J. Math. Soc. Japan
Vol. 59, No. 4 (2007) pp. 913–951
doi: 10.2969/jmsj/05940913

Companion forms and the structure of p-adic Hecke algebras II

By Masami Ohta

(Received Aug. 11, 2006)
(Revised Aug. 24, 2006)

Abstract. The subject of this paper is to study the structure of the Eisenstein component of Hida's universal ordinary p-adic Hecke algebra attached to modular forms (rather than cusp forms). We give a sufficient condition for such a ring to be Gorenstein in terms of companion forms in characteristic p; and also a numerical criterion which assures the validity of that condition. This type of result was already obtained in our previous work, in which two cases were left open. The purpose of this work is to extend our method to cover these remaining cases. New ingredients of the proof consist of: a new construction of a pairing between modular forms over a finite field; and a comparison result for ordinary modular forms of weight two with respect to $\Gamma_1(N)$ and $\Gamma_1(N) \cap \Gamma_0(p)$. We also describe the Iwasawa module attached to the cyclotomic $\boldsymbol{Z}_p$-extension of an abelian number field in terms of the Eisenstein ideal, when an appropriate Eiesenstein component is Gorenstein.

Introduction.

This article is a continuation of our previous investigation [**O4**] under the same title, and is of nature supplementary to it.

We fix a prime number $p \geq 5$, and a positive integer N prime to p, throughout this paper. Let $\mathfrak{r}$ be the ring of integers of a finite extension of $\boldsymbol{Q}_p$, and $\mathfrak{k}$ its residue field. We denote by $\Lambda_{\mathfrak{r}}$ the Iwasawa algebra over $\mathfrak{r}$, by which we mean the completed group algebra over $\mathfrak{r}$ of the multiplicative group $1 + p\boldsymbol{Z}_p$. As usual, we fix a topological generator γ of $1 + p\boldsymbol{Z}_p$, and identify $\Lambda_{\mathfrak{r}}$ with the ring of formal power series $\mathfrak{r}[[T]]$ via $\gamma \leftrightarrow 1 + T$.

We then consider Hida's universal ordinary p-adic Hecke algebra $e\mathscr{H}(N;\mathfrak{r})$ (resp. $e\,h(N;\mathfrak{r})$) of level N over $\mathfrak{r}$ attached to modular forms (resp. cusp forms). One of its definition is that it is the $\Lambda_{\mathfrak{r}}$-algebra generated by all Hecke operators $T(n)$ acting on ordinary $\Lambda_{\mathfrak{r}}$-adic modular forms (resp. $\Lambda_{\mathfrak{r}}$-adic cusp forms) of level N. It is an algebra finite and flat over $\Lambda_{\mathfrak{r}}$, and hence can be decomposed as a direct sum of localizations at its finite number of maximal ideals.

Take primitive Dirichlet characters χ and ψ defined modulo u and v, respectively. We assume that $uv = N$, and that $\mathfrak{r}$ contains the values of χ and ψ. Set $\vartheta := \chi\omega^i$ with ω the Teichmüller character, and assume that

$$\begin{cases} (\vartheta\psi)(-1) = 1; & \text{and} \\ (\vartheta, \psi) \neq (\omega^2, \mathbf{1}), (\mathbf{1}, \mathbf{1}) \end{cases}$$

2000 *Mathematics Subject Classification.* Primary 11F33; Secondary 11F80.
Key Words and Phrases. p-adic Hecke algebras, companion forms, Iwasawa theory.

where $\mathbf{1}$ denotes the trivial character. We can associate, in a natural manner, a $\Lambda_{\mathfrak{r}}$-adic Eisenstein series $\mathscr{E}(\vartheta,\psi)$ of level N, which interpolates classical Eisensein series. Define the Eisenstein ideal $\mathscr{I}(\vartheta,\psi)$ of $e\mathscr{H}(N;\mathfrak{r})$ as the annihilator of $\mathscr{E}(\vartheta,\psi)$. There is the unique maximal ideal $\mathfrak{M}(\vartheta,\psi)=\mathfrak{M}$ of $e\mathscr{H}(N;\mathfrak{r})$ containing it, the Eisenstein maximal ideal attached to $\mathscr{E}(\vartheta,\psi)$, and we are interested in the structure of the localization $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ at this maximal ideal. (Even if $(\vartheta,\psi)=(\omega^2,\mathbf{1})$ or $(\mathbf{1},\mathbf{1})$, we can consider $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$. But these cases are of no interest to us: in each case, the ring $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ is isomorphic to $\Lambda_{\mathfrak{r}}$, and the Iwasawa module $\mathrm{Gal}(L_\infty/K_\infty)_{(\vartheta\omega)^{-1}}$ below vanishes.)

On the other hand, with χ and ψ as above, we can associate the classical Eisenstein series of weight m and level N:

$$E_m(\chi,\psi):=c+\sum_{n=1}^{\infty}\left(\sum_{0<t|n}\chi(t)\psi\left(\frac{n}{t}\right)t^{m-1}\right)q^n$$

with some constant c, for each integer $m\geq 1$ satisfying $(\chi\psi)(-1)=(-1)^m$, unless $k=2$ and $\chi=\psi=\mathbf{1}$.

For the exponent i as above, we take an integer d such that $d\equiv i \bmod p-1$ and $0\leq d\leq p-2$; and set $k:=d+2$. Let $M_k(\Gamma_1(N);\mathfrak{k})$ be the space of modular forms of weight k with respect to $\Gamma_1(N)$ over $\mathfrak{k}$ (in the sense of Katz [**Ka1**]). Then the annihilator of the image of $E_k(\chi,\psi)$ in $M_k(\Gamma_1(N);\mathfrak{k})$, in the Hecke algebra acting on this space, is a maximal ideal and hence we can consider the corresponding localization $M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}$. Setting $k':=p+1-k$, we similarly define the localization $M_{k'}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}$ using $E_{k'}(\psi,\chi)$. In the following theorem, we denote by θ the operator introduced by Serre and Katz, which acts as $q(d/dq)$ on q-expansions:

THEOREM I. *Assume that p does not divide $\varphi(N)$ (the Euler function), and also that $\chi(p)\neq\psi(p)$ when $d=p-2$.*

1) *If the dimension over $\mathfrak{k}$ of the space*:

$$\{f\in M_{k'}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}\mid \theta^k f=\theta g \text{ with some } g\in M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}\}$$

is one, then $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ is a Gorenstein ring;

2) *If the number*:

$$\left(\prod_{\substack{l|N\\ l\nmid \mathrm{cond}(\chi^{-1}\psi)}}(l^{k'}-(\chi\psi^{-1})(l))\right)B_{k',\chi^{-1}\psi}\in\mathfrak{r}$$

is a unit, then the $\mathfrak{k}$-vector space in 1) *is one-dimensional. Here, $B_{k',\chi^{-1}\psi}$ denotes the generalized Bernoulli number.*

As a consequence, the numerical condition in 2) implies that $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ is Gorenstein. This type of result was, among other things, already obtained by Skinner

and Wiles [**SW**], when $\psi = \mathbf{1}$. In our previous work [**O4**], we used a method totally different from [**SW**], and proved Theorem I for $1 \leq d \leq p-3$. (In [**O4**, Theorems 3.2.3 and 3.3.2], we stated the results using the space of f as above with $g \in M_k(\Gamma_1(N); \mathfrak{k})$ rather than in $M_k(\Gamma_1(N); \mathfrak{k})_{\mathfrak{m}}$; but that formulation is equivalent to the present one. See [**O4**, Proposition 3.1.2] and the proof of Lemma 2.3.3 in the text.) The purpose of this paper is to extend our method to cover the remaining cases where $d = 0$ and $d = p-2$.

We will also extend the results in [**O4**, 3.4]. To state this, let χ be a Dirichlet character of conductor N, and assume that $\vartheta = \chi\omega^i$ is even. We take $\mathfrak{r}$ as the ring generated over $\boldsymbol{Z}_p$ by the values of χ. Let K be the imaginary abelian extension of $\boldsymbol{Q}$ corresponding to $\vartheta\omega$, and K_∞ its cyclotomic $\boldsymbol{Z}_p$-extension. Let L_∞ be the maximal unramified abelian pro-p-extension of K_∞. The character $(\vartheta\omega)^{-1}$ induces a ring homomorphism of $\boldsymbol{Z}_p[\mathrm{Gal}(K/\boldsymbol{Q})]$ to $\mathfrak{r}$, and using this, we form the tensor product

$$\mathrm{Gal}(L_\infty/K_\infty)_{(\vartheta\omega)^{-1}} := \mathrm{Gal}(L_\infty/K_\infty) \otimes_{\boldsymbol{Z}_p[\mathrm{Gal}(K/\boldsymbol{Q})]} \mathfrak{r}$$

(the "$(\vartheta\omega)^{-1}$-part" of $\mathrm{Gal}(L_\infty/K_\infty)$). Via the isomorphism: $\mathfrak{r}[[\mathrm{Gal}(K_\infty/K)]] \xrightarrow{\sim} \Lambda_{\mathfrak{r}}$ induced by the p-cyclotomic character, we consider this group as a $\Lambda_{\mathfrak{r}}$-module in the usual manner. Let $I(\vartheta, \mathbf{1}) = I$ be the image of $\mathscr{I}(\vartheta, \mathbf{1})_{\mathfrak{M}(\vartheta,\mathbf{1})}$ in $e\,h(N; \mathfrak{r})_{\mathfrak{M}(\vartheta,\mathbf{1})}$, the Eisenstein ideal of $e\,h(N; \mathfrak{r})_{\mathfrak{M}(\vartheta,\mathbf{1})}$.

THEOREM II. *Assume that $p \nmid \varphi(N)$, and that $\chi(p) \neq 1$ when $d = p-2$. If $e\,\mathscr{H}(N; \mathfrak{r})_{\mathfrak{M}(\vartheta,\mathbf{1})}$ is a Gorenstein ring, we have an isomorphism*

$$\mathrm{Gal}(L_\infty/K_\infty)_{(\vartheta\omega)^{-1}} \cong (I/I^2)^\dagger$$

of $\Lambda_{\mathfrak{r}}$-modules. Here, $(I/I^2)^\dagger$ has the same underlying group as I/I^2 on which the action of $\Lambda_{\mathfrak{r}}$ is twisted by the involutive $\mathfrak{r}$-automorphism of $\Lambda_{\mathfrak{r}}$ given by: $T \mapsto \gamma^{-1}(1+T)^{-1} - 1$.

Let us now explain the contents of the text.

In our proof of Theorem I for $1 \leq d \leq p-3$ in [**O4**], aside from our former works, inportant roles were played by:

(i) Ulmer's pairing between modular forms over finite fields ([**U1**]); and

(ii) Gouvêa's comparison theorem for ordinary modular forms with respect to $\Gamma_1(N)$ and $\Gamma_1(N) \cap \Gamma_0(p)$ ([**Go**]).

In the cases excluded in [**O4**], some problems arise regarding these points.

As for (i), though Ulmer defined his pairing for cusp forms of weight k with $2 \leq k \leq p$, his construction, as it stands, does not extend to a pairing

$$M_k(\Gamma_1(N); \mathfrak{k}) \times S_k(\Gamma_1(N); \mathfrak{k}) \to \mathfrak{k}$$

for $k = p$. In Section 1, we give a new construction of such a pairing. It is based on another idea of Ulmer: Instead of considering the Selmer group of the universal elliptic curve over the Igusa curve, we make use of a pairing between modular forms on supersingular elliptic curves defined in [**U1**]. Applying a suitable power of the θ-operator

and twisting, we obtain from it a pairing of the form above, which is compatible with the Hecke operators $T(l)$ (for prime numbers $l \neq p$) and the diamond operators. In general, this new pairing has larger left kernel than the previous one, but we show that it behaves well on ordinary components. Our main result in this direction is Theorem 1.6.5. Though we need this new pairing only in studying the special case where $d = p-2$, we hope that it is of independent interest.

On the other hand, as for (ii), Gouvêa's argument was based on the fact that no "p-new" form of weight $k \geq 3$ with respect to $\Gamma_1(N) \cap \Gamma_0(p)$ is ordinary, which fails to hold when $k = 2$. In Section 2, we take another method, using the trace mapping for modular forms of weight two, from $\Gamma_1(N) \cap \Gamma_0(p)$ to $\Gamma_1(N)$, to establish a comparison result for "p-old" ordinary components. See Theorem 2.2.11 for this. This also allows us to extend some of results of Gouvêa to the weight two case. With this theorem and its corollary, the proof of Theorem I proceeds almost in the same way as in [**O4**] when $d = 0$.

In Section 3, we give the proof of Theorem I when $d = p-2$. As for the part 1), we first show that the one-dimensionality of the space in question is actually equivalent to that of $M_1(\Gamma_1(N); \mathfrak{k})_{\mathfrak{m}'}$ itself. We then argue under this latter assumption, employing our new pairing for $k = p$, to prove 1).

In the final Section 4, we prove Theorem II, using the method of Harder and Pink [**HP**] and Kurihara [**Ku**], along the same line as in our previous works.

CORRECTION TO [**O4**]: The proof of the statement that the Eisenstein ideal I^* is generated by $T^*(l) - 1 - lT^*(l,l)$ with prime numbers $l \nmid Np$ ([**O4**, p. 170, l. 6]) was incomplete. Corrected proof will be given in 4.1 in the text.

1. Pairings between modular forms over finite fields.

1.1. Preliminaries.

We throughout fix a prime number $p \geq 5$, and a positive integer N prime to p. We first fix our terminology on algebraic theory of modular forms.

For an integer k, a modular form f of weight k with respect to $\Gamma_1(N)$ (in the sense of Katz [**Ka1**]) over a $\boldsymbol{Z}[1/N]$-algebra R is a rule which assigns to each pair (E, α) consisting of:

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

a section $f(E, \alpha) \in \Gamma(S, \underline{\omega}_E^{\otimes k})$ satisfying:

$$\begin{cases} \text{the formation of } f(E,\alpha) \text{ is compatible with cartesian squares;} \\ f \text{ is holomorphic at every cusp.} \end{cases} \tag{1.1.2}$$

Here, $\underline{\omega}_E$ is the direct image of $\Omega^1_{E/S}$ to S; and for the precise meaning of the second condition above, see [**Ka1**, 1.1 and 1.2]; and also Hida [**Hi**, Section 1]. We denote by $M_k(\Gamma_1(N); R)$ the space of all such forms. An element of this space is called a cusp form if it vanishes at every cusp (cf. loc. cit.); and we denote by $S_k(\Gamma_1(N); R)$ the subspace of

cusp forms. The formation of $M_k(\Gamma_1(N);R)$ and $S_k(\Gamma_1(N);R)$ commutes with the change of base rings provided that $k \geq 2$; and in addition that 6 is invertible in the base rings when $N = 1$ (cf. Gross [**Gr**, Proposition 2.5, Section 10]). However, this property does not hold when $k = 1$ (cf. Serre [**S1**]). We stress that, for forms of weight one over finite fields, we use this definition, rather than to restrict to forms that is obtained by reduction from the ones in characteristic zero.

Via the q-expansion at the cusp infinity, we have injections:

$$\begin{cases} M_k(\Gamma_1(N);R) \hookrightarrow R[[q]], \\ S_k(\Gamma_1(N);R) \hookrightarrow R[[q]]. \end{cases} \tag{1.1.3}$$

We will often identify the spaces in the left-hand side with their images in $R[[q]]$. When R is a subring of $\boldsymbol{C}$, $M_k(\Gamma_1(N);R)$ (resp. $S_k(\Gamma_1(N);R)$) may be identified with the space of modular forms (resp. cusp forms) in the classical sense having q-expansions with coefficients in R. More generally, when R is a $\boldsymbol{Z}[1/6N]$-algebra and $k \geq 2$, we have the following description as subsets of $R[[q]]$:

$$\begin{cases} M_k(\Gamma_1(N);R) = (M_k(\Gamma_1(N);\boldsymbol{C}) \cap \boldsymbol{Z}[[q]]) \otimes_{\boldsymbol{Z}} R, \\ S_k(\Gamma_1(N);R) = (S_k(\Gamma_1(N);\boldsymbol{C}) \cap \boldsymbol{Z}[[q]]) \otimes_{\boldsymbol{Z}} R. \end{cases} \tag{1.1.4}$$

We denote by $X_1(N)_{/R}$ the usual modular curve over R attached to $\Gamma_1(N)$. It is the smooth compactification of the (coarse) moduli scheme $Y_1(N)_{/R}$ classifying the pairs as in (1.1.1).

From now on, until the end of 1.6*, we assume that* $N \geq 5$. Then $Y_1(N)_{/R}$ is in fact the fine moduli scheme, and there is the invertible sheaf $\underline{\omega}$ corresponding to the universal elliptic curve on it. The sheaf $\underline{\omega}$ extends to an invertible sheaf on $X_1(N)_{/R}$ in a natural manner (cf. [**Gr**, Section 2], [**Ka1**, 1.5]), and we will use the same symbol $\underline{\omega}$ for this. We then have the following identification:

$$\begin{cases} M_k(\Gamma_1(N);R) = H^0(X_1(N)_{/R}, \underline{\omega}^{\otimes k}), \\ S_k(\Gamma_1(N);R) = H^0(X_1(N)_{/R}, \underline{\omega}^{\otimes k}(-\text{cusps})) \end{cases} \tag{1.1.5}$$

the symbol "cusps" meaning the reduced divisor supported at cusps. We recall that there is a canonical isomorphism:

$$\underline{\omega}^{\otimes 2} \cong \Omega^1_{X_1(N)_{/R}/R}(\text{cusps}) \tag{1.1.6}$$

called the Kodaira-Spencer isomorphism (cf. [**Gr**, Proposition 2.3], [**Ka1**, 1.5]).

