4.2), this implies that $f \mid_2 T(p) = f = (1 + p)f$, i.e. f is annihilated by the Eisenstein ideal of $\mathbf{T}(M; \mathbb{Z}_{(p)})^{\varepsilon'_+}$. By (3.4.2), such an f cannot exist. □

Now assume that N is divisible by a prime $p \geq 5$, and set $M = N/p$. Let

$$\Phi := J_0(N)_{/\overline{\mathbb{F}}_p}/J_0(N)^0_{/\overline{\mathbb{F}}_p} \tag{3.5.7}$$

be the group of connected components of $J_0(N)_{/\overline{\mathbb{F}}_p} = J_0(N)_{/\mathbb{F}_p} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$. By functoriality, G_{AL} acts on this group.

LEMMA (3.5.8) *Let the notation be as above. The group $\Phi[p^\infty]$ is cyclic, and w_p acts as -1, while w_l acts as the identity for any $l \mid M$, on this group.*

PROOF Let D be the degree-0 part of the free abelian group on the irreducible components Z_∞ and Z_0 of $X_0(N)_{/\mathbb{F}_p}$. Ribet [Ri, Theorem 2.4, Proposition 3.2] has shown that there is a functorial homomorphism $\theta : D \to \Phi$ whose cokernel is annihilated by 12. Therefore we have $\Phi[p^\infty] = \mathrm{Im}(\theta)[p^\infty]$, and this is clearly cyclic. Since w_p (resp. w_l with $l \mid M$) interchanges Z_∞ and Z_0 (resp. leaves Z_∞ and Z_0 stable), our result follows. See also Lorenzini [L, Section 2] where the mapping θ and the action of w_p are described more directly and generally. □

We are ready to prove the following

PROPOSITION (3.5.9) *Let $N = pM$ with a prime $p \geq 5$. Assume that $I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}$ is a proper ideal of $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$. Then under the notation* (3.5.1)–(3.5.3), *the dimension of $\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[\mathfrak{P}^{\boldsymbol{\varepsilon}}_p]$ over $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}/\mathfrak{P}^{\boldsymbol{\varepsilon}}_p$ is at most one.*

PROOF Let T be the maximal torus of $J_0(N)^0_{/\mathbb{F}_p}$. Then it is well-known that $J_0(N)^0_{/\mathbb{F}_p}/T$ is canonically isomorphic to $J_0(M)_{/\mathbb{F}_p} \times J_0(M)_{/\mathbb{F}_p}$. Via this isomorphism, the endomorphism $T(l)$ ($l \nmid N$) (resp. $w_{l'}$ ($l' \mid M$)) of $J_0(N)_{/\mathbb{F}_p}$ induces $T(l) \times T(l)$ (resp. $w_{l'} \times w_{l'}$) on $J_0(M)_{/\mathbb{F}_p} \times J_0(M)_{/\mathbb{F}_p}$, while w_p on $J_0(N)_{/\mathbb{F}_p}$ interchanges the two factors of $J_0(M)_{/\mathbb{F}_p} \times J_0(M)_{/\mathbb{F}_p}$. Since $T(\overline{\mathbb{F}}_p)$ has no non-trivial p-torsion, we have the exact sequence

$$0 \to (J_0(M)_{/\mathbb{F}_p} \times J_0(M)_{/\mathbb{F}_p})(\overline{\mathbb{F}}_p)[p^\infty] \to \mathcal{G}_p(N) \to \Phi[p^\infty] \to 0\,.$$

Assume for the moment that $M > 1$ and write $\boldsymbol{\varepsilon} = (\varepsilon_1, \boldsymbol{\varepsilon}')$ where $\varepsilon_1 = \pm 1$ corresponds to the prime factor p of N and $\boldsymbol{\varepsilon}' \in \boldsymbol{E}'$.

If $\boldsymbol{\varepsilon} \neq (-1, \boldsymbol{\varepsilon}'_+)$, the previous lemma implies that

$$\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}} \cong J_0(M)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty]^{\boldsymbol{\varepsilon}'}\,.$$

Since we are assuming that $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \neq I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}$, it follows from (3.4.2) that $\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+$ and hence $\boldsymbol{\varepsilon}' \neq \boldsymbol{\varepsilon}'_+$. Therefore by (3.5.5), we obtain

$$\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[\mathfrak{P}^{\boldsymbol{\varepsilon}}_p] \cong J_0(M)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty]^{\boldsymbol{\varepsilon}'}[\mathfrak{P}'^{\boldsymbol{\varepsilon}'}_p]$$

where $\mathfrak{P}'^{\boldsymbol{\varepsilon}'}_p = (I'^{\boldsymbol{\varepsilon}'}_{\mathbb{Z}_{(p)}}, p) \subseteq \mathbf{T}(M;\mathbb{Z}_{(p)})$. Our claim then follows from (3.5.4).