1.2. Modular forms over finite fields.

We fix a finite field $\mathfrak{k}$ of characteristic p, and consider modular forms over this field. We set $C := X_1(N)_{/\mathfrak{k}}$ and $C^0 := Y_1(N)_{/\mathfrak{k}}$ for notational simplicity. The invertible sheaf $\underline{\omega}$ on C has positive degree, and we have:

$$\begin{cases} H^0(C, \underline{\omega}^{\otimes m}) = 0 & \text{for } m < 0, \\ H^1(C, \underline{\omega}^{\otimes m}) = 0 & \text{for } m \geq 2. \end{cases} \tag{1.2.1}$$

Let $A \in M_{p-1}(\Gamma_1(1); \mathfrak{k})$ be the form corresponding to the Hasse invariant. Then there is an exact sequence of sheaves on C considered by Serre ([**S1**], [**S2**]):

$$0 \to \underline{\omega}^{\otimes(k-p+1)} \overset{\times A}{\to} \underline{\omega}^{\otimes k} \to \underline{SS}_k \to 0 \tag{1.2.2}$$

$\underline{SS}_k$ being the skyscraper sheaf defined by the exactness of the sequence. Taking the long exact sequence of cohomology, we obtain an exact sequence:

$$\begin{aligned} 0 \to M_{k-p+1}(\Gamma_1(N); \mathfrak{k}) \overset{\times A}{\to} M_k(\Gamma_1(N); \mathfrak{k}) \to SS_k(\Gamma_1(N); \mathfrak{k}) \\ \to H^1(C, \underline{\omega}^{\otimes(k-p+1)}) \to H^1(C, \underline{\omega}^{\otimes k}) \to 0 \end{aligned} \tag{1.2.3}$$

where $SS_k(\Gamma_1(N); \mathfrak{k}) := H^0(C, \underline{SS}_k)$ is the space of modular forms of weight k with respect to $\Gamma_1(N)$ on supersingular elliptic curves. Its element f may be identified with a rule as in 1.1 with the pairs (E, α) restricted to supersingular elliptic curves over extension fields of $\mathfrak{k}$.

The Kodaira-Spencer isomorphism (1.1.5) and the Serre duality give us the isomorphism:

$$H^1(C, \underline{\omega}^{\otimes m}) \cong H^0(C, \underline{\omega}^{\otimes(2-m)}(-\text{cusps}))^\vee = S_{2-m}(\Gamma_1(N); \mathfrak{k})^\vee \tag{1.2.4}$$

where the superscript "$\vee$" indicates the $\mathfrak{k}$-dual. Thus the exact sequence (1.2.3) reads:

$$\begin{cases} 0 \to SS_k(\Gamma_1(N); \mathfrak{k}) \to S_{p+1-k}(\Gamma_1(N); \mathfrak{k})^\vee \to S_{2-k}(\Gamma_1(N); \mathfrak{k})^\vee \to 0 \quad (k < 0); \\ 0 \to \mathfrak{k} \to SS_0(\Gamma_1(N); \mathfrak{k}) \to S_{p+1}(\Gamma_1(N); \mathfrak{k})^\vee \to S_2(\Gamma_1(N); \mathfrak{k})^\vee \to 0 \quad (k = 0); \\ 0 \to M_1(\Gamma_1(N); \mathfrak{k}) \to SS_1(\Gamma_1(N); \mathfrak{k}) \to S_p(\Gamma_1(N); \mathfrak{k})^\vee \to S_1(\Gamma_1(N); \mathfrak{k})^\vee \to 0 \ (k = 1); \\ 0 \to M_k(\Gamma_1(N); \mathfrak{k}) \to SS_k(\Gamma_1(N); \mathfrak{k}) \to S_{p+1-k}(\Gamma_1(N); \mathfrak{k})^\vee \to 0 \ (2 \leq k \leq p-2); \\ 0 \to \mathfrak{k} \overset{\times A}{\to} M_{p-1}(\Gamma_1(N); \mathfrak{k}) \to SS_{p-1}(\Gamma_1(N); \mathfrak{k}) \to S_2(\Gamma_1(N); \mathfrak{k})^\vee \to 0 \ (k = p-1); \\ 0 \to M_1(\Gamma_1(N); \mathfrak{k}) \overset{\times A}{\to} M_p(\Gamma_1(N); \mathfrak{k}) \to SS_p(\Gamma_1(N); \mathfrak{k}) \to S_1(\Gamma_1(N); \mathfrak{k})^\vee \to 0 \ (k = p); \\ 0 \to M_{k-p+1}(\Gamma_1(N); \mathfrak{k}) \overset{\times A}{\to} M_k(\Gamma_1(N); \mathfrak{k}) \to SS_k(\Gamma_1(N); \mathfrak{k}) \to 0 \quad (k \geq p+1). \end{cases} \tag{1.2.5}$$

When $k \geq p-1$, the injection $\times A : M_{k-p+1}(\Gamma_1(N); \mathfrak{k}) \to M_k(\Gamma_1(N); \mathfrak{k})$ preserves q-expansions. In the following, we often identify $f \in M_{k-p+1}(\Gamma_1(N); \mathfrak{k})$ with $Af \in M_k(\Gamma_1(N); \mathfrak{k})$, and thus regard $M_{k-p+1}(\Gamma_1(N); \mathfrak{k})$ as a subspace of $M_k(\Gamma_1(N); \mathfrak{k})$.

There are standard operators acting on $M_k(\Gamma_1(N); \mathfrak{k})$ and $S_k(\Gamma_1(N); \mathfrak{k})$: the diamond operators $\langle a \rangle$ for $a \in (\boldsymbol{Z}/N\boldsymbol{Z})^\times$ and the Hecke operators $T(n)$ for positive integers n, for $k \geq 1$. We recall that there is an automorphism $\langle a \rangle$ of C over $\mathfrak{k}$, which, on points of C^0, is given by:

$$\langle a\rangle(E,\alpha) = (E, a\alpha) \tag{1.2.6}$$

for each $a \in (\boldsymbol{Z}/N\boldsymbol{Z})^\times$. For $f \in M_k(\Gamma_1(N);\mathfrak{k})$, we have

$$(f|\langle a\rangle)(E,\alpha) := f(\langle a\rangle(E,\alpha)) = f(E,a\alpha). \tag{1.2.7}$$

If l is a prime number different from p, then we have:

$$(f|T(l))(E,\alpha) = \frac{1}{l}\sum_{\varphi} \varphi^*(f(E', \varphi\circ\alpha)). \tag{1.2.8}$$

Here, the sum runs over $l+1$ isogenies $\varphi : E \to E'$ of degree l when $l \nmid N$; and over l isogenies φ as above such that $\varphi\circ\alpha$ is injective when $l \mid N$ (cf. 1.6 below for $T(n)$).

The same formulas as (1.2.7) and (1.2.8) define operators on $SS_k(\Gamma_1(N);\mathfrak{k})$, which we denote by the same symbols. (But it is not clear how to define $T(p)$ on this space.) The natural mapping $i_k : M_k(\Gamma_1(N);\mathfrak{k}) \to SS_k(\Gamma_1(N);\mathfrak{k})$ clearly commutes with $\langle a\rangle$ and $T(l)$ $(l \neq p)$.

The injection $\times A : M_{k-p+1}(\Gamma_1(N);\mathfrak{k}) \to M_k(\Gamma_1(N);\mathfrak{k})$ commutes with $\langle a\rangle$ and $T(n)$ for all n, provided that $k-p+1 \geq 2$. When $k-p+1=1$, this mapping commutes with $\langle a\rangle$ and $T(l)$ $(l \neq p)$, but *does not* commute with $T(p)$ (cf. [**Gr**, Proposition 4.1] for the description of $T(p)$ of weight one; cf. also (3.1.2) below).

1.3. Ulmer's pairing between modular forms on supersingular elliptic curves.

The purpose of this subsection is to recall Ulmer's results from [**U1**, Section 7]. First, let E_{p+1} be the classical Eisenstein series of weight $p+1$ and level one (normalized so that its constant term of the q-expansion is one), and set

$$B := -\frac{1}{12}E_{p+1} \pmod p \in M_{p+1}(\Gamma_1(1);\boldsymbol{F}_p). \tag{1.3.1}$$

Let k and k' be non-negative integers satisfying $k+k' = p+1$. Ulmer considered the pairing

$$\langle\ ,\ \rangle : SS_{k'}(\Gamma_1(N);\mathfrak{k}) \times SS_k(\Gamma_1(N);\mathfrak{k}) \to \mathfrak{k} \tag{1.3.2}$$

defined by the formula

$$\langle f, g\rangle := \sum_{(E,\alpha)} \frac{f(E,\alpha)g(E,\alpha)}{B(E,\alpha)} \tag{1.3.3}$$

where the sum runs over all supersingular geometric points of C (with values in a fixed algebraic closure of $\mathfrak{k}$).

Since B does not vanish at supersingular points, the formula above makes sense,

and it is easy to see that the value above in fact belongs to $\mathfrak{k}$. This pairing is clearly non-degenerate.

Let $X := I_1(N)_{/\mathfrak{k}}$ be the Igusa curve of level Np over $\mathfrak{k}$, and denote by the same symbol $\underline{\omega}$ the pull-back of the previous $\underline{\omega}$ by the natural morphism: $X \to C$. Then there is a canonical section $a \in H^0(X, \underline{\omega})$ as defined in [**Gr**, Proposition 5.2]. For $h \in M_m(\Gamma_1(N); \mathfrak{k}) = H^0(C, \underline{\omega}^{\otimes m})$ $(m \geq 0)$, we can associate a rational function $\underline{h} := h/a^m$ on X.

For $f \in M_{k'}(\Gamma_1(N); \mathfrak{k})$ and $g \in M_k(\Gamma_1(N); \mathfrak{k})$, we can define $\langle f, g \rangle$ by the same formula as above, which is equal to $\langle i_{k'}(f), i_k(g) \rangle$. Since the morphism: $X \to C$ ramifies totally at supersingular points, it may be rewritten as:

$$\langle f, g \rangle = \sum_{x:\text{supersingular}} \frac{\underline{f} \cdot \underline{g}}{\underline{B}}(x) \tag{1.3.4}$$

the sum running over all supersingular geometric points of X. On the other hand, there is a canonical differential, denoted dq/q, on X whose divisor satisfies $(dq/q) = p\sum_{x:\text{supersingular}}(x) - \sum_{v:\text{cuspidal}}(v)$ (cf. [**Gr**, p. 463], [**U1**, p. 254]). Later, we will need the following results due to Ulmer:

PROPOSITION 1.3.5. *For $f \in M_{k'}(\Gamma_1(N); \mathfrak{k})$ and $g \in M_k(\Gamma_1(N); \mathfrak{k})$, we have*

$$\langle f, g \rangle = \sum_{x:\text{supersingular}} \mathrm{Res}_x\left(\underline{f} \cdot \underline{g}\frac{dq}{q}\right).$$

PROOF. This follows from (1.3.4) and the fact that the differential $\underline{B}dq/q$ has a simple pole with residue one at each supersingular point (Ulmer [**U2**, Lemma 3.4]). □

COROLLARY 1.3.6. *Under the pairing* (1.3.2)*, the exact annihilator of the image of $S_k(\Gamma_1(N); \mathfrak{k})$ in $SS_k(\Gamma_1(N); \mathfrak{k})$ is the image of $M_{k'}(\Gamma_1(N); \mathfrak{k})$ in $SS_{k'}(\Gamma_1(N); \mathfrak{k})$.*

PROOF. If $f \in M_{k'}(\Gamma_1(N); \mathfrak{k})$ (resp. $g \in S_k(\Gamma_1(N); \mathfrak{k})$), $\underline{f}$ (resp. $\underline{g}$) has poles of order at most k' (resp. k) at supersingular points, and is holomorphic elsewhere. Since $\underline{g}$ vanishes at cusps, it follows from the proposition that $\langle f, g \rangle = 0$, by the residue formula. It is therefore enough to show that the sum of the dimensions of the images of $M_{k'}(\Gamma_1(N); \mathfrak{k}) \to SS_{k'}(\Gamma_1(N); \mathfrak{k})$ and $S_k(\Gamma_1(N); \mathfrak{k}) \to SS_k(\Gamma_1(N); \mathfrak{k})$ is equal to $\dim_{\mathfrak{k}} SS_{k'}(\Gamma_1(N); \mathfrak{k})$, which follows from (1.2.5). □

1.4. Twisted pairing $\langle\ ,\ \rangle^*$.

We continue to assume that $N \geq 5$, and fix a finite field $\mathfrak{k}$ of characteristic p. We moreover assume that $\mathfrak{k}$ contains a primitive N-th root ζ_N of unity, and fix this ζ_N. Then we can define an automorphism w_N of C over $\mathfrak{k}$ by the following rule on points of C^0:

$$\begin{cases} w_N(E, \alpha) = (E^*, \alpha^*) \text{ where} \\ E^* := E/\alpha(\boldsymbol{\mu}_N) \text{ with the quotient morphism } \phi : E \to E^*; \\ \alpha^*(\zeta_N) := \phi(t_\alpha) \text{ with } t_\alpha \text{ a section of } E_N \text{ such that } e_{N,E}(\alpha(\zeta_N), t_\alpha) = \zeta_N. \end{cases} \tag{1.4.1}$$

Here $e_{N,E}(\ ,\ )$ is the Weil pairing on E_N. It is easy to see that $w_N^2 = \langle -1 \rangle$.

For $g \in SS_k(\Gamma_1(N); \mathfrak{k})$ (or $M_k(\Gamma_1(N); \mathfrak{k})$), we define $g|w_N \in SS_k(\Gamma_1(N); \mathfrak{k})$ (or $M_k(\Gamma_1(N); \mathfrak{k})$, respectively) by the formula:

$$(g|w_N)(E, \alpha) := \phi^*(g(E^*, \alpha^*)). \tag{1.4.2}$$

Clearly, the oparator " $|w_N$" induces automorphisms of the respective spaces; and it preserves $S_k(\Gamma_1(N); \mathfrak{k})$.

DEFINITION 1.4.3. Under the assumptions above, we define the twisted pairing

$$\langle\ ,\ \rangle^* : SS_{k'}(\Gamma_1(N); \mathfrak{k}) \times SS_k(\Gamma_1(N); \mathfrak{k}) \to \mathfrak{k}$$

by the formula:

$$\langle f, g \rangle^* := \langle f, g|w_N \rangle.$$

We are now going to look at the behavior of $\langle a \rangle$ and $T(l)$ with respect to this pairing. First, we have:

$$\langle f|\langle a \rangle, g \rangle^* = \langle f, g|\langle a \rangle \rangle^*. \tag{1.4.4}$$

In fact, since B is a modular form of level one, the value $B(E, \alpha)$ is independent of α, and we have

$$\langle f|\langle a \rangle, g \rangle^* = \sum_{(E,\alpha)} \frac{f(E, \alpha)(g|w_N)(E, a^{-1}\alpha)}{B(E, \alpha)}.$$

Our claim follows from this and the relation $w_N \circ \langle a \rangle^{-1} = \langle a \rangle \circ w_N$ (cf. [**O4**, (2.4.6)] where we treated the Igusa curve case).

PROPOSITION 1.4.5. *Let l be a prime number different from p. Then the twisted pairing above satisfies*:

$$\langle f|T(l), g \rangle^* = l^{k'-1} \langle f, g|T(l) \rangle^*.$$

PROOF. To prove our proposition, let us consider the oriented graph G whose vertices consist of supersingular geometric points (E, α)'s of C, and whose edges consist of isogenies $\varphi : (E, \alpha) \to (E', \alpha')$ (i.e. isogenies $\varphi : E \to E'$ such that $\varphi \circ \alpha = \alpha'$) of degree l. Call $e(G)$ the set of edges of G, and for each $\varphi \in e(G)$, denote by $i(\varphi)$ (resp. $t(\varphi)$) the initial vertex (resp. the terminal vertex) of φ. Clearly, every vertex is an initial vertex of some edge, and it is easy to see that every vertex is also a terminal vertex of some edge.

If $\varphi : E \to E'$ is an isogeny of degree l between supersingular elliptic curves, we have $\varphi^*(B(E')) = lB(E)$ by Robert [**R**, Théorème B]. Thus using the terminology above, we

have:

$$\langle f|T(l),g\rangle^* = \sum_{\varphi\in e(G)} \frac{\varphi^*(f(t(\varphi)))(g|w_N)(i(\varphi))}{\varphi^*(B(t(\varphi)))}.$$

For $\varphi \in e(G)$, let ${}^t\varphi$ be the isogeny dual to φ. Then since f (resp. B) is of weight k' (resp. $p+1$), the above sum is equal to:

$$\sum_{\varphi\in e(G)} \frac{l^{k'} f(t(\varphi)){}^t\varphi^*((g|w_N)(i(\varphi)))}{l^{p+1}B(t(\varphi))} = l^{-k} \sum_{(E',\alpha')} \sum_{\varphi:(E,\alpha)\to(E',\alpha')} \frac{f(E',\alpha'){}^t\varphi^*((g|w_N)(E,\alpha))}{B(E',\alpha')}$$

where the first sum in the right-hand side ranges over the vertices of G, and the second one over $\varphi \in e(G)$ such that $t(\varphi) = (E',\alpha')$.