Next assume that $\boldsymbol{\varepsilon} = (-1, \boldsymbol{\varepsilon}'_+)$. This time, (3.5.6) implies that

$$\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[\mathfrak{P}^{\boldsymbol{\varepsilon}}_p] \hookrightarrow \Phi[p^\infty]^{\boldsymbol{\varepsilon}}[\mathfrak{P}^{\boldsymbol{\varepsilon}}_p]\,.$$

Since $\Phi[p^\infty]$ is a cyclic group by the previous lemma, the conclusion follows. This second argument also settles the case $M = 1$. □

From (3.5.4) and (3.5.9), we deduce:

THEOREM (3.5.10) *Let p be an odd prime. We further assume that $p \geq 5$ when $3 \mid N$. If $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$ is not the zero ring, the Pontrjagin dual of $\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}]$ is a cyclic module over $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$.*

PROOF If $I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}} = \mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$, the conclusion is obvious, and hence we assume otherwise in what follows. The ideal $\mathfrak{P}^{\boldsymbol{\varepsilon}}_p$ is thus a maximal ideal of $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$.

Let us indicate by the superscript "$\widehat{\ }$" the Pontrjagin dual. By (3.5.4) and (3.5.9), $\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[\mathfrak{P}^{\boldsymbol{\varepsilon}}_p]\widehat{\ } \cong \mathcal{G}_p(N)^{\boldsymbol{\varepsilon}\widehat{\ }}/\mathfrak{P}^{\boldsymbol{\varepsilon}}_p = (\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}\widehat{\ }})_{\mathfrak{P}^{\boldsymbol{\varepsilon}}_p}/\mathfrak{P}^{\boldsymbol{\varepsilon}}_p$ is a cyclic module over $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}_{\mathfrak{P}^{\boldsymbol{\varepsilon}}_p}$, where the subscript "$\mathfrak{P}^{\boldsymbol{\varepsilon}}_p$" means the localization. Nakayama's lemma implies that $(\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}\widehat{\ }})_{\mathfrak{P}^{\boldsymbol{\varepsilon}}_p}$ is a cyclic $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}_{\mathfrak{P}^{\boldsymbol{\varepsilon}}_p}$-module. Since $\mathfrak{P}^{\boldsymbol{\varepsilon}}_p$ is the unique maximal

ideal containing $I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}$, we see that $\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}]\widehat{\ } \cong \mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}\widehat{\ }/I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}} = (\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}\widehat{\ })_{\mathfrak{P}^{\boldsymbol{\varepsilon}}_p}/I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}$ is a cyclic $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}_{\mathfrak{P}^{\boldsymbol{\varepsilon}}_p}$-module, and our conclusion follows. □

3.6. Rational torsion in $J_0(N)$. Recall that $X_0(N)$ has 2^m cusps all of which are rational over $\mathbb{Q}$. We denote by $\mathcal{C}(N)$ the subgroup of $J_0(N)(\mathbb{Q})$ consisting of the classes of divisors of degree zero supported at the cusps. Its order, the cuspidal class number of $X_0(N)$, was computed by Takagi:

THEOREM (3.6.1) ([T, Theorem 5.1]). *We have*

$$|\mathcal{C}(N)| = 2^a \times \prod_{\boldsymbol{\varepsilon}\in\boldsymbol{E}} c(N;\boldsymbol{\varepsilon})$$

with an integer $a \geq 0$, where the numbers $c(N;\boldsymbol{\varepsilon})$ are given by (3.1.2). (Takagi's theorem also gives the exponent a explicitly, but we will not need this.)

For any odd prime p, $J_0(N)(\mathbb{Q})[p^\infty]$ and $\mathcal{C}(N)[p^\infty]$ are modules over $\mathbf{T}(N;\mathbb{Z}_{(p)})$, and we can decompose them as in (2.1.3). The following is the main result of this paper:

THEOREM (3.6.2). *Let p be an odd prime, and assume that $p \geq 5$ when 3 divides N. Then we have*

$$J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}} = \mathcal{C}(N)[p^\infty]^{\boldsymbol{\varepsilon}} \cong \mathbb{Z}_{(p)}/c(N;\boldsymbol{\varepsilon})\mathbb{Z}_{(p)}$$

for all $\boldsymbol{\varepsilon} \in \boldsymbol{E}$.

PROOF. We first claim that $|J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}}| \leq |\mathbb{Z}_{(p)}/c(N;\boldsymbol{\varepsilon})\mathbb{Z}_{(p)}|$ for each $\boldsymbol{\varepsilon} \in \boldsymbol{E}$. Let $\boldsymbol{\varepsilon} = (\varepsilon_1,\dots,\varepsilon_m)$. The homomorphism $\prod_{i=1}^m(1+\varepsilon_i w_{l_i}) : J_0(N) \to (\prod_{i=1}^m(1+\varepsilon_i w_{l_i}))J_0(N)$ sends $J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}}$ isomorphically onto its image. The cotangent space of $J_0(N)$ at the origin is canonically isomorphic to $S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Q})$, and the image of the cotangent mapping of the above homomorphism corresponds to $S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Q})^{\boldsymbol{\varepsilon}}$. Therefore when this space is trivial, $J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}}$ is also trivial. We may thus assume that $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \neq \{0\}$.

In general, when l is an odd prime, the reduction modulo l mapping $J_0(N)(\mathbb{Q}) \to J_0(N)_{/\mathbb{F}_l}(\mathbb{F}_l)$ is injective on the torsion part (including the l-torsion part) of $J_0(N)(\mathbb{Q})$ by Katz [K3, Appendix]. (One can also deduce this from the result of Raynaud [Ra, Théorème 3.3.3.]) On the other hand, when l' is a prime not dividing N, we see from the Eichler-Shimura congruence relation that $T(l') = 1 + l'$ on $J_0(N)_{/\mathbb{F}_{l'}}(\mathbb{F}_{l'})$. Noting that p is odd, it is easy to deduce that $I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}$ annihilates $J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}}$.

Therefore $J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}}$ is mapped injectively into $\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}]$ by the reduction modulo p mapping, and we especially have

$$|J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}}| \leq |\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}]|\,.$$

But by (3.5.10), we have

$$|\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}]| \leq |\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}/I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}|\,,$$

while by (3.1.3), we have

$$|\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}/I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}| = |\mathbb{Z}_{(p)}/c(N;\boldsymbol{\varepsilon})\mathbb{Z}_{(p)}|\,,$$

which proves our claim.

Consequently, we obtain

$$|J_0(N)(\mathbb{Q})[p^\infty]| \leq \prod_{\boldsymbol{\varepsilon}\in\boldsymbol{E}} |\mathbb{Z}_{(p)}/c(N;\boldsymbol{\varepsilon})\mathbb{Z}_{(p)}|\,.$$

By Takagi's theorem, the right hand side is equal to $|\mathcal{C}(N)[p^\infty]|$. Since $\mathcal{C}(N)[p^\infty]$ is *a priori* contained in $J_0(N)(\mathbb{Q})[p^\infty]$, we conclude that

$$J_0(N)(\mathbb{Q})[p^\infty] = \mathcal{C}(N)[p^\infty]$$

and that the above inequalities are in fact equalities. Thus for each $\boldsymbol{\varepsilon} \in \boldsymbol{E}$, we have

$$J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}} = \mathcal{C}(N)[p^\infty]^{\boldsymbol{\varepsilon}}$$

and its order is equal to $|\mathbb{Z}_{(p)}/c(N;\boldsymbol{\varepsilon})\mathbb{Z}_{(p)}|$.

It remains to show that each $\mathcal{C}(N)[p^\infty]^{\boldsymbol{\varepsilon}}$ is a cyclic group. This is obvious when $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_+$, and hence we assume otherwise. Then we have seen in the course of the proof of (3.2.5) that $(\mathbb{Z}_{(p)}[\mathcal{C}_N]^0)^{\boldsymbol{\varepsilon}}$ is a free $\mathbb{Z}_{(p)}$-module of rank one. Therefore, its quotient group $\mathcal{C}(N)[p^\infty]^{\boldsymbol{\varepsilon}}$ is cyclic. □

From the proof above, we also obtain the following partial generalization of [Ma, II, Proposition (14.9)]:

COROLLARY (3.6.3). *Let p be as in the previous theorem. Then $\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}]$ coincides with the image of $\mathcal{C}(N)[p^\infty]^{\boldsymbol{\varepsilon}}$ under the reduction modulo p mapping.*

PROOF. We have proved this assertion under the assumption $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \neq \{0\}$. But if $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} = \{0\}$, both $\mathcal{G}_p(N)^{\boldsymbol{\varepsilon}}[I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}]$ and $\mathcal{C}(N)[p^\infty]^{\boldsymbol{\varepsilon}}$ are trivial. □

As the final remark, we note the following: We needed the assumption that $p \neq 3$ when $3 \mid N$ only to assure (3.5.9). If that proposition holds in the case $p = 3$, then (3.6.2) also holds without this assumption.

References

[A] A. AGASHE, Rational torsion in elliptic curves and the cuspidal subgroup, preprint.

[AL] A. O. L. ATKIN and J. LEHNER, Hecke operators on $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[D] P. DELIGNE, Courbes elliptiques: Formulaire, d'après J. Tate, In: *Modular functions of one variable IV*, Lecture Notes in Math. **476** (1975), 53–73.

[DR] P. DELIGNE and M. RAPOPORT, Les schémas de modules de courbes elliptiques, In: *Modular functions of one variable II*, Lecture Notes in Math. **349** (1973), 143–316.

[E1] B. EDIXHOVEN, The weight in Serre's conjectures on modular forms, Invent. Math. **109** (1992), 563–594.

[E2] B. EDIXHOVEN, Serre's conjecture, In: *Modular forms and Fermat's Last Theorem*, ed. by G. Cornell, J. Silverman and G. Stevens, Springer-Verlag (1997), 209–242.

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

[H] E. HECKE, Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik, Abh. Math. Sem. Hamburg **5** (1927), 199–224 (Math. Werke No. 24).

[K1] N. KATZ, p-adic properties of modular schemes and modular forms, In: *Modular functions of one variable III*, Lecture Notes in Math. **350** (1973), 69–190.

[K2] N. KATZ, p-adic interpolation of real analytic Eisenstein series, Ann. Math. **104** (1976), 459–571.

[K3] N. KATZ, Galois properties of torsion points on abelian varieties, Invent. Math. **62** (1981), 481–502.

[KM] N. KATZ and B. MAZUR, Arithmetic moduli of elliptic curves, Ann. of Math. Stud. **108** (1985).

[KL] D. KUBERT and S. LANG, *Modular units*, Springer-Verlag (1981).

[L] D. LORENZINI, Torsion points on the modular Jacobian $J_0(N)$, Comp. Math. **96** (1995), 149–172.

[Ma] B. MAZUR, Modular curves and the Eisenstein ideal, Publ. Math. IHES **47** (1977), 33–186.

[MR] B. MAZUR and K. RIBET, Two-dimensional representations in the arithmetic of modular curves, Astérisque **196–197** (1991), 215–255.

[Mu] D. MUMFORD, *Abelian varieties*, Oxford Univ. Press (1970).

[Og1] A. OGG, Rational points on certain elliptic modular curves, Proc. Symp. Pure Math. **24** (1973), 221–231.

[Og2] A. OGG, Diophantine equations and modular forms, Bull. AMS **81** (1975), 14–27.

[Oh1] M. OHTA, On the p-adic Eichler-Shimura isomorphism for Λ-adic cusp forms, J. reine angew. Math. **463** (1995), 49–98.

[Oh2] M. OHTA, Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties, J. Math. Soc. Japan **65** (2013), 733–772.

[Ra] M. RAYNAUD, Schémas en groupes de type $(p, \dots, p)$, Bull. Soc. Math. Fr. **102** (1974), 241–280.

[Ri] K. RIBET, On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, Invent. Math. **100** (1990), 431–476.

[Se1] J.-P. SERRE, Sur la topologie des variétés algébriques en caractéristique p, Symp. Int. Top. Alg., Mexico (1958), 24–53 (Œuvre I, No. 38).

[Se2] J.-P. SERRE, Formes modulaires et fonctions zêta p-adiques, In: *Modular functions of one variable III*, Lecture Notes in Math. **350** (1973), 191–268.

[Sh] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton Univ. Press (1971).

[T] T. TAKAGI, The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free, J. Alg. **193** (1997), 180–213.

Present Address:
TOKAI UNIVERSITY,
HIRATSUKA, KANAGAWA 259–1292, JAPAN.
e-mail: ohta@tokai-u.jp