Let $\varphi : (E,\alpha) \to (E',\alpha')$ be an edge of G. Set $w_N(E,\alpha) = (E^*,\alpha^*)$ and $w_N(E',\alpha') = (E'^*,\alpha'^*)$ with $\phi : E \to E^*$ and $\phi' : E' \to E'^*$ the quotient morphisms, respectively. Then $\mathrm{Ker}(\phi') = \varphi\circ\alpha(\boldsymbol{\mu}_N)$ is annihilated by $\phi\circ{}^t\varphi$, and there is a unique isogeny $\varphi^\star : E'^* \to E^*$ of degree l such that $\phi\circ{}^t\varphi = \varphi^\star\circ\phi'$. Let t_α (resp. $t_{\alpha'}$) be a point of E_N (resp. E'_N) as in (1.4.1). We have

$$\zeta_N = e_{N,E'}(\alpha'(\zeta_N), t_{\alpha'}) = e_{N,E}(\alpha(\zeta_N), {}^t\varphi(t_{\alpha'}))$$

and $\varphi^\star\circ\alpha'^*(\zeta_N) = \phi\circ{}^t\varphi(t_{\alpha'})$. We may therefore take ${}^t\varphi(t_{\alpha'})$ for t_α, and hence we have $\varphi^\star\circ\alpha'^* = \alpha^*$, i.e. $\varphi^\star : (E'^*,\alpha'^*) \to (E^*,\alpha^*)$ gives an edge of G. If we start with this isogeny and apply the above construction once again, we easily see that the isogeny $(\varphi^\star)^\star$ from $w_N^2(E,\alpha) = \langle -1\rangle(E,\alpha)$ to $w_N^2(E',\alpha') = \langle -1\rangle(E',\alpha')$ is given by φ.

Now w_N induces a bijection from the set of vertices of G to itself. The argument above shows that this, together with the correspondence $\varphi \mapsto \varphi^\star$, gives an orientation-reversing automorphism of G. It therefore follows that the sum

$$\sum_{\varphi:(E,\alpha)\to(E',\alpha')} {}^t\varphi^*((g|w_N)(E,\alpha))$$

over $\varphi \in e(G)$ such that $t(\varphi) = (E',\alpha')$ is equal to the sum

$$\sum_{\varphi^\star:(E'^*,\alpha'^*)\to(E^*,\alpha^*)} \phi'^*\circ(\varphi^\star)^*(g(E^*,\alpha^*))$$

over $\varphi^\star \in e(G)$ such that $i(\varphi^\star) = (E'^*,\alpha'^*)$. This is equal to $l(g|T(l)|w_N)(E',\alpha')$, and our conclusion follows. □

1.5. Pairing $[\ ,\ ]_k$ on modular forms over finite fields.

Recall that the modular form B does not vanish at supersingular points, and hence multiplication by it induces an isomorphism

$$\times B : SS_k(\Gamma_1(N);\mathfrak{k}) \xrightarrow{\sim} SS_{k+p+1}(\Gamma_1(N);\mathfrak{k}) \tag{1.5.1}$$

for eack k. Since B is of level one, we have:

$$\langle a\rangle \circ (\times B) = (\times B) \circ \langle a\rangle. \tag{1.5.2}$$

From the result of Robert cited in the previous subsection, we have:

$$T(l) \circ (\times B) = l(\times B) \circ T(l). \tag{1.5.3}$$

Let θ be the operator of Serre and Katz acting on modular forms over finite fields whose effect on q-expansions is given by $q(d/dq)$. We have the following relations:

$$\begin{cases} \langle a\rangle \circ \theta = \theta \circ \langle a\rangle; \\ T(l) \circ \theta = l\theta \circ T(l). \end{cases} \tag{1.5.4}$$

In general, for a modular form f over a finite field, we denote by $w(f)$ its filtration (cf. [**Gr**, Section 4]; we set $w(0) := -\infty$). We will frequently use the following fact:

PROPOSITION 1.5.5 (cf. [**Gr**, Proposition 4.10]). *Let f have filtration $k \geq 0$.*

i) *If $(k,p) = 1$, then $w(\theta f) = k + p + 1$.*

ii) *Set $k' := p + 1 - k$. If $2 \leq k \leq p$, then $w(\theta^{k'} f) \leq k' + p + 1$. Here, the equality holds if and only if $f|T(p) \neq 0$ and $w(f|T(p)) = k$.*

See [**Gr**], loc. cit. for the proof. We remark that, in the second assertion, the condition $w(f|T(p)) = k$ follows automatically from the non-vanishing of $f|T(p)$ when $2 \leq k \leq p-2$; but this is not true when $k = p-1$ or p for non-eigenforms. For $k = p-1$, if g is a form of filtration $p-1$ satisfying $g|T(p) = 0$, then $f = g + A$ has filtration $p-1$, but $w(f|T(p)) = 0$. On the other hand, when $k = p$, let g be a form of filtration one, and set $f = g|V_p$ with V_p the usual "Frobenius operator", whose effect on q-expansions is given by: $\sum_{n=0}^{\infty} a_n q^n \mapsto \sum_{n=0}^{\infty} a_n q^{pn}$. We have $w(f) = p$, but $w(f|T(p)) = w(g) = 1$ in which case $\theta f = 0$.

Recall that, according to our convention in 1.2, we identify $f \in M_{k-p+1}(\Gamma_1(N);\mathfrak{k})$ with $Af \in M_k(\Gamma_1(N);\mathfrak{k})$.

DEFINITION 1.5.6. Assume that $\mathfrak{k}$ contains a primitive N-th root of unity. For $2 \leq k \leq p$, set $k' = p + 1 - k$. Let $i_k : M_k(\Gamma_1(N);\mathfrak{k}) \to SS_k(\Gamma_1(N);\mathfrak{k})$ be the mapping deduced from (1.2.2), and $j_k : M_k(\Gamma_1(N);\mathfrak{k}) \to SS_{k'}(\Gamma_1(N);\mathfrak{k})$ the composite of: $M_k(\Gamma_1(N);\mathfrak{k}) \xrightarrow{\theta^{k'}} M_{k'+p+1}(\Gamma_1(N);\mathfrak{k}) \xrightarrow{i_{k'+p+1}} SS_{k'+p+1}(\Gamma_1(N);\mathfrak{k}) \xrightarrow{(\times B)^{-1}} SS_{k'}(\Gamma_1(N);\mathfrak{k})$. Using the pairing in 1.4.3, we define

$$[\ ,\ ]_k : M_k(\Gamma_1(N);\mathfrak{k}) \times M_k(\Gamma_1(N);\mathfrak{k}) \to \mathfrak{k}$$

by the formula $[f,g]_k := \langle j_k(f), i_k(g)\rangle^*$.

PROPOSITION 1.5.7. *The pairing above satisfies*

$$\begin{cases} [f|\langle a\rangle, g]_k = [f, g|\langle a\rangle]_k; \text{ and} \\ [f|T(l), g]_k = [f, g|T(l)]_k \text{ for all prime numbers } l \neq p. \end{cases}$$

PROOF. This follows from (1.4.4), Proposition 1.4.5, (1.5.2), (1.5.3) and (1.5.4). □

PROPOSITION 1.5.8. *Assume that* $2 \leq k \leq p$, *and consider the pairing*

$$[\ ,\ ]_k : M_k(\Gamma_1(N);\mathfrak{k}) \times S_k(\Gamma_1(N);\mathfrak{k}) \to \mathfrak{k}.$$

Its left kernel consists of the forms $f \in M_k(\Gamma_1(N);\mathfrak{k})$ *satisfying*: $\theta^{k'} f - \theta g \in M_{k'+2}(\Gamma_1(N);\mathfrak{k})$ *with some* $g \in M_{k'}(\Gamma_1(N);\mathfrak{k})$.

PROOF. First note that $M_{k'+p+1}(\Gamma_1(N);\mathfrak{k})/M_{k'+2}(\Gamma_1(N);\mathfrak{k}) \xrightarrow{\sim} SS_{k'+p+1}(\Gamma_1(N);\mathfrak{k})$ by (1.2.5). We see from Corollary 1.3.6 that f belongs to the left kernel if and only if $\theta^{k'} f - Bg' \in M_{k'+2}(\Gamma_1(N);\mathfrak{k})$ for some $g' \in M_{k'}(\Gamma_1(N);\mathfrak{k})$. But for $h \in M_{k'}(\Gamma_1(N);\mathfrak{k})$, we have $\theta h = A\partial h - k'Bh$ with $\partial h \in M_{k'+2}(\Gamma_1(N);\mathfrak{k})$ (cf. Katz [**Ka2**, III]). Our assertion follows from this. □

We remark that in general the pairing above has larger left kernel than Ulmer's pairing $(\ ,\ )_k$ (or its twisted version $(\ ,\ )_k^*$) considered in [**O4**], whose left kernel consists precisely of the forms with companions. In fact, if $f \in M_k(\Gamma_1(N);\mathfrak{k})$ satisfies $f|T(p) = 0$, then $w(\theta^{k'} f) \leq k' + 2$ by Proposition 1.5.5, and hence $j_k(f) = 0$. But such a form cannot have a companion, since $\theta^{k'} f = \theta g$ with $g \in M_{k'}(\Gamma_1(N);\mathfrak{k})$ implies that $w(\theta^{k'} f) = k' + p + 1$. In the next subsection, however, we will see that our new pairing $[\ ,\ ]_k$ has as good property as Ulmer's one on ordinary components.

1.6. Ordinary components.

We denote by $H_k(\Gamma_1(N);\mathfrak{k})$ (resp. $h_k(\Gamma_1(N);\mathfrak{k})$) the Hecke algebra attached to $M_k(\Gamma_1(N);\mathfrak{k})$ (resp. $S_k(\Gamma_1(N);\mathfrak{k})$); i.e. it is the $\mathfrak{k}$-subalgebra of $\mathrm{End}_{\mathfrak{k}}(M_k(\Gamma_1(N);\mathfrak{k}))$ (resp. $\mathrm{End}_{\mathfrak{k}}(S_k(\Gamma_1(N);\mathfrak{k}))$) generated by all $\langle a\rangle$ and $T(l)$ with prime numbers l including $l = p$. We denote by $H_k^{(p)}(\Gamma_1(N);\mathfrak{k})$ its $\mathfrak{k}$-subalgebra generated by $\langle a\rangle$ and $T(l)$ with $l \neq p$. We first note the following fact.

LEMMA 1.6.1. *We have* $H_k(\Gamma_1(N);\mathfrak{k}) = H_k^{(p)}(\Gamma_1(N);\mathfrak{k})$ *for* $1 \leq k \leq p-2$.

PROOF. When $2 \leq k \leq p-2$, this is [**O4**, Lemma 2.5.4]. The proof in the case where $k = 1$ is similar. (But remember that we are employing the definition of Katz, and $M_1(\Gamma_1(N);\mathfrak{k})$ may contain elements that are not liftable to forms of weight one in characteristic zero.) Since we need the argument of the proof later, we outline it.

In general, we can define the Hecke operators $T(n)$ on $M_k(\Gamma_1(N);\mathfrak{k})$ for positive integers n by the usual formulas:

$$\begin{cases} T(l^{e+1}) = T(l)T(l^e) - l^{k-1}\langle l\rangle T(l^{e-1}) \text{ for prime numbers } l \nmid N; \\ T(l^e) = T(l)^e \text{ for prime numbers } l \mid N; \\ T(n) = \prod_i T(l_i^{e_i}) \text{ if } n = \prod_i l_i^{e_i} \text{ is the prime decomposition.} \end{cases}$$

Clearly, $H_k(\Gamma_1(N);\mathfrak{k})$ is generated over $\mathfrak{k}$ by all $T(n)$. For $f \in M_k(\Gamma_1(N);\mathfrak{k})$, let $a(m;f)$ be the coefficient of q^m of the q-expansion of f. Then one can prove, without difficulty, that $a(1;f|T(n)) = a(n;f)$.

Consider the pairing:

$$M_k(\Gamma_1(N);\mathfrak{k}) \times H_k(\Gamma_1(N);\mathfrak{k}) \to \mathfrak{k}$$

defined by $(f,t) = a(1;f|t)$. The fact above shows that the left kernel of this pairing consists of (the forms whose q-expansions are) constants. When $1 \le k \le p-2$, it reduces to $\{0\}$, and it follows from a standard argument that this pairing is perfect.

It is therefore enough to show that the mapping:

$$M_k(\Gamma_1(N);\mathfrak{k}) \to \mathrm{Hom}_{\mathfrak{k}}(H_k^{(p)}(\Gamma_1(N);\mathfrak{k}),\mathfrak{k})$$

sending f to the mapping $t \mapsto a(1;f|t)$ is injective. Its kernel consists of the forms whose q-expansions are power series in q^p. By [**Ka2**, II, Corollary (5)], these are the images of V_p, and hence the kernel reduces to $\{0\}$ when $1 \le k \le p-2$. □

The algebra $H_k(\Gamma_1(N);\mathfrak{k})$ is finite over $\mathfrak{k}$, and it can be decomposed as a direct sum

$$H_k(\Gamma_1(N);\mathfrak{k}) = \oplus_{\mathfrak{n}} H_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}} \tag{1.6.2}$$

of localizations at maximal ideals. For each $\mathfrak{n}$, $\mathfrak{n}^{(p)} := \mathfrak{n} \cap H_k^{(p)}(\Gamma_1(N);\mathfrak{k})$ is a maximal ideal of $H_k^{(p)}(\Gamma_1(N);\mathfrak{k})$. For any $H_k(\Gamma_1(N);\mathfrak{k})$-module M, we write $M_{\mathfrak{n}^{(p)}}$ for the localization at $\mathfrak{n}^{(p)}$ of M viewed as an $H_k^{(p)}(\Gamma_1(N);\mathfrak{k})$-module. Equivalently, we have $M_{\mathfrak{n}^{(p)}} = M \otimes_{H_k(\Gamma_1(N);\mathfrak{k})} H_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$.

As for the Hecke algebras of weight $k = p-1$ and p, the following holds:

LEMMA 1.6.3. *Assume that* $M_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \cap \mathfrak{k}A = \{0\}$ (*resp.* $M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \cap V_pM_1(\Gamma_1(N);\mathfrak{k}) = \{0\}$). *Then we have* $H_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} = H_{p-1}^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$ (*resp.* $H_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} = H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$).

PROOF. Apply the same argument as in the proof of Lemma 1.6.1 to the pairing

$$M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \times H_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \to \mathfrak{k}$$

for $k = p-1$ and p. □

We now consider the pairings

$$\begin{cases} [\ ,\ ]_{k,\mathfrak{n}} : M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}} \times M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}} \to \mathfrak{k}, \\ [\ ,\ ]_{k,\mathfrak{n}^{(p)}} : M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \times M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \to \mathfrak{k} \end{cases} \tag{1.6.4}$$

induced from the one constructed in the previous subsection. Note that these pairings are the same things when $2 \le k \le p-2$, by Lemma 1.6.1.

THEOREM 1.6.5. *Suppose that $2 \le k \le p$, and $\mathfrak{k}$ contains a primitive N-th root of unity. Let $\mathfrak{n}$ be a maximal ideal of $H_k(\Gamma_1(N);\mathfrak{k})$. We assume that $T(p)$ is a unit in the ring $H_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$, and moreover that the assumption in the previous lemma is satisfied when $k = p-1$. Then the left kernel of the pairing*

$$[\ ,\ ]_{k,\mathfrak{n}^{(p)}} : M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \times S_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \to \mathfrak{k}$$

consists of the forms with companions; i.e. it is $\{ f \in M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \mid \theta^{k'} f = \theta g$ with some $g \in M_{k'}(\Gamma_1(N);\mathfrak{k})\}$.

PROOF. We first show that, when $2 \le k \le p-1$, $i_{k'+p+1} \circ \theta^{k'} : M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \to SS_{k'+p+1}(\Gamma_1(N);\mathfrak{k}) \cong M_{k'+p+1}(\Gamma_1(N);\mathfrak{k})/M_{k'+2}(\Gamma_1(N);\mathfrak{k})$ is injective; or equivalently, that $w(\theta^{k'} f) = k' + p + 1$ for any non-zero $f \in M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$. Indeed, if $2 \le k \le p-2$, this immediately follows from Proposition 1.5.5, ii), since $T(p)$ induces an automorphism of $M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$. If $k = p-1$, the kernel of $i_{p+3} \circ \theta^2$ consists of those $f \in M_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$ such that $w(f|T(p)) \le 0$, by Proposition 1.5.5, ii). Again, since $T(p)$ induces an automorphism of $M_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$, our assumption implies that such an f must be zero. This proves our claim.

Now to prove the theorem, we may replace $\mathfrak{k}$ by its finite extension, since the base extension of the pairing above to such an extension is a direct sum of similar pairings. We may therefore assume that $H_k(\Gamma_1(N);\mathfrak{k})/\mathfrak{n} = \mathfrak{k}$. Let $\alpha(n)$ (resp. $\delta(a)$) be the image of $T(n)$ (resp. $\langle a \rangle$) to this residue field, and set $\eta(l) := T(l) - \alpha(l)$ for prime numbers $l \ne p$, and $\xi(a) := \langle a \rangle - \delta(a)$, both belonging to $\mathfrak{n}^{(p)}$. Any element of $M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$ is annihilated by sufficiently high powers of these elements. If we set $\eta_c(l) := l^{-c}T(l) - \alpha(l)$, then it follows from (1.5.4) that $\theta^c \circ \eta(l) = \eta_c(l) \circ \theta^c$ and $\theta^c \circ \xi(a) = \xi(a) \circ \theta^c$.

Assume that a non-zero $f \in M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$ belongs to the left kernel of the pairing in question. If $f' \in M_k(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}'^{(p)}}$ with a maximal ideal $\mathfrak{n}'^{(p)}$ of $H_k^{(p)}(\Gamma_1(N);\mathfrak{k})$ different from $\mathfrak{n}^{(p)}$, it follows from Proposition 1.5.7 that $[f, f']_k = 0$, i.e. f belongs to the left kernel of the pairing $[\ ,\ ]_k : M_k(\Gamma_1(N);\mathfrak{k}) \times S_k(\Gamma_1(N);\mathfrak{k}) \to \mathfrak{k}$. Thus there are $g \in M_{k'}(\Gamma_1(N);\mathfrak{k})$ and $h \in M_{k'+2}(\Gamma_1(N);\mathfrak{k})$ such that $\theta^{k'} f = \theta g + h$ by Proposition 1.5.8, and our goal will be to show that $h = 0$. For this, we first see from the remarks above that $\theta(\eta_{k'-1}(l)^m g)$ and $\theta(\xi(a)^m g)$ belong to $M_{k'+2}(\Gamma_1(N);\mathfrak{k})$ for m sufficiently large. But since $1 \le k' \le p-1$, Proposition 1.5.5, i) implies that these elements cannnot belong to $M_{k'+2}(\Gamma_1(N);\mathfrak{k})$ unless they vanish. This in turn implies that h is annihilated by sufficiently high powers of $\eta_{k'}(l)$ and $\xi(a)$.

We now prove the theorem when $2 \le k \le p-1$. To do this, let us consider the maximal ideal $\mathfrak{n}_1^{(p)}$ of $H_{k'+p+1}^{(p)}(\Gamma_1(N);\mathfrak{k})$ generated by $\eta_{k'}(l)$ and $\xi(a)$. There is an integer $t \ge 1$ such that $\mathfrak{n}_1^{(p)t}\theta^{k'} f = \{0\}$ but $\mathfrak{n}_1^{(p)t-1}\theta^{k'} f \ne \{0\}$. Thus there is an $\alpha \in \mathfrak{n}_1^{(p)t-1}$ such that

$\alpha\theta^{k'}f$ is a non-zero element annihilated by $\mathfrak{n}_1^{(p)}$. We see from (1.5.4) that there is an $\alpha' \in H_k^{(p)}(\Gamma_1(N);\mathfrak{k})$ satisfying $\alpha\theta^{k'}f = \theta^{k'}\alpha' f$. It follows that the constant term of the q-expansion of $\alpha\theta^{k'}f$ is zero, and also that this element is annihilated by $T(p)$. Especially, it is a common eigenform of all $T(n)$. If we denote by $b(n)$ the corresponding eigenvalues, the q-expansion of $\alpha\theta^{k'}f$ is of the form $c\sum_{n=1}^{\infty} b(n)q^n$ with some $c \in \mathfrak{k}^\times$. From the first part of the proof, this form has filtration $k' + p + 1$.

On the other hand, assume that $h \neq 0$. We have seen that it is annihilated by sufficiently high powers of $\mathfrak{n}_1^{(p)}$. It, being an image of θ, is also annihilated by $T(p)$. We can argue in the same way as above to conculde that there is a $\beta \in H_{k'+2}^{(p)}(\Gamma_1(N);\mathfrak{k})$ such that βh has q-expansion of the form $d\sum_{n=1}^{\infty} b(n)q^n$ with $d \in \mathfrak{k}^\times$. Since $w(\beta h) \leq k' + 2$, this is a contradiction.

Finally, we consider the case where $k = p$. Let f, g and h be as above. The argument above shows that $g \in M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$. Therefore, $f_0 := f - g$ belongs to $M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$, and it satisfies $\theta f_0 = h \in M_3(\Gamma_1(N);\mathfrak{k})$. If $w(f_0) \leq 1$, one easily concludes that $h = 0$; and hence we assume that $w(f_0) = p$. Then $f_0|T(p) \neq 0$, but we have $w(f_0|T(p)) = 1$ by Proposition 1.5.5, ii). Consider the subspace

$$\left\{ f' \in M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \mid w(f'|T(p)) \leq 1 \right\}$$

of $M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$. It clearly contains

$$M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \cap V_p M_1(\Gamma_1(N);\mathfrak{k}) = V_p(M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}})$$

and is mapped isomorphically onto

$$M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}} \cap M_1(\Gamma_1(N);\mathfrak{k}) = M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}^{(p)}}$$

by $T(p)$. Since these two spaces have the same dimension, we conclude that f_0 lies in the image of V_p, and hence $\theta f_0 = 0$. □

1.7. Lower level case.

So far, we discussed under the assumption $N \geq 5$. In this subsection, we treat the remaining case where $N \leq 4$, which is in fact routine.

We take and fix an integer $n \geq 3$ prime to Np. Let Y_n be the (not necessarily connected) modular curve over $\mathfrak{k}$ classifying triples (E, α, β) with (E, α) as in (1.1.1), together with a full level n structure $\beta : \boldsymbol{Z}/n\boldsymbol{Z} \times \boldsymbol{Z}/n\boldsymbol{Z} \xrightarrow{\sim} E_n$, over $\mathfrak{k}$-schemes. We denote by X_n the smooth compactification of Y_n.

The group $G_n := GL_2(\boldsymbol{Z}/n\boldsymbol{Z})$ acts on Y_n in a natural manner; i.e. $g \in G_n$ sends (E, α, β) to $(E, \alpha, \beta \circ g)$.

In the following, we assume that no prime factor of n is congruent to ± 1 modulo p, so that the order of G_n is prime to p. Then the correspondence $M \mapsto M^{G_n}$ (the invariants under G_n) gives an exact functor from the category of $\mathfrak{k}[G_n]$-modules to that of $\mathfrak{k}$-vector spaces. We also note the following elementary fact: Let V and W be finite dimensional $\mathfrak{k}$-vector spaces on which G_n acts $\mathfrak{k}$-linearly. If

$$\langle\ ,\ \rangle : V \times W \to \mathfrak{k}$$

is a non-degenerate $\mathfrak{k}$-bilinear pairing satisfying $\langle gv, gw\rangle = \langle v, w\rangle$, its restriction to $V^{G_n} \times W^{G_n}$ is non-degenarate.

Now we have the invertible sheaf $\underline{\omega}$ on X_n, and also the spaces $M_k(\Gamma_1(N) \cap \Gamma(n); \mathfrak{k}) = H^0(X_n, \underline{\omega}^{\otimes k})$ and $S_k(\Gamma_1(N) \cap \Gamma(n); \mathfrak{k}) = H^0(X_n, \underline{\omega}^{\otimes k}(-\text{cusps}))$ as in 1.1. The group G_n acts on these spaces via the pull-back of sections: $g^* f(E, \alpha, \beta) = f(E, \alpha, \beta \circ g)$. We have $M_k(\Gamma_1(N) \cap \Gamma(n); \mathfrak{k})^{G_n} = M_k(\Gamma_1(N); \mathfrak{k})$ and $S_k(\Gamma_1(N) \cap \Gamma(n); \mathfrak{k})^{G_n} = S_k(\Gamma_1(N); \mathfrak{k})$ (cf. Edixhoven [**E**, 2.1]).

We have the exact sequence (1.2.2) on X_n, and hence the space $SS_k(\Gamma_1(N) \cap \Gamma(n); \mathfrak{k}) = H^0(X_n, \underline{SS}_k)$ on which G_n acts. We set

$$SS_k(\Gamma_1(N); \mathfrak{k}) := SS_k(\Gamma_1(N) \cap \Gamma(n); \mathfrak{k})^{G_n}. \tag{1.7.1}$$

This space does not depend on the choice of auxiliary level n, up to canonical isomorphisms. We may in fact identify $f \in SS_k(\Gamma_1(N); \mathfrak{k})$ with a "rule" on supersingular (E, α) over extension fields of $\mathfrak{k}$ as in 1.2. This description also allows us to define $f|\langle a\rangle$ and $f|T(l)$ by (1.2.7) and (1.2.8), respectively.

Since the Kodaira-Spencer isomorphism (1.1.6) on X_n and the Serre duality pairing are functorial, we see that $H^1(X_n, \underline{\omega}^{\otimes m})^{G_n} \cong S_{2-m}(\Gamma_1(N); \mathfrak{k})^\vee$. Thus taking G_n-invariants from the long exact sequence deduced from (1.2.2) on X_n, we have the same exact sequences as in (1.2.5) for $N \leq 4$ also.

For non-negative integers k and k' such that $k + k' = p + 1$, we can define

$$\langle\ ,\ \rangle_n : SS_{k'}(\Gamma_1(N) \cap \Gamma(n); \mathfrak{k}) \times SS_k(\Gamma_1(N) \cap \Gamma(n); \mathfrak{k}) \to \mathfrak{k} \tag{1.7.2}$$

by the same formula as (1.3.3), the sum being over the supersingular geometric points of the $\mathfrak{k}$-scheme X_n. It is clear that this pairing satisfies $\langle g^* f, g^* h\rangle_n = \langle f, h\rangle_n$ for any $g \in G_n$. Thus its restriction, multiplied by $\deg(X_n / X_1(N)_{/\mathfrak{k}})^{-1}$, gives us a non-degenerate pairing

$$\langle\ ,\ \rangle : SS_{k'}(\Gamma_1(N); \mathfrak{k}) \times SS_k(\Gamma_1(N); \mathfrak{k}) \to \mathfrak{k}. \tag{1.7.3}$$

This pairing is independent of n, and enjoys the property stated in Corollary 1.3.6, for the same reason.

From now on, we assume that $\mathfrak{k}$ contains a primitive N-th root of unity. We define an automorphism $w_N^{(n)}$ of X_n by $w_N^{(n)}(E, \alpha, \beta) := (E^*, \alpha^*, \beta^*)$, where E^* and α^* are as in (1.4.1) and $\beta^* := \phi \circ \beta$. It commutes with the action of G_n, and induces w_N on $X_n/G_n = X_1(N)_{/\mathfrak{k}}$, defined by (1.4.1) for this coarse moduli scheme. We then obtain automorphisms "$|w_N^{(n)}$" and "$|w_N$" of $SS_k(\Gamma_1(N) \cap \Gamma(n); \mathfrak{k})$ and $SS_k(\Gamma_1(N); \mathfrak{k})$ as (1.4.2). Using these operators, we define the twisted pairings

$$\begin{cases} \langle\ ,\ \rangle_n^* : SS_{k'}(\Gamma_1(N) \cap \Gamma(n); \mathfrak{k}) \times SS_k(\Gamma_1(N) \cap \Gamma(n); \mathfrak{k}) \to \mathfrak{k}, \text{ and} \\ \langle\ ,\ \rangle^* : SS_{k'}(\Gamma_1(N); \mathfrak{k}) \times SS_k(\Gamma_1(N); \mathfrak{k}) \to \mathfrak{k} \end{cases} \tag{1.7.4}$$

by $\langle f,h\rangle_n^* := \langle f,h|w_N^{(n)}\rangle$ and $\langle f,h\rangle^* := \langle f,h|w_N\rangle$, respectively. Clearly, the restriction of the former pairing to $SS_{k'}(\Gamma_1(N);\mathfrak{k}) \times SS_k(\Gamma_1(N);\mathfrak{k})$ is a non-zero constant multiple of the latter.

For an integer a (resp. b) prime to N (resp. n), we denote by $\langle a\rangle_N$ (resp. $\langle b\rangle_n$) the automorphism of X_n given by $\langle a\rangle_N(E,\alpha,\beta) := (E,a\alpha,\beta)$ (resp. $\langle b\rangle_n(E,\alpha,\beta) := (E,\alpha,b\beta)$) on non-cuspidal points. Then for the same reason as (1.4.4) and Proposition 1.4.5, we have

$$\langle f|\langle a\rangle_N,h\rangle_n^* = \langle f,h|\langle a\rangle_N\rangle_n^*, \quad \text{and} \tag{1.7.5}$$

$$\langle f|T(l),h\rangle_n^* = l^{k'-1}\langle f,h|T(l)|\langle l\rangle_n^{-1}\rangle_n^* \tag{1.7.6}$$

for any prime number $l \nmid np$. Since there are infinitely many prime numbers $n \not\equiv \pm 1 \pmod p$, we conclude that (1.4.4) and Proposition 1.4.5 are valid for $N \le 4$.

With all these in mind, the arguments in 1.5 and 1.6 apply to the case where $N \le 4$ without change.

2. *p*-adic Hecke algebras of Eisenstein type when $d = 0$.

2.1. *p*-adic Hecke algebras.

We first review basic terminologies and results on p-adic Hecke algebras. For more details, the reader is referred to our previous work [**O4**], and the references cited there.

As in 1.1, we fix a prime number $p \ge 5$, and a positive integer N prime to p. We fix a finite extension F of $\boldsymbol{Q}_p$, with its ring of integers $\mathfrak{r}$. We denote by ϖ a prime element of F, and by $\mathfrak{k} := \mathfrak{r}/(\varpi)$ the residue field of F.

In the previous section, we have already introduced Hecke algebras over $\mathfrak{k}$. Similarly we let

$$\begin{cases} H_k(\Gamma_1(N);\mathfrak{r}) \subset \mathrm{End}_{\mathfrak{r}}(M_k(\Gamma_1(N);\mathfrak{r})), \\ h_k(\Gamma_1(N);\mathfrak{r}) \subset \mathrm{End}_{\mathfrak{r}}(S_k(\Gamma_1(N);\mathfrak{r})) \end{cases} \tag{2.1.1}$$

be the Hecke algebras over $\mathfrak{r}$; i.e. the left-hand side is the $\mathfrak{r}$-subalgebra of the right-hand side generated by all $T(l)$ with prime numbers l and the diamond operators $\langle a\rangle$, or equivalently by all $T(n)$ with positive integers n.

As for congruence subgroups of level divisible by p, explicitly for $\Gamma = \Gamma_1(Np)$ or $\Gamma_1(N)\cap\Gamma_0(p)$, we simply define $M_k(\Gamma;R)$ and $S_k(\Gamma;R)$ by the formula (1.1.4) with $\Gamma_1(N)$ replaced by Γ, and define Hecke algebras $H_k(\Gamma;R)$ and $h_k(\Gamma;R)$ acting on these spaces in the same way as above, for $R = \mathfrak{r}$ or $\mathfrak{k}$. (We will use these objects only for $k \ge 2$.)

On the other hand, let

$$\begin{cases} e\,\mathscr{H}(N;\mathfrak{r}), \\ e\,h(N;\mathfrak{r}) \end{cases} \tag{2.1.2}$$

be Hida's universal ordinary p-adic Hecke algebras of level N attached to modular forms and cusp forms, acting on the space of ordinary $\Lambda_{\mathfrak{r}}$-adic modular forms and the space of ordinary $\Lambda_{\mathfrak{r}}$-adic cusp forms of level N, respectively. These are algebras over the completed group algebra $\mathfrak{r}[[(\boldsymbol{Z}/Np\boldsymbol{Z})^{\times} \times (1+p\boldsymbol{Z}_p)]]$ and hence over the Iwasawa algebra $\Lambda_{\mathfrak{r}} := \mathfrak{r}[[1+p\boldsymbol{Z}_p]]$. As usual, we fix a topological generator γ of the multiplicative group $1+p\boldsymbol{Z}_p$, and use it to identify $\Lambda_{\mathfrak{r}}$ with the ring of formal power series $\mathfrak{r}[[T]]$ via $\gamma \leftrightarrow 1+T$. As $\Lambda_{\mathfrak{r}}$-algebras, $e\mathscr{H}(N;\mathfrak{r})$ and $e\,h(N;\mathfrak{r})$ are finite and flat.

Set

$$\omega_d := (1+T) - \gamma^d \in \Lambda_{\mathfrak{r}} \tag{2.1.3}$$

for a non-negative integer d. Then we have canonical isomorphisms via the specialization, sending $T(n)$ to $T(n)$:

$$\begin{cases} e\mathscr{H}(N;\mathfrak{r})/\omega_d \xrightarrow{\sim} e\,H_{d+2}(\Gamma_1(Np);\mathfrak{r}), \\ e\mathscr{H}(N;\mathfrak{r})^{(i)}/\omega_d \xrightarrow{\sim} e\,H_{d+2}(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r}) \text{ whenever } d \equiv i \bmod p-1 \end{cases} \tag{2.1.4}$$

and similarly for cuspidal Hecke algebras. Here and henceforth ω denotes the Teichmüller character, the superscript "(i)" indicates the ω^i-eigenspace with respect to the action of $(\boldsymbol{Z}/p\boldsymbol{Z})^{\times}$, and e denotes Hida's idempotent attached to $T(p)$.

Now take and fix primitive Dirichlet characters χ and ψ of conductors u and v, respectively, satisfying $uv = N$. We assume that $\mathfrak{r}$ contains their values. Setting $\vartheta := \chi\omega^i$, the formal power series in q

$$\mathscr{E}(\vartheta,\psi) := \delta(\psi)G(T,\vartheta\omega^2) + \sum_{n=1}^{\infty}\left(\sum_{\substack{0<t|n \\ p\nmid t}} \vartheta(t)\psi\left(\frac{n}{t}\right)A_t(T)\right)q^n \in \Lambda_{\mathfrak{r}}[[q]] \tag{2.1.5}$$

gives an ordinary $\Lambda_{\mathfrak{r}}$-adic modular form of level N (the $\Lambda_{\mathfrak{r}}$-adic Eisenstein series attached to ϑ and ψ), provided that $(\vartheta\psi)(-1) = 1$ and $(\vartheta,\psi) \neq (\omega^{-2},\mathbf{1})$. We will always assume that these two conditions are fulfilled. Here, $\delta(\psi) = 1/2$ or 0 according as ψ is the trivial character $\mathbf{1}$ or not; $G(T,\vartheta\omega^2)$ is a twist of the power series attached, by Iwasawa, to the p-adic L-function: $G(\gamma^s-1,\vartheta\omega^2) = L_p(-1-s,\vartheta\omega^2)$; and $A_t(T) = t(1+T)^{s(t)}$ if $t\omega^{-1}(t) = \gamma^{s(t)}$. This $\Lambda_{\mathfrak{r}}$-adic Eisenstein series has the following interpolation property:

$$\begin{aligned} \mathscr{E}(\vartheta,\psi)|_{T=\gamma^d-1} &= \delta(\psi)L(-1-d,(\chi\omega^{i-d})_1) + \sum_{n=1}^{\infty}\left(\sum_{0<t|n}(\chi\omega^{i-d})_1(t)\psi\left(\frac{n}{t}\right)t^{d+1}\right)q^n \\ &:= E_{d+2}((\chi\omega^{i-d})_1,\psi) \in M_{d+2}(\Gamma_1(Np),\mathfrak{r}) \end{aligned} \tag{2.1.6}$$

for any integer $d \geq 0$, where $(\chi\omega^{i-d})_1$ is the character modulo up induced from $\chi\omega^{i-d}$.

The series $\mathscr{E}(\vartheta,\psi)$ is a common eigenform of all $T(n) \in e\mathscr{H}(N;\mathfrak{r})$, and the eigenvalue of $T(n)$ is given by the coefficient of q^n in (2.1.5). We set:

$$\begin{cases} \mathscr{I}(\vartheta,\psi) = \mathscr{I} := (\text{the annihilator of } \mathscr{E}(\vartheta,\psi) \text{ in } e\,\mathscr{H}(N;\mathfrak{r})), \\ \mathfrak{M}(\vartheta,\psi) = \mathfrak{M} := (\mathscr{I}(\vartheta,\psi), T, \varpi). \end{cases} \tag{2.1.7}$$

These ideals of $e\,\mathscr{H}(N;\mathfrak{r})$ are called the Eisenstein ideal and the Eisenstein maximal ideal attached to $\mathscr{E}(\vartheta,\psi)$.

Let $e\,\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ be the localization of the Hecke algebra at $\mathfrak{M}$. This local ring is contained in $e\,\mathscr{H}(N;\mathfrak{r})^{(i)}$. In the following, we take an integer $d \geq 0$ congruent to i modulo $p-1$, and set $k := d+2$. We will henceforth consider $e\,H_k(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})$ as an algebra over $e\,\mathscr{H}(N;\mathfrak{r})$ via the projection $e\,\mathscr{H}(N;\mathfrak{r}) \twoheadrightarrow e\,\mathscr{H}(N;\mathfrak{r})^{(i)}$ and (2.1.4); and thus consider any $e\,H_k(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})$-module as an $e\,\mathscr{H}(N;\mathfrak{r})$-module. We then have an isomorphism:

$$e\,\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}/\omega_d \xrightarrow{\sim} e\,H_k(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})_{\mathfrak{M}}. \tag{2.1.8}$$

The image of $\mathfrak{M}$ in $e\,H_k(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})$ is the maximal ideal corresponding to $E_k(\chi_1,\psi) \in e\,M_k(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})$ in the same way as (2.1.7), and the right-hand side in (2.1.8) is nothing but the localization at this maximal ideal.

Further, the reduction modulo ϖ induces isomorphisms:

$$\begin{cases} e\,H_k(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})/\varpi \xrightarrow{\sim} e\,H_k(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{k}), \text{ and hence} \\ e\,H_k(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})_{\mathfrak{M}}/\varpi \xrightarrow{\sim} e\,H_k(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{k})_{\mathfrak{M}} \end{cases} \tag{2.1.9}$$

for $2 \leq k \not\equiv 0 \pmod{p-1}$. In fact, this is contained in [**O4**, Corollary 1.4.2] for $k \geq 3$. For $k=2$, we argue as follows: We have a perfect pairing

$$e\,\mathscr{H}(N;\mathfrak{r})^{(0)} \times e\,M(N;\Lambda_{\mathfrak{r}})^{(0)} \to \Lambda_{\mathfrak{r}}$$

between the Hecke algebra and the space of $\Lambda_{\mathfrak{r}}$-adic modular forms ([**O4**, Corollary 1.4.3]). Reducing this modulo $\omega_0 = T$, we have a perfect pairing

$$e\,H_2(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r}) \times e\,M_2(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r}) \to \mathfrak{r}$$

from which (2.1.9) follows.

LEMMA 2.1.10. *Let the notation be as above, and assume that p does not divide $\varphi(N)$ when $i \equiv -2 \pmod{p-1}$. Then $e\,\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ is a Gorenstein ring if and only if $e\,H_k(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{k})_{\mathfrak{M}}$ is.*

PROOF. In general, a local Noetherian ring A is a Gorenstein ring if and only if so is $A/(a)$ for a non zero-divisor a in the maximal ideal. Thus when $i \not\equiv -2 \pmod{p-1}$, our assertion follows from (2.1.8) and (2.1.9). Even when $i \equiv -2 \pmod{p-1}$, our assumption assures us that the second isomorphism in (2.1.9) holds ([**O4**, Corollary 1.5.4]). □

In [**O4**], we gave sufficient conditions for the rings above to be Gorenstein, further reducing the problem to forms and Hecke algebras of level N. In that consideration, we excluded the case where $i \equiv 0$ or -1 modulo $p-1$. The purpose of the rest of this paper is to cover these remaining cases, taking $d = 0$ or $d = p-2$, respectively.

For later use, we record here the following lemma which is a slight generalization of [**O4**, Lemma 3.2.2]:

LEMMA 2.1.11. *Assume that* $p \nmid \varphi(N)$, *and also that* $\chi(p) \neq \psi(p)$ *when* $i \equiv -1 \pmod{p-1}$. *Let*

$$0 \to e\, S(N;\Lambda_{\mathfrak{r}})_{\mathfrak{M}} \to e\, M(N;\Lambda_{\mathfrak{r}})_{\mathfrak{M}} \to \Lambda_{\mathfrak{r}} \to 0$$

be the canonical exact sequence of $e\,\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$*-modules considered in* [**O3**, (3.1.5)]. *Then the congruence module associated with this sequence vanishes if and only if* $e\, S(N;\Lambda_{\mathfrak{r}})_{\mathfrak{M}} = \{0\}$.

PROOF. We only need to prove the "only if" part. By the main result (1.5.5) and the argument in 3.2, loc. cit., the congruence module in question vanishes if and only if $e\, h(N;\mathfrak{r})_{\mathfrak{M}}/I(\vartheta,\psi)_{\mathfrak{M}} = \{0\}$, where $I(\vartheta,\psi)$ is the image of $\mathscr{I}(\vartheta,\psi)$ in $e\, h(N;\mathfrak{r})$. By Nakayama's lemma, this implies that $e\, h(N;\mathfrak{r})_{\mathfrak{M}} = \{0\}$. Since $e\, h(N;\mathfrak{r})_{\mathfrak{M}}$ is isomorphic to the $\Lambda_{\mathfrak{r}}$-dual of $e\, S(N;\Lambda_{\mathfrak{r}})_{\mathfrak{M}}$, our conclusion follows. □

2.2. Trace mappings for modular forms of weight two.

Let p and N be as in the previous subsection. We take and fix integers x, y and w satisfying $px - Nyw = 1$, and set

$$W_p := \begin{bmatrix} px & y \\ Npw & p \end{bmatrix}. \tag{2.2.1}$$

It is easy to see that, if $W'_p = \begin{bmatrix} px' & y' \\ Npw' & p \end{bmatrix}$ is another choice, then both $W_p^{-1}W'_p$ and $W_pW_p'^{-1}$ belong to $\Gamma_1(N) \cap \Gamma_0(p)$.

We have the following disjoint decomposition:

$$\Gamma_1(N) = \coprod_{i=0}^{p-1} (\Gamma_1(N) \cap \Gamma_0(p)) \begin{bmatrix} 1 & 0 \\ Ni & 1 \end{bmatrix} \coprod (\Gamma_1(N) \cap \Gamma_0(p)) \begin{bmatrix} 1 & -w \\ -Ny & px \end{bmatrix}. \tag{2.2.2}$$

For $f \in M_k(\Gamma_1(N) \cap \Gamma_0(p); \boldsymbol{C})$, we set

$$\mathrm{Tr}(f) := \sum_{i=0}^{p-1} f|\begin{bmatrix} 1 & 0 \\ Ni & 1 \end{bmatrix} + f|\begin{bmatrix} 1 & -w \\ -Ny & px \end{bmatrix}. \tag{2.2.3}$$

Here, we have used the usual convention:

$$\left(f|\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)(z) = (ad-bc)^{\frac{k}{2}}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right). \tag{2.2.4}$$

It is clear that $\mathrm{Tr}(f)$ belongs to $M_k(\Gamma_1(N); \boldsymbol{C})$.

LEMMA 2.2.5. *Set* $\tau_M := \begin{bmatrix} 0 & -1 \\ M & 0 \end{bmatrix}$. *Then for any* $f \in M_k(\Gamma_1(N) \cap \Gamma_0(p); \boldsymbol{C})$, *we have*:

$$\mathrm{Tr}(f|\tau_{Np}) = p^{1-\frac{k}{2}} f|T(p)|\tau_N + f|W_p|\tau_N.$$

Here, $T(p)$ *in the right-hand side is the Hecke operator of level* Np.

PROOF. This follows from the relations:

$$\tau_{Np}\begin{bmatrix} 1 & 0 \\ Ni & 1 \end{bmatrix} = \begin{bmatrix} 1 & -i \\ 0 & p \end{bmatrix}\tau_N; \quad \tau_{Np}\begin{bmatrix} 1 & -w \\ -Ny & px \end{bmatrix} = \begin{bmatrix} px & y \\ Npw & p \end{bmatrix}\tau_N.$$

□

It is easy to see that the mapping Tr commutes with $T(l)$ with prime numbers $l \neq p$ and the diamond operators. In fact, as for $T(l)$, we have

$$\Gamma_1(N)\begin{bmatrix} 1 & 0 \\ 0 & l \end{bmatrix}\Gamma_1(N) = (\Gamma_1(N) \cap \Gamma_0(p))\begin{bmatrix} 1 & 0 \\ 0 & l \end{bmatrix}\Gamma_1(N).$$

Decomposing this into a disjoint sum of right cosets with respect to $\Gamma_1(N) \cap \Gamma_0(p)$ in two ways, we have the desired commutativity.

From now on, we assume that $k = 2$ and turn to the algebraic theory. First note that, via the correspondence $f \mapsto f(dq/q)$, $M_2(\Gamma_1(N) \cap \Gamma_0(p); \boldsymbol{C})$ is isomorphic to the space of differential forms on the modular curve attached to $\Gamma_1(N) \cap \Gamma_0(p)$, having at most simple poles at cusps. Then Tr corresponds to the trace mapping for differentials from this curve to $X_1(N)_{/\boldsymbol{C}}$. It follows that Tr induces a mapping from $M_2(\Gamma_1(N) \cap \Gamma_0(p); \boldsymbol{Q})$ to $M_2(\Gamma_1(N); \boldsymbol{Q})$, and hence the one with $\boldsymbol{Q}$ replaced by F.

LEMMA 2.2.6. *The mapping* Tr *sends* $e\, M_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})$ *to* $M_2(\Gamma_1(N); \mathfrak{r})$.

PROOF. We may assume that $\mathfrak{r}$ contains a primitive Np-th root of unity ζ_{Np}.

The action of τ_{Np} (resp. τ_N) on the complex upper half plane H induces an automorphism of $X_1(Np)_{/\boldsymbol{Q}(\zeta_{Np})}$ (resp. $X_1(N)_{/\boldsymbol{Q}(\zeta_{Np})}$). Also the action of W_p on H induces an automorphism of $X_1(Np)_{/\boldsymbol{Q}(\zeta_{Np})}$. When $y = -1$, this is w_ζ with $\zeta = e^{2\pi i/p}$, in the notation of [**Gr**, (6.4)].

Let $X_1(Np)_{/\mathfrak{r}}$ be the normalization of the projective j-line $X_1(1)_{/\mathfrak{r}}$ in $X_1(Np)_{/F}$. The closed fibre of this scheme consists of two irreducible components C_∞ and C_0, which meet the cusp sections $i\infty$ and 0, respectively. There is the sheaf of regular differentials

Ω on this curve. In [**Gr**, Section 8 (cf. also Section 10)], Gross studied the connection between $L_{\mathfrak{r}} := H^0(X_1(Np)_{/\mathfrak{r}}, \Omega)$ and cusp forms of weight two with respect to $\Gamma_1(Np)$ over $\mathfrak{r}$. Replacing Ω with $\Omega(\text{cusps})$, and especially $L_{\mathfrak{r}}$ with $L'_{\mathfrak{r}} := H^0(X_1(Np)_{/\mathfrak{r}}, \Omega(\text{cusps}))$, one easily checks that [**Gr**, Proposition 8.4], remains true for modular forms. Thus, for $f \in M_2(\Gamma_1(Np); F)$, $\omega_f := f(dq/q)$ belongs to $L'_{\mathfrak{r}}$ if and only if f and $f|w_\zeta$ both belong to $M_2(\Gamma_1(Np); \mathfrak{r})$. Since τ_{Np} induces an automorphism of $X_1(Np)_{/\mathfrak{r}}$ which interchanges C_∞ and C_0, this holds if and only if f and $f|\tau_{Np}$ belong to $M_2(\Gamma_1(Np); \mathfrak{r})$, for the same reason. When this is the case, the restriction of ω_f to C_∞ (resp. C_0) gives a differential ν (resp. ν'), and we write $\omega_f \equiv (\nu, \nu') \mod \varpi L'_{\mathfrak{r}}$. With these terminologies, if moreover $f \in M_2(\Gamma_1(N) \cap \Gamma_0(p); F)$, we have the formula:

$$\omega_{f|T(p)} \equiv (\nu|T(p), -\nu|w_\zeta) \mod \varpi L'_{\mathfrak{r}}$$

by [**Gr**, Proposition 6.10] (cf. the proof of [**Gr**, Proposition 8.18]).

Now assume that $f \in e\, M_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})$. We then have $f|\tau_{Np} \in M_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})$. Indeed, this was proved for cusp forms in the course of the proof of [**O2**, (2.2.4)], based on the above formula of Gross. The discussion above allows us to apply the same method for modular forms. Consequently, $f|\tau_{Np}|T(p) + f|\tau_{Np}|W_p =: g$ has the q-expansion with coefficients in $\mathfrak{r}$, so that ω_g belongs to $H^0(X_1(N)_{/\mathfrak{r}}, \Omega^1_{X_1(N)_{/\mathfrak{r}}/\mathfrak{r}}(\text{cusps}))$, by the previous lemma. Since τ_N induces an automorphism of $X_1(N)_{/\mathfrak{r}}$, the same holds for $\omega_g \circ \tau_N = \omega_{g|\tau_N}$. Again by the previous lemma, our conclusion follows. □

In the following, we denote by e_0 the idempotent attached to $T(p) \in H_k(\Gamma_1(N); \mathfrak{r})$.

LEMMA 2.2.7. *The Hecke algebra $e\, H_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})$ is generated over $\mathfrak{r}$ by $T(l)$ with prime numbers $l \neq p$ and the diamond operators.*

PROOF. In view of (2.1.9), it is enough to prove the same assertion for $e\, H_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{k})$. On the other hand, we have the identity as subsets of $\mathfrak{k}[[q]]$:

$$e\, M_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{k}) = e_0 M_{p+1}(\Gamma_1(N); \mathfrak{k})$$

([**O4**, Proposition 1.3.5]); and hence an isomorphism

$$e\, H_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{k}) \cong e_0 H_{p+1}(\Gamma_1(N); \mathfrak{k})$$

of $\mathfrak{k}$-algebras, sending $T(l)$ to $T(l)$ and $\langle a \rangle$ to $\langle a \rangle$. We can then apply the standard argument (cf. the proof of Lemma 1.6.1) for the ring in the right-hand side. □

Now $ee_0 = e$ and we have an isomorphism

$$e : e_0 M_2(\Gamma_1(N); \mathfrak{r}) \xrightarrow{\sim} e\, M_2(\Gamma_1(N); \mathfrak{r}) \subseteq e\, M_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r}). \tag{2.2.8}$$

This is proved by Gouvêa for cusp forms ([**Go**, Lemma 2 and Lemma 3]); and the same

proof works for modular forms. This isomorphism commutes with $T(l)$ with prime numbers $l \neq p$ and the diamond operators. Thus we obtain a surjective ring homomorphism:

$$e\, H_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r}) \twoheadrightarrow e_0 H_2(\Gamma_1(N); \mathfrak{r}) \tag{2.2.9}$$

sending $T(l)$ to $T(l)$ and $\langle a \rangle$ to $\langle a \rangle$, by Lemma 1.6.1 and Lemma 2.2.7.

Consequently, for any maximal ideal $\mathfrak{n}$ of $H_2(\Gamma_1(N); \mathfrak{r})$ which is ordinary (in the sense that $T(p) \notin \mathfrak{n}$), there is a unique ordinary maximal ideal $\mathfrak{n}_p$ of $H_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})$ such that (2.2.9) induces a homomorphism:

$$H_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})_{\mathfrak{n}_p} \twoheadrightarrow H_2(\Gamma_1(N); \mathfrak{r})_{\mathfrak{n}}. \tag{2.2.10}$$

Assume that $H_2(\Gamma_1(N); \mathfrak{r})/\mathfrak{n} = \mathfrak{k}$. The natural homomorphism of $H_2(\Gamma_1(N); \mathfrak{r})$ to this residue field factors through $H_2(\Gamma_1(N); \mathfrak{k})$ (cf. [**O4**, Corollary 1.4.2]). Then a common eigenform $f \in M_2(\Gamma_1(N); \mathfrak{k})$ corresponds to this latter homomorphism. In this case, $\mathfrak{n}$ is the annihilator of f in $H_2(\Gamma_1(N); \mathfrak{r})$.

THEOREM 2.2.11. *Let $\mathfrak{n}$ be an ordinary maximal ideal of $H_2(\Gamma_1(N); \mathfrak{r})$, and let $\mathfrak{n}_p$ be as in* (2.2.10)*. Then the trace mapping induces an isomorphism*

$$\mathrm{Tr} : M_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})_{\mathfrak{n}_p} \xrightarrow{\sim} M_2(\Gamma_1(N); \mathfrak{r})_{\mathfrak{n}}$$

and hence the one obtained by reduction modulo ϖ

$$\mathrm{Tr} : M_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{k})_{\mathfrak{n}_p} \xrightarrow{\sim} M_2(\Gamma_1(N); \mathfrak{k})_{\mathfrak{n}}.$$

PROOF. Let $H_2^{(p)}(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})$ be the $\mathfrak{r}$-subalgebra of $H_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})$ generated by $T(l)$ with prime numbers $l \neq p$ and the diamond operators. We may view $\mathrm{Tr} : e\, M_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r}) \to M_2(\Gamma_1(N); \mathfrak{r})$ as a homomorphism of $H_2^{(p)}(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})$-modules. The inverse image of $\mathfrak{n}$ via $H_2^{(p)}(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r}) \twoheadrightarrow H_2(\Gamma_1(N); \mathfrak{r})$ and that of $e\mathfrak{n}'$ via $H_2^{(p)}(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r}) \twoheadrightarrow e\, H_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})$ coincide. The localization of Tr above at this maximal ideal gives the first homomorphism in the theorem, which is compatible with (2.2.10).

Let $\mathfrak{r}'$ be the ring of integers of a finite extension of F. Then the base extension of the first homomorphism to $\mathfrak{r}'$ is a direct sum of mappings of the same type. We may thus assume that $H_2(\Gamma_1(N); \mathfrak{r})/\mathfrak{n} = \mathfrak{k}$, so that $\mathfrak{n}$ corresponds to an eigenform $f \in M_2(\Gamma_1(N); \mathfrak{k})$ as above. Moreover, it is enough to prove the latter assertion.

It is clear from the construction (2.2.8)-(2.2.10) that $e(M_2(\Gamma_1(N); \mathfrak{r})_{\mathfrak{n}})$ is contained in $M_2(\Gamma_1(N) \cap \Gamma_0(p); \mathfrak{r})_{\mathfrak{n}_p}$, and hence we have the following (not necessarily commutative) diagram:

$$\begin{array}{ccc} M_2(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})_{\mathfrak{n}_p} & \xrightarrow{\mathrm{Tr}} & M_2(\Gamma_1(N);\mathfrak{r})_{\mathfrak{n}} \subseteq e_0\, M_2(\Gamma_1(N);\mathfrak{r}) \\ {\scriptstyle i}\nwarrow & & \downarrow{\scriptstyle e} \\ & & e\,(M_2(\Gamma_1(N);\mathfrak{r})_{\mathfrak{n}}) \end{array}$$

where i is the inclusion mapping. Since $T(p)$ of level N and that of Np coincide in characteristic p, by reducing modulo ϖ, we obtain the diagram:

$$\begin{array}{ccc} M_2(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{k})_{\mathfrak{n}_p} & \xrightarrow{\mathrm{Tr}} & M_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}} \\ {\scriptstyle i}\nwarrow & & \| \\ & & M_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}} \end{array}$$

which commutes because $\mathrm{Tr}\circ i = p+1$. This shows the surjectivity of Tr, and also that

$$M_2(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{k})_{\mathfrak{n}_p} = \mathrm{Ker}(\mathrm{Tr}) \oplus i(M_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}})$$

as modules over $H_2(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{k})_{\mathfrak{n}_p}$.

If $\mathrm{Ker}(\mathrm{Tr})$ does not reduce to $\{0\}$, then there is a non-zero element g in this space annihilated by $\mathfrak{n}_p$. Under our assumption, it is the unique eigenform (up to constant multiples) corresponding to the algebra homomorphism:

$$H_2(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{k}) \twoheadrightarrow H_2(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})_{\mathfrak{n}_p}/\mathfrak{n}_p \cong H_2(\Gamma_1(N);\mathfrak{r})_{\mathfrak{n}}/\mathfrak{n}.$$

It follows that g is a constant multiple of f, which is clearly absurd. □

COROLLARY 2.2.12. *With the same notation as above, we have an isomorphism*:

$$H_2(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})_{\mathfrak{n}_p} \xrightarrow{\sim} H_2(\Gamma_1(N);\mathfrak{r})_{\mathfrak{n}}.$$ □

REMARK 2.2.13. It follows from this corollary that there is a unique maximal ideal $\mathfrak{N}$ of $e\,\mathscr{H}(N;\mathfrak{r})$ such that (2.1.4) induces an isomorphism:

$$e\,\mathscr{H}(N;\mathfrak{r})_{\mathfrak{N}}/\omega_0 \xrightarrow{\sim} H_2(\Gamma_1(N);\mathfrak{r})_{\mathfrak{n}}$$

and similar assertion holds for Hecke algebras attached to cusp forms. This extends [**Go**, Corollary 6] to the case where $k=2$. With this, one immediately extends the assertions from Proposition 7 to Corollary 10 in [**Go**] to this case.

2.3. Proof of Theorem I when $d = 0$.

The purpose of this subsection is to prove Theorem I in the introduction when $d = 0$; and hence $k = 2$ and $k' = p - 1$. After Corollary 2.2.12, the proof in fact proceeds along the same line as in [**O4**], as we will see below.

In general, for Dirichlet characters χ and ψ of conductors u and v, respectively, we have the well-known Eisenstein series of level $N = uv$ and weight $m \geq 2$

$$E_m(\chi,\psi) := \delta(\psi)L(1-m,\chi) + \sum_{n=1}^{\infty}\left(\sum_{0<t|n}\chi(t)\psi\left(\frac{n}{t}\right)t^{m-1}\right)q^n \in M_m(\Gamma_1(N);\boldsymbol{C}) \quad (2.3.1)$$

whenever $(\chi\psi)(-1) = (-1)^m$, except for the case where $k = 2$ and $\chi = \psi = \mathbf{1}$.

In the following, we fix characters χ and ψ as above such that $\chi\psi$ is even, and assume that $\mathfrak{r}$ contains their values. The Eisenstein maximal ideal of $e\mathscr{H}(N;\mathfrak{r})$ to be considered is $\mathfrak{M}(\chi,\psi) =: \mathfrak{M}$. We assume that $p \nmid \varphi(N)$.

First, in the exceptional case where $\chi = \psi = \mathbf{1}$, we note that $e\mathscr{H}(1;\mathfrak{r})_{\mathfrak{M}} = \Lambda_{\mathfrak{r}}$. Indeed, we have $G(0,\omega^2) = (p-1)/12$ (cf. (2.1.6)), and hence $G(T,\omega^2)$ is a unit of $\Lambda_{\mathfrak{r}}$. By the main result (1.5.5) in [**O3**], the congruence module considered in Lemma 2.1.11 vanishes, and $e\,M(1;\Lambda_{\mathfrak{r}})_{\mathfrak{M}}$ is a free $\Lambda_{\mathfrak{r}}$-module of rank one.

We thus henceforth assume that $(\chi,\psi) \neq (\mathbf{1},\mathbf{1})$. Let $\mathfrak{m} = \mathfrak{m}(2;\chi,\psi)$ and $\mathfrak{m}' = \mathfrak{m}(p-1;\psi,\chi)$ be the maximal ideals of $H_2(\Gamma_1(N);\mathfrak{r})$ and $H_{p-1}(\Gamma_1(N);\mathfrak{r})$ associated with $E_2(\chi,\psi) \in M_2(\Gamma_1(N);\mathfrak{r})$ and $E_{p-1}(\psi,\chi) \in M_{p-1}(\Gamma_1(N);\mathfrak{r})$, respectively. If we indicate by tilde the reduction modulo ϖ, $\mathfrak{m}$ (resp. $\mathfrak{m}'$) is the annihilator of $\widetilde{E}_2(\chi,\psi)$ (resp. $\widetilde{E}_{p-1}(\psi,\chi)$) in $H_2(\Gamma_1(N);\mathfrak{r})$ (resp. $H_{p-1}(\Gamma_1(N);\mathfrak{r})$). We note that

$$\theta^{p-1}\widetilde{E}_2(\chi,\psi) = \theta\widetilde{E}_{p-1}(\psi,\chi). \quad (2.3.2)$$

Now take $\mathfrak{m}$ for the ideal $\mathfrak{n}$ in the previous subsection. Then we have $H_2(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})_{\mathfrak{n}_p} = e\,H_2(\Gamma_1(N)\cap\Gamma_0(p);\mathfrak{r})_{\mathfrak{M}}$. Thus by Lemma 2.1.10 and Corollary 2.2.12, $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ is a Gorenstein ring if and only if so is $H_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}$. Since the pairing

$$M_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}} \times H_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}} \to \mathfrak{k}$$

considered in 1.6 is perfect, the condition above is equivalent to the cyclicity of $M_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}$ as a module over $H_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}$.

To prove Theorem I, part 1), we may assume that $\mathfrak{k}$ contains a primitive N-th root of unity. We can then consider the pairing given by (1.6.4)

$$[\ ,\ ]_{2,\mathfrak{m}} : M_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}} \times S_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}} \to \mathfrak{k}.$$

(Instead of this, we could also use the twisted version of Ulmer's pairing $(\ ,\ )_2^*$ studied in [**O4**, 2.5].)

LEMMA 2.3.3. *Let K_2 be the left kernel of this pairing. We have*:

$$K_2 = \{f \in M_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}} \mid \theta^{p-1}f = \theta g \text{ with some } g \in M_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}\}.$$

PROOF. By Theorem 1.6.5, K_2 consists of $f \in M_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}$ such that $\theta^{p-1}f = \theta g$ with some $g \in M_{p-1}(\Gamma_1(N);\mathfrak{k})$.

The space $M_{p-1}(\Gamma_1(N);\mathfrak{k})$ contains $\mathfrak{k}A$. This subspace is annihilated by the maximal ideal $\mathfrak{n}_0$ of $H_{p-1}(\Gamma_1(N);\mathfrak{k})$ generated by $T(l)-(1+l^{-1})$ (resp. $T(l)-1$) with prime numbers l such that $l \nmid Np$ (resp. $l \mid Np$), and $\langle a\rangle - 1$. If $\mathfrak{n}$ is a maximal ideal different from $\mathfrak{n}_0$, we have $H_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}} \cap \mathfrak{k}A = \{0\}$, and it follows from the same argument as in Lemma 1.6.1 or Lemma 1.6.3 that $H_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}}$ is generated over $\mathfrak{k}$ by $T(l)$ with prime numbers $l \neq p$ and the diamond operators.

Let g be as above. From the relation (1.5.4), for m sufficiently large, we have:

$$\theta^{p-1}(T(l) - (\widetilde{\chi}(l)l + \widetilde{\psi}(l)))^m f = l^m \theta(T(l) - (\widetilde{\psi}(l)l^{-1} + \widetilde{\chi}(l)))^m g = 0$$

for any prime number $l \neq p$, and

$$\theta^{p-1}(\langle a\rangle - \widetilde{\chi}\widetilde{\psi}(a))^m f = \theta(\langle a\rangle - \widetilde{\chi}\widetilde{\psi}(a))^m g = 0.$$

Express g in the form $\sum_{\mathfrak{n}} g_{\mathfrak{n}}$ with $g_{\mathfrak{n}} \in M_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}}$, the sum running over all maximal ideals of $H_{p-1}(\Gamma_1(N);\mathfrak{k})$. The relations above show that $g = g_{\mathfrak{m}'} + g_{\mathfrak{n}_0}$, and also that $(T(l) - (\widetilde{\psi}(l)l^{-1} + \widetilde{\chi}(l)))^m g_{\mathfrak{n}_0} \in \mathfrak{k}A$. Since there is a prime number l such that $T(l) - (\widetilde{\psi}(l)l^{-1} + \widetilde{\chi}(l))$ is a unit in $H_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}_0}$, $g_{\mathfrak{n}_0}$ itself belongs to $\mathfrak{k}A$. We therefore have $\theta^{p-1}f = \theta g_{\mathfrak{m}'}$. □

Set

$$K_{p-1} = \{g \in M_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'} \mid \theta^2 g = \theta f \text{ with some } f \in M_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}\}.$$

Again noting that $M_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'} \cap \mathfrak{k}A = \{0\}$, we see that the correspondence $f \leftrightarrow g$ gives a bijection between K_2 and K_{p-1}, and hence $\dim_{\mathfrak{k}} K_2 = \dim_{\mathfrak{k}} K_{p-1}$. Consequently, if we assume that $\dim_{\mathfrak{k}} K_{p-1} = 1$, it follows from (2.3.2) that the pairing $[\ ,\ ]_{2,\mathfrak{m}}$ gives the perfect pairing

$$M_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}/\mathfrak{k}\widetilde{E}_2(\chi,\psi) \times S_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}} \to \mathfrak{k}$$

and this implies that $M_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}$ is a cyclic module over $H_2(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}$ (cf. [**O4**, Lemma 3.3.1]). This settles the part 1) of Theorem I when $d = 0$.

As for the part 2), set $\mathfrak{M}' := \mathfrak{M}(\psi\omega^{p-3}, \chi)$ and consider the exact sequence

$$0 \to e\,S(N;\Lambda_{\mathfrak{r}})_{\mathfrak{M}'} \to e\,M(N;\Lambda_{\mathfrak{r}})_{\mathfrak{M}'} \to \Lambda_{\mathfrak{r}} \to 0$$

of $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}'}$-modules. The number given in the part 2) is a unit multiple of the value at $T=\gamma^{p-3}-1$ of the power series in [**O3**, (1.5.4)], with θ and ψ there replaced by $\psi\omega^{p-3}$ and χ, respectively. By the main result (1.5.5) in [**O3**], the condition given in the part 2) implies that the congruence module attached to the exact sequence above vanishes. It follows from Lemma 2.1.11 that $eM(N;\Lambda_{\mathfrak{r}})_{\mathfrak{M}'}$ is free of rank one over $\Lambda_{\mathfrak{r}}$. For the same reason as [**O4**, Theorem 3.2.3], we have $\dim_{\mathfrak{k}} M_{p-1}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}=1$, which completes the proof.

3. *p*-adic Hecke algebras of Eisenstein type when $d=p-2$.

3.1. Modular forms of weight one and weight p over finite fields.

The purpose of this section is to prove Theorem I in the introduction, when $d=p-2$ (and hence $k=p$ and $k'=1$). As in 2.1, $\mathfrak{r}$ (resp. $\mathfrak{k}=\mathfrak{r}/(\varpi)$) denotes the ring of integers of a finite extension F of $\boldsymbol{Q}_p$ (resp. its residue field).

Recall that by $M_1(\Gamma_1(N);\mathfrak{k})$, we mean the space of modular forms of weight one in the sense of Katz. There is a natural (q-expansion preserving) injection $\times A: M_1(\Gamma_1(N);\mathfrak{k})\hookrightarrow M_p(\Gamma_1(N);\mathfrak{k})$ by means of which we consider $M_1(\Gamma_1(N);\mathfrak{k})$ as a subspace of $M_p(\Gamma_1(N);\mathfrak{k})$. Also, the operator V_p induces an injection from $M_1(\Gamma_1(N);\mathfrak{k})$ to $M_p(\Gamma_1(N);\mathfrak{k})$. These mappings commute with all $T(l)$ with prime numbers $l\neq p$ and the diamond operators. We consider the subspace

$$M_p^{\mathrm{old}}(\Gamma_1(N);\mathfrak{k}):=M_1(\Gamma_1(N);\mathfrak{k})+V_pM_1(\Gamma_1(N);\mathfrak{k})\subseteq M_p(\Gamma_1(N);\mathfrak{k}). \tag{3.1.1}$$

Here note that $M_1(\Gamma_1(N);\mathfrak{k})\cap V_pM_1(\Gamma_1(N);\mathfrak{k})=\{0\}$ since any non-zero element of $V_pM_1(\Gamma_1(N);\mathfrak{k})$ has filtration p. To distinguish the p-th Hecke operator $T(p)$ of weight p and that of weight one, we use the symbol U_p for the former and retain the symbol $T(p)$ for the latter, in this section. We recall that

$$f|T(p)=f|U_p+f|\langle p\rangle|V_p \tag{3.1.2}$$

for $f\in M_1(\Gamma_1(N);\mathfrak{k})$ ([**Gr**, (4.7)]). Thus, via the isomorphism

$$M_p^{\mathrm{old}}(\Gamma_1(N);\mathfrak{k})\xrightarrow{\sim}M_1(\Gamma_1(N);\mathfrak{k})\oplus M_1(\Gamma_1(N);\mathfrak{k}) \text{ given by } f+g|V_p\mapsto(f,g) \tag{3.1.3}$$

U_p on the left commutes with the mapping $(f,g)\mapsto(f|T(p)+g,-f|\langle p\rangle)$ on the right. Especially, $M_p^{\mathrm{old}}(\Gamma_1(N);\mathfrak{k})$ is an $H_p(\Gamma_1(N);\mathfrak{k})$-submodule of $M_p(\Gamma_1(N);\mathfrak{k})$.

Take Dirichlet characters χ and ψ such that the product of their conductors is N. We will always assume that $(\chi\psi)(-1)=-1$. We also assume that $\mathfrak{r}$ contains the values of χ and ψ. We can then consider the Eisenstein series $E_p(\chi,\psi)\in M_p(\Gamma_1(N);\mathfrak{r})$ defined by (2.3.1). As for the Eisenstein series of weight one, it is known that the series given by

$$E_1(\chi,\psi):=c(\chi,\psi)+\sum_{n=1}^{\infty}\left(\sum_{0<t|n}\chi(t)\psi\left(\frac{n}{t}\right)\right)q^n \tag{3.1.4}$$

$$\text{with } c(\chi,\psi)=\begin{cases} 0 \text{ if } \chi\neq\mathbf{1} \text{ and } \psi\neq\mathbf{1};\\ \dfrac{L(0,\psi)}{2} \text{ if } \chi=\mathbf{1};\\ \dfrac{L(0,\chi)}{2} \text{ if } \psi=\mathbf{1}\end{cases}$$

is a modular form of level N and weight one, which in fact belongs to $M_1(\Gamma_1(N);\mathfrak{r})$. As before, let us indicate by tilde the reduction modulo ϖ. Then these are related by the following

LEMMA 3.1.5. $\widetilde{E}_p(\chi,\psi)=\widetilde{E}_1(\chi,\psi)-\widetilde{\chi}(p)\widetilde{E}_1(\chi,\psi)|V_p$.

PROOF. It is easy to see that the coefficients of q^n of both sides coincide, for each positive integer n. It follows that $\widetilde{E}_p(\chi,\psi)-(\widetilde{E}_1(\chi,\psi)-\widetilde{\chi}(p)\widetilde{E}_1(\chi,\psi)|V_p)\in M_p(\Gamma_1(N);\mathfrak{k})$ is a constant, which can be no other than zero. (Of course, one can also directly check that the constant terms of both sides agree, using the congruence property of generalized Bernoulli numbers.) □

Let $\mathfrak{m}:=\mathfrak{m}(p;\chi,\psi)$ be the maximal ideal of $H_p(\Gamma_1(N);\mathfrak{r})$ generated by the annihilator of $E_p(\chi,\psi)$ and ϖ. Let $H_p^{(p)}(\Gamma_1(N);\mathfrak{r})$ be, as before, the subalgebra of $H_p(\Gamma_1(N);\mathfrak{r})$ generated by $T(l)$ with prime numbers $l\neq p$ and the diamond operators, and define its maximal ideal $\mathfrak{m}^{(p)}$ in the same manner as above. By a slight abuse of notation, we define the ideal $\mathfrak{m}':=\mathfrak{m}(1;\psi,\chi)$ of $H_1(\Gamma_1(N);\mathfrak{k})$ as the annihilator of $\widetilde{E}_1(\psi,\chi)=\widetilde{E}_1(\chi,\psi)$, because of the absence of the corresponding object over $\mathfrak{r}$. Thus $\mathfrak{m}^{(p)}$ is generated by $T(l)-(\chi(l)l^{p-1}+\psi(l))$ $(l\neq p)$, $\langle a\rangle-\chi(a)\psi(a)$ and ϖ; and $\mathfrak{m}$ is generated by these elements and $U_p-\psi(p)$. On the other hand, $\mathfrak{m}'$ is generated by $T(l)-(\widetilde{\chi}(l)+\widetilde{\psi}(l))$ for *all* prime numbers l and $\langle a\rangle-\widetilde{\chi}(a)\widetilde{\psi}(a)$.

By Lemma 1.6.1, the natural homomorphism of $H_p^{(p)}(\Gamma_1(N);\mathfrak{r})$ to $H_1(\Gamma_1(N);\mathfrak{k})$ is surjective, and hence it maps $\mathfrak{m}^{(p)}$ onto $\mathfrak{m}'$. We therefore have:

$$M_p^{\mathrm{old}}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}=M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}+V_p(M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}). \tag{3.1.6}$$

LEMMA 3.1.7. *A maximal ideal of* $H_p(\Gamma_1(N);\mathfrak{r})$ *containing* $\mathfrak{m}^{(p)}$ *is either* $\mathfrak{m}$ *or* $\mathfrak{m}(p;\psi,\chi)=:\mathfrak{n}$.

PROOF. Let $\mathfrak{a}$ be a maximal ideal of $H_p(\Gamma_1(N);\mathfrak{r})$ containing $\mathfrak{m}^{(p)}$. To the natural homomorphism: $H_p(\Gamma_1(N);\mathfrak{r})\to H_p(\Gamma_1(N);\mathfrak{r})/\mathfrak{a}=:\mathfrak{k}'$, with a finite extension $\mathfrak{k}'$ of $\mathfrak{k}$, corresponds a common eigenform f of all Hecke operators in $M_p(\Gamma_1(N);\mathfrak{k}')$ which we may assume that $a(1;f)=1$. Let α be the eigenvalue of U_p for f.

Since the homomorphism above sends $T(l)$ to $\widetilde{\chi}(l)+\widetilde{\psi}(l)$ for $l\neq p$, and $\langle a\rangle$ to $\widetilde{\chi}(a)\widetilde{\psi}(a)$, respectively, we see that $\widetilde{E}_p(\chi,\psi)-f$ is a power series in q^p, that is, there is a $g\in M_1(\Gamma_1(N);\mathfrak{k}')$ such that $\widetilde{E}_p(\chi,\psi)-f=g|V_p$. Applying U_p to this equation, we get: $\widetilde{\psi}(p)\widetilde{E}_p(\chi,\psi)-\alpha f=g$, and hence $(\widetilde{\psi}(p)-\alpha)\widetilde{E}_p(\chi,\psi)=g-\alpha g|V_p$.

If $\alpha=\widetilde{\psi}(p)$, then we have $\mathfrak{a}=\mathfrak{m}$. Otherwise, $g':=(\widetilde{\psi}(p)-\alpha)^{-1}g$ satisfies $\widetilde{E}_p(\chi,\psi)=$

$g' - \alpha g'|V_p$, which belongs to $M_p^{\mathrm{old}}(\Gamma_1(N); \mathfrak{k}')$. We see from the previous lemma that $g' = \widetilde{E}_1(\chi, \psi)$ and $\alpha = \widetilde{\chi}(p)$. In this case, we have $\mathfrak{a} = \mathfrak{n}$. □

COROLLARY 3.1.8. *If $\widetilde{\chi}(p) \neq \widetilde{\psi}(p)$, we have*:

$$M_{\mathfrak{m}^{(p)}} = M_{\mathfrak{m}} \oplus M_{\mathfrak{n}}.$$

for any $H_p(\Gamma_1(N); \mathfrak{r})$-module M. □

3.2. Proof of Theorem I when $d = p - 2$.

We keep the notation introduced in the previous subsection. We henceforth assume that $p \nmid \varphi(N)$ and $\chi(p) \neq \psi(p)$, so that $\widetilde{\chi}(p) \neq \widetilde{\psi}(p)$. Thus in the terminology of [**O3**, (1.4.10)], the pairs $(\chi\omega^{-1}, \psi)$ and $(\psi\omega^{-1}, \chi)$ are not exceptional. Now the condition in Theorem I, part 1) in the introduction reduces to a rather stronger one:

PROPOSITION 3.2.1. *Let the assumption be as above. Then the dimension of the space*

$$\{f \in M_1(\Gamma_1(N); \mathfrak{k})_{\mathfrak{m}'} \mid \theta^p f (= \theta f) = \theta g \text{ with some } g \in M_p(\Gamma_1(N); \mathfrak{k})_{\mathfrak{m}}\}$$

over $\mathfrak{k}$ is one if and only if $\dim_{\mathfrak{k}} M_1(\Gamma_1(N); \mathfrak{k})_{\mathfrak{m}'} = 1$.

The "if" part is clear, since we have $\theta\widetilde{E}_1(\chi, \psi) = \theta\widetilde{E}_p(\chi, \psi)$. To prove the other part, we make use of the following elementary lemma:

LEMMA 3.2.2. *Let K be a field, and a and b different elements of K. Let V be a finite dimensional vector space over K. Suppose we are given a K-linear transformation T of V which has only one eigenvalue $a + b$. Set $W := V \oplus V$ and define a K-linear transformation U of W by $U(x, y) := (Tx + y, -abx)$. We have*:

1) *The eigenvalues of U on W are a and b*;

2) *Let $W(U, a)$ (resp. $W(U, b)$) be the maximal subspace of W on which $U - a1_W$ (resp. $U - b1_W$) acts nilpotently. Then* $\dim_K W(U, a) = \dim_K W(U, b) = \dim_K V$, *and the projection to the first factor maps $W(U, a)$ and $W(U, b)$ isomorphically onto V.*

PROOF. The operator U satisfies the quadratic relation: $U^2 - (T \oplus T)U + ab1_W = 0$, and hence its possible eigenvalues are a and b.

If $x_0 \in V$ is an eigenvector of T, then $(x_0, -bx_0)$ (resp. $(x_0, -ax_0)$) is an eigenvector of U with the eigenvalue a (resp. b), which proves the first assertion.

The second part follows by induction on the dimension of V over K: This is clear from the above observation when $\dim_K V = 1$. Then the validity of our claim for V/Kx_0 and its linear transformation induced by T easily implies the validity for V and T. □

PROOF OF PROPOSITION 3.2.1. We apply the lemma above to the following situation: $K = \mathfrak{k}$, $V = M_1(\Gamma_1(N); \mathfrak{k})_{\mathfrak{m}'}$, $T = T(p)$, $a = \widetilde{\chi}(p)$ and $b = \widetilde{\psi}(p)$.

Since $p \nmid \varphi(N)$, the diamond action of $(\boldsymbol{Z}/N\boldsymbol{Z})^\times$ on $M_1(\Gamma_1(N); \mathfrak{k})_{\mathfrak{m}'}$ is given by the character $\widetilde{\chi}\widetilde{\psi}$, and hence the operator U on W in the lemma corresponds to U_p on

$M_p^{\mathrm{old}}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}} =: W'$ via (3.1.3). It thus follows from the lemma that $W' = W'(U_p, \widetilde{\chi}(p)) \oplus W'(U_p, \widetilde{\psi}(p))$, and note here that $M_p^{\mathrm{old}}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}} = W'(U_p, \widetilde{\psi}(p))$. It also follows that, for any $f \in M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}$, there is an element $g \in W'(U_p, \widetilde{\psi}(p))$ of the form $f + h|V_p$, which clearly satisfies $\theta f = \theta g$. This completes the proof. □

We now consider the perfect pairing:

$$M_p(\Gamma_1(N);\mathfrak{k}) \times H_p(\Gamma_1(N);\mathfrak{k}) \to \mathfrak{k} \tag{3.2.3}$$

which sends (f,t) to $a(1;f|t)$ (cf. [**O4**, 1.4]).

LEMMA 3.2.4. *Assume that* $\dim_{\mathfrak{k}} M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'} = 1$, *i.e.* $M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'} = \mathfrak{k}\widetilde{E}_1(\chi,\psi)$. *Then we have an isomorphism*:

$$H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}} \cong \mathrm{Hom}_{\mathfrak{k}}\left(\frac{M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}}{\mathfrak{k}\widetilde{E}_1(\chi,\psi)|V_p}, \mathfrak{k}\right)$$

of $H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}$*-modules.*

PROOF. The left kernel of the pairing

$$M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}} \times H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}} \to \mathfrak{k}$$

induced from (3.2.3) is $(V_p M_1(\Gamma_1(N);\mathfrak{k}))_{\mathfrak{m}^{(p)}}$, as seen in the course of the proof of Lemma 1.6.1. This is equal to: $V_p(M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}) = \mathfrak{k}\widetilde{E}_1(\chi,\psi)|V_p$. As a consequence, we see that $H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}} \neq H_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}$, and also that the pairing above induces an injective homomorphism:

$$\frac{M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}}{\mathfrak{k}\widetilde{E}_1(\chi,\psi)|V_p} \hookrightarrow \mathrm{Hom}_{\mathfrak{k}}(H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}, \mathfrak{k})$$

of $H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}$-modules. But we have

$$\dim_{\mathfrak{k}} M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}} = \dim_{\mathfrak{k}} H_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}$$

$$> \dim_{\mathfrak{k}} H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}} \geq \dim_{\mathfrak{k}} M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}} - 1.$$

This shows that the two modules above have the same dimension over $\mathfrak{k}$. □

COROLLARY 3.2.5. *Assume that* $\dim_{\mathfrak{k}} M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'} = 1$. *Then as a module over* $H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}$,

$$\mathrm{Hom}_{\mathfrak{k}}\left(\frac{S_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}}{S_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}\cap \mathfrak{k}\widetilde{E}_1(\chi,\psi)|V_p},\mathfrak{k}\right)$$

is cyclic.

PROOF. The module in question is a quotient of the module in the right-hand side of the isomorphism above. □

We now prove the part 1) of Theorem I in the introduction. We thus assume that $\dim_{\mathfrak{k}} M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}=1$, and want to show that $M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}/\mathfrak{k}\widetilde{E}_p(\chi,\psi)$ is a cyclic module over $H_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}$. As in 2.3 or [**O4**, 3.3], this would finish the proof. To do this, we may assume that $\mathfrak{k}$ contains a primitive N-th root of unity, and then we invoke the pairing

$$[\ ,\ ]_{p,\mathfrak{m}^{(p)}} : M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}\times S_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}\to\mathfrak{k} \tag{3.2.6}$$

considered in 1.6. It is at this stage we really need our new pairing. In view of Corollary 3.1.8, it follows from Theorem 1.6.5 that the left kernel of $[\ ,\ ]_{p,\mathfrak{m}^{(p)}}$ consists of $f\in M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}$ such that $\theta f=\theta g$ with some $g\in M_1(\Gamma_1(N);\mathfrak{k})$. But such a g must belong to $M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}$ (cf. the proof of Lemma 2.3.3, or [**O4**, Proposition 3.1.2]). Since the kernel of θ on $M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}$ is $V_p(M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'})$, our assumption implies that the left kernel of $[\ ,\ ]_{p,\mathfrak{m}^{(p)}}$ is $\mathfrak{k}\widetilde{E}_1(\chi,\psi)+\mathfrak{k}\widetilde{E}_1(\chi,\psi)|V_p=\mathfrak{k}\widetilde{E}_p(\chi,\psi)+\mathfrak{k}\widetilde{E}_p(\psi,\chi)$. Noting that $S_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}$ belongs to the right kernel by Definition 1.5.6 and (1.2.5), we have injections:

$$\frac{M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}}{\mathfrak{k}\widetilde{E}_p(\chi,\psi)+\mathfrak{k}\widetilde{E}_p(\psi,\chi)}\hookrightarrow \mathrm{Hom}_{\mathfrak{k}}\left(\frac{S_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}}{S_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}},\mathfrak{k}\right)\hookrightarrow \mathrm{Hom}_{\mathfrak{k}}(S_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}},\mathfrak{k})$$

of $H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}$-modules. Comparing the dimensions over $\mathfrak{k}$, we see that the two mappings above are in fact isomorphisms. We have especially shown that $S_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}=\{0\}$, i.e. $\widetilde{E}_1(\chi,\psi)$ is not a cusp form. This in turn implies that the above three modules are cyclic over $H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}$ by Corollary 3.2.5. Especially, so are

$$\frac{M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}}{\mathfrak{k}\widetilde{E}_p(\chi,\psi)+\mathfrak{k}\widetilde{E}_p(\psi,\chi)}\cong\frac{M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}}{\mathfrak{k}\widetilde{E}_p(\chi,\psi)}\oplus\frac{M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}}}{\mathfrak{k}\widetilde{E}_p(\psi,\chi)}.$$

We conclude that its quotient $M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}/\mathfrak{k}\widetilde{E}_p(\chi,\psi)$ is also a cyclic module over $H_p^{(p)}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}^{(p)}}$, and hence over $H_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}}$.

We next turn to the proof of the part 2) of Theorem I. For this, we consider the maximal ideal $\mathfrak{M}':=\mathfrak{M}(\psi\omega^{-1},\chi)$ of $e\mathscr{H}(N;\mathfrak{r})$.

Since our pair $(\psi\omega^{-1},\chi)$ is not exceptional, we have a canonical exact sequence:

$$0 \to e\,S(N;\Lambda_{\mathfrak{r}})_{\mathfrak{M}'} \to e\,M(N;\Lambda_{\mathfrak{r}})_{\mathfrak{M}'} \to \Lambda_{\mathfrak{r}} \to 0$$

of $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}'}$-modules. Remembering that $1-(\chi^{-1}\psi)(p)$ is a unit in $\mathfrak{r}$, and letting $T=\gamma^{-1}-1$ for the power series given in [**O3**, (1.5.4)] for $(\psi\omega^{-1},\chi)$ in place of (θ,ψ), we see that the numerical assumption in the part 2) implies the vanishing of the conguence module attached to this exact sequence, by [**O3**, (1.5.5)]. It follows that $e\,M(N;\Lambda_{\mathfrak{r}})_{\mathfrak{M}'}$ is isomorphic to $\Lambda_{\mathfrak{r}}$ by Lemma 2.1.11, and hence $e\,M_p(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{M}'}$ is isomorphic to $\mathfrak{r}$. We conclude from this that $\dim_{\mathfrak{k}} M_p(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}}=1$.

On the other hand, it follows from Lemma 3.2.2 and the proof of Proposition 3.2.1 that $M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}$ and $M_p^{\mathrm{old}}(\Gamma_1(N);\mathfrak{k})_{\mathfrak{n}}=W'(U_p,\widetilde{\chi}(p))$ have the same dimension over $\mathfrak{k}$. The assumption in the part 2) thus implies that $\dim_{\mathfrak{k}} M_1(\Gamma_1(N);\mathfrak{k})_{\mathfrak{m}'}=1$. This completes the proof.

4. Application to Iwasawa theory.

4.1. Generators of Hecke algebras.

In this section, we will exclusively consider the case where $\psi=\mathbf{1}$. We thus fix a Dirichlet character χ of conductor N, and let $\vartheta=\chi\omega^i$ be even. As before, we assume that $\mathfrak{r}$ contains the values of ϑ, and let $\mathfrak{M}:=\mathfrak{M}(\vartheta,\mathbf{1})$ be the corresponding Eisenstein maximal ideal of $e\mathscr{H}(N;\mathfrak{r})$. We will always assume that $p\nmid\varphi(N)$, and that $(\vartheta,\mathbf{1})$ is not exceptional, i.e. $\chi(p)\neq 1$ when $i\equiv -1 \bmod p-1$.

The purpose of this subsection is to prove the following

PROPOSITION 4.1.1. *The algebra $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ is generated over $\Lambda_{\mathfrak{r}}$ by $T(l)$ with prime numbers l not dividing Np.*

In [**O4**, 3.4], we used this fact to establish Theorem 3.4.12 there. However, its proof was incomplete, since the one given in Remark 3.3.3, loc. cit. implicitly assumed that the Galois representation attached to $e\,M_2(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{M}}$ can be realized over the subalgebra of $e\,H_2(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{M}}$ of the same type as in the proposition, which is not obvious even if $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ is Gorenstein. In the following, we give a corrected and detailed version of the proof. The basic idea is, as in [**O4**], due to Wiles [**Wi2**].

We first note that, since $p\nmid\varphi(N)$, $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ is generated over $\Lambda_{\mathfrak{r}}$ by $T(l)$ with prime numbers l ([**O3**, (3.1.1)]). Take an integer $d\geq 0$ and let $\mathfrak{m}:=\mathfrak{m}(d+2;(\chi\omega^{i-d})_1,\mathbf{1})$ be the Eisenstein maximal ideal of $H_{d+2}(\Gamma_1(Np);\mathfrak{r})$ corresponding to $E_{d+2}((\chi\omega^{i-d})_1,\mathbf{1})$. By (2.1.4) and (2.1.6), we have an isomorphism:

$$e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}/\omega_d \xrightarrow{\sim} e\,H_{d+2}(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{M}} = H_{d+2}(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}}. \tag{4.1.2}$$

It is enough to show that the ring in the right-hand side is generated over $\mathfrak{r}$ by $T(l)$ with $l\nmid Np$, by Nakayama's lemma.

For this, we fix $d\geq 0$ such that $d\not\equiv i \bmod p-1$, and set $k:=d+2$, so that $(\chi\omega^{i-d})_1=\chi\omega^{i-d}$. Let $H_k^{(Np)}(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}}$ be the $\mathfrak{r}$-subalgebra of $H_k(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}}$ generated by $T(l)$ with prime numbers $l\nmid Np$.

LEMMA 4.1.3. *We can take a basis of* $M_k(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}} \otimes_{\mathfrak{r}} \overline{\boldsymbol{Q}}_p$ *whose members consist of common eigenforms of all* $T(n)$.

PROOF. It is enough to show the same assertion for the subspace of cusp forms.

The Hecke algebra $H_k^{(Np)}(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}}$ acts semi-simply on $S_k(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}} \otimes_{\mathfrak{r}} \overline{\boldsymbol{Q}}_p$. Let f be a common eigenform of $H_k^{(Np)}(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}}$ in this space. Then, fixing an embedding $\overline{\boldsymbol{Q}} \hookrightarrow \overline{\boldsymbol{Q}}_p$, there is a primitive form $f^0 \in S_k(\Gamma_1(Np);\overline{\boldsymbol{Q}})$ having the same eigenvalues as f for all elements in $H_k^{(Np)}(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}}$. If the conductor of f^0 is c, f is a linear combination of $f^0(tz)$ with positive divisors t of Np/c.

Now every element of $M_k(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}}$ has the same Nebentypus character (cf. loc. cit.), and it must be $\chi\omega^{i-d}$, the character of $E_k(\chi\omega^{i-d},\mathbf{1})$. The same holds for f^0, and hence $c = Np$. □

We thus take a basis $f_0, f_1, \cdots, f_m$ of $M_k(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}} \otimes_{\mathfrak{r}} \overline{\boldsymbol{Q}}_p$ as in the lemma, with $f_0 = E_k(\chi\omega^{i-d},\mathbf{1})$ and with f_j cusp forms for $j \geq 1$. We assume that $a(1;f_j) = 1$ for each j.

Let F_j be the extension of F generated by $a(n;f_j)$ $(n \geq 0)$. We denote by $\mathfrak{r}_j$ the ring of integers of F_j, and let ϖ_j be a prime element of $\mathfrak{r}_j$. Then we have the congruences:

$$a(n;f_j) \equiv a(n;f_0) \mod \varpi_j \quad \text{for all } n \geq 1 \tag{4.1.4}$$

and hence especially

$$a(q;f_j) \equiv 1 \mod \varpi_j \quad \text{for any prime divisor } q \text{ of } Np. \tag{4.1.5}$$

For $j \geq 1$, let

$$\rho_j : \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q}) \to GL_2(F_j) \tag{4.1.6}$$

be Deligne's p-adic representation associated with f_j. Namely, it is unramified outside Np, and if Φ_l is a *geometric* Frobenius at a prime $l \nmid Np$, we have

$$\det(X - \rho_j(\Phi_l)) = X^2 - a(l;f_j)X + l^{k-1}(\chi\omega^{i-d})(l). \tag{4.1.7}$$

We will denote by κ the p-cyclotomic character of $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$. For $j = 0$, we simply define

$$\rho_0 : \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q}) \to GL_2(F) \text{ by } \rho_0 = \begin{bmatrix} (\chi\omega^{i-d})^{-1}\kappa^{1-k} & 0 \\ 0 & 1 \end{bmatrix}. \tag{4.1.8}$$

This representation clearly satisfies (4.1.7) for f_0.

Set

$$\mathfrak{R} := \mathfrak{r}_0 \oplus \cdots \oplus \mathfrak{r}_m. \tag{4.1.9}$$

It follows from the previous lemma that $H_k(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}}$ is isomorphic to the subring $\mathfrak{R}_1$ of $\mathfrak{R}$ generated over $\mathfrak{r}$ by $(a(l;f_0),\cdots,a(l;f_m))$ for all prime numbers l. On the other hand, by the relation (4.1.7) and the Čebotarev density theorem, $H_k^{(Np)}(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}}$ corresponds to the subring $\mathfrak{R}_2$ of $\mathfrak{R}_1$ generated over $\mathfrak{r}$ by $(\operatorname{tr}\rho_0(\sigma),\cdots,\operatorname{tr}\rho_m(\sigma))$ for all $\sigma\in\operatorname{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$, via this isomorphism.

LEMMA 4.1.10. *Let q be a prime factor of N. Then $H_k^{(Np)}(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}}$ contains $T(q)$.*

PROOF. We first consider f_j with $j\geq 1$, keeping in mind that its conductor is exactly Np. Let $\pi_j=\otimes_{l\leq\infty}\pi_{j,l}$ be the automorphic representation of $GL_2(\boldsymbol{Q}_{\boldsymbol{A}})$ associated with f_j. By (4.1.5), the L-function of f_j has a non-trivial Euler factor at q, but the character $\chi\omega^{i-d}$ of f_j ramifies at q. It follows that the local representation $\pi_{j,q}$ is a principal series representation (cf. Mazur and Wiles [**MW**, Chapter 3, Section 2, Proposition 2]). Then by a result of Langlands [**L**], the restriction of ρ_j to a decomposition group D_q of (some prime above) q is of the form:

$$\rho_j\mid_{D_q}\cong\begin{bmatrix}\mu_1 & 0\\ 0 & \mu_2\end{bmatrix}=:\rho'_{j,q}$$

with μ_1 (resp. μ_2) ramified (resp. unramified), and moreover the local Euler factor corresponding to this representation coincides with that of f_j, i.e. $a(q;f_j)=\mu_2(\Phi_q)$.

Since $\det\rho_j=(\chi\omega^{i-d})^{-1}\kappa^{1-k}$ by (4.1.7), there is an element σ_q of the inertia subgroup I_q of D_q such that $\mu_1(\sigma_q)=\chi^{-1}(\sigma_q)\neq 1$, or equivalently $\chi(\sigma_q)-1\in\mathfrak{r}^{\times}$. We then have:

$$\rho'_{j,q}(\Phi_q)=\begin{bmatrix}\mu_1(\Phi_q) & 0\\ 0 & a(q;f_j)\end{bmatrix}\quad\text{and}\quad\rho'_{j,q}(\Phi_q\sigma_q)=\begin{bmatrix}\mu_1(\Phi_q)\chi^{-1}(\sigma_q) & 0\\ 0 & a(q;f_j)\end{bmatrix}.$$

Clearly, the same holds for ρ_0. Consequently, we have

$$(\chi(\sigma_q)-1)(a(q;f_0),\cdots,a(q;f_m))\in\mathfrak{R}_2$$

which completes the proof. □

The proof of Proposition 4.1.1 will be complete with the following

LEMMA 4.1.11. *The algebra $H_k^{(Np)}(\Gamma_1(Np);\mathfrak{r})_{\mathfrak{m}}$ contains $T(p)$.*

PROOF. Instead of Langlands' result, we make use of a result of Wiles [**Wi1**]. Namely, by Theorem 2.1.4, loc. cit., we have

$$\rho_j\mid_{D_p}\cong\begin{bmatrix}\varepsilon_1 & 0\\ * & \varepsilon_2\end{bmatrix}=:\rho'_{j,p}$$

with ε_2 unramified and $\varepsilon_2(\Phi_p) = a(p; f_j)$ for $j \geq 1$. (According to our convention (4.1.7), the representation ρ_j is contragredient to the one in [**Wi1**].) The same holds trivially for ρ_0.

There is an element $\sigma_p \in I_p$ such that $\det \rho_j(\sigma_p) = \omega^{d-i}(\sigma_p) \neq 1$, and thus

$$\rho'_{j,p}(\sigma_p) = \begin{bmatrix} \omega^{d-i}(\sigma_p) & 0 \\ * & 1 \end{bmatrix}.$$

The rest of the proof then proceeds in the same way as in the previous lemma. □

From the proposition we have just proved, we obtain

COROLLARY 4.1.12. *The Eisenstein ideal* $\mathscr{I}_{\mathfrak{M}} = \mathscr{I}(\vartheta, \mathbf{1})_{\mathfrak{M}}$ *of* $e\,\mathscr{H}(N; \mathfrak{r})_{\mathfrak{M}}$ *is generated by* $T(l) - (1 + \vartheta(l)A_l(T))$ *with primes* l *not dividing* Np.

4.2. Proof of Theorem II.

We are now going to describe the proof of Theorem II in the introduction. This is indeed a repetition of the arguments already appeared in our previous works. We will be thus brief when they can be found elswehere. The method is due to Harder and Pink [**HP**] and Kurihara [**Ku**].

We consider the Galois representation on

$$\begin{cases} e^* ES_p(N)_{\mathfrak{r}} = e^* \left(\varprojlim_{r \geq 1} H^1_{\text{ét}}(X_1(Np^r)_{/\boldsymbol{Q}} \otimes_{\boldsymbol{Q}} \overline{\boldsymbol{Q}}, \boldsymbol{Z}_p) \otimes_{\boldsymbol{Z}_p} \mathfrak{r} \right), \\ e^* GES_p(N)_{\mathfrak{r}} = e^* \left(\varprojlim_{r \geq 1} H^1_{\text{ét}}(Y_1(Np^r)_{/\boldsymbol{Q}} \otimes_{\boldsymbol{Q}} \overline{\boldsymbol{Q}}, \boldsymbol{Z}_p) \otimes_{\boldsymbol{Z}_p} \mathfrak{r} \right). \end{cases} \tag{4.2.1}$$

On individual cohomology groups in the right-hand sides, we let Hecke correspondences act covariantly, and use the notation $T^*(n)$ for the n-th Hecke operators acting on these groups. We denote by the same symbol $T^*(n)$ the endomorphisms of the groups in the parentheses determined by such $T^*(n)$'s. The symbol e^* then stands for Hida's idempotent attached to $T^*(p)$. As in our previous works (cf. [**O3**, 1.2]), we denote by $e^* h^*(N; \mathfrak{r})$ and $e^* \mathscr{H}^*(N; \mathfrak{r})$ Hida's Hecke algebras acting on the above cohomology groups, respectively. These algebras are generated over $\Lambda_{\mathfrak{r}}$ by all $T^*(n)$, and in fact canonically $\Lambda_{\mathfrak{r}}$-isomorphic to $e\,h(N; \mathfrak{r})$ and $e\,\mathscr{H}(N; \mathfrak{r})$ via the correspondence $T^*(n) \leftrightarrow T(n)$, respectively.

Now let the notation and the assumption be as in the beginning of this section, with $\mathfrak{r}$ the ring generated by the values of ϑ over $\boldsymbol{Z}_p$. We denote by $\mathfrak{M}^*$ and $\mathscr{I}^*$ the ideals of $e^* \mathscr{H}^*(N; \mathfrak{r})$ corresponding to $\mathfrak{M} = \mathfrak{M}(\vartheta, \mathbf{1})$ and $\mathscr{I} = \mathscr{I}(\vartheta, \mathbf{1})$ via the isomorphism above, and let I (resp. I^*) be the image of $\mathscr{I}_{\mathfrak{M}}$ (resp. $\mathscr{I}^*_{\mathfrak{M}^*}$) in $e\,h(N; \mathfrak{r})_{\mathfrak{M}}$ (resp. $e^*\,h^*(N; \mathfrak{r})_{\mathfrak{M}^*}$).

For notational simplicity, we set

$$\begin{cases} \mathfrak{h}^* := e^* h^*(N;\mathfrak{r})_{\mathfrak{M}^*}, \\ \mathfrak{H}^* := e^* \mathscr{H}^*(N;\mathfrak{r})_{\mathfrak{M}^*}, \\ X := e^* ES_p(N)_{\mathfrak{r},\mathfrak{M}^*}, \\ Y := e^* GES_p(N)_{\mathfrak{r},\mathfrak{M}^*}. \end{cases} \tag{4.2.2}$$

We then have

$$\mathfrak{h}/I \cong \mathfrak{h}^*/I^* \cong \Lambda_{\mathfrak{r}}/(G(T,\vartheta\omega^2)) \tag{4.2.3}$$

([**O3**, (1.5.5) and 3.2]). We henceforth assume that $G(T,\vartheta\omega^2) \notin \Lambda_{\mathfrak{r}}^{\times}$ for otherwise $\mathfrak{h}^*$ is a zero-ring (cf. the proof of Lemma 2.1.11) and $\mathrm{Gal}(L_\infty/K_\infty)_{(\vartheta\omega)^{-1}}$ in the introduction vanishes.

We know that

$$X^{I_p} = Y^{I_p} =: X_+ \tag{4.2.4}$$

is free of rank one over $\mathfrak{h}^*$, and

$$\begin{cases} X/X_+ \cong \mathrm{Hom}_{\Lambda_{\mathfrak{r}}}(\mathfrak{h}^*, \Lambda_{\mathfrak{r}}) \\ Y/X_+ \cong \mathrm{Hom}_{\Lambda_{\mathfrak{r}}}(\mathfrak{H}^*, \Lambda_{\mathfrak{r}}) \end{cases} \tag{4.2.5}$$

as modules over $\mathfrak{h}^*$ and $\mathfrak{H}^*$, respectively ([**O2**, (2.3.6)] and [**O4**, Lemma 3.4.4]).

From now on, we assume that $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$, or equivalently $\mathfrak{H}^*$, is Gorenstein, so that Y/X_+ is free of rank one over $\mathfrak{H}^*$. Set

$$\widetilde{X} := Y \otimes_{\mathfrak{H}^*} \mathfrak{h}^* \tag{4.2.6}$$

and consider the diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_+ & \longrightarrow & X & \longrightarrow & X/X_+ & \longrightarrow & 0 \quad \text{(exact)} \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & X_+ & \longrightarrow & \widetilde{X} & \longrightarrow & (Y/X_+) \otimes_{\mathfrak{H}^*} \mathfrak{h}^* & \longrightarrow & 0 \quad \text{(split)}. \end{array} \tag{4.2.7}$$

The $\mathfrak{H}^*$-module Y/X is isomorphic to $\mathscr{C}_p(N)_{\mathfrak{r},\mathfrak{M}^*}$ in the notation of [**O1**, 4.3], and by [**O3**, (2.3.6) and (3.1.2)], this is isomorphic to $\mathfrak{H}^*/\mathscr{I}^*$. We then see that the $\mathfrak{h}^*$-module $\mathrm{Coker}(X \to \widetilde{X})$ is isomorphic to $\mathfrak{h}^*/I^*$, and the two vertical arrows in (4.2.7) are injective.

We can give a natural splitting of the lower exact sequence in (4.2.7): If $i \not\equiv -1 \bmod p-1$, we choose $\sigma_0 \in I_p$ in such a way that $\kappa(\sigma_0) = \omega(\sigma_0)$ and $\omega^{-i-1}(\sigma_0) \neq 1$, and let $\widetilde{X}_-$ be the eigensubspace of $\widetilde{X}$ on which σ_0 acts as $\omega^{-i-1}(\sigma_0)$. If, on the other hand, $i \equiv -1 \bmod p-1$, we choose a geometric Frobenius Φ_p in such a way that $\kappa(\Phi_p) = 1$, and let $\widetilde{X}_-$

be the eigensubspace of $\widetilde{X}$ on which Φ_p acts as $\chi(p)T^*(p)^{-1}$. This $\widetilde{X}_-$ gives the desired splitting image of $(Y/X_+)\otimes_{\mathfrak{H}^*}\mathfrak{h}^*$ (cf. [**O3**, 3.4]). In the same manner, we can define $X_-\subseteq X$ and split the upper exact sequence in (4.2.7).

We therefore have

$$\widetilde{X}=\widetilde{X}_-\oplus X_+\cong\mathfrak{h}^{*\oplus 2} \tag{4.2.8}$$

and get a representation

$$\widetilde{\rho}:\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})\to GL_{\mathfrak{h}^*}(\widetilde{X})\cong GL_2(\mathfrak{h}^*). \tag{4.2.9}$$

Write $\widetilde{\rho}(\sigma)=\begin{bmatrix}\widetilde{a}(\sigma) & \widetilde{b}(\sigma)\\ \widetilde{c}(\sigma) & \widetilde{d}(\sigma)\end{bmatrix}$, and denote by $\widetilde{B}$ (resp. $\widetilde{C}$) the ideal of $\mathfrak{h}^*$ generated by all $\widetilde{b}(\sigma)$ (resp. $\widetilde{c}(\sigma)$). We have

$$\begin{cases}\widetilde{a}(\Phi_l)+\widetilde{d}(\Phi_l)=T^*(l)\text{ for any prime }l\nmid Np,\\ \det\widetilde{\rho}(\sigma)=(\vartheta\omega)^{-1}(\sigma)(\kappa\omega^{-1})(\sigma)^{-1}\iota((\kappa\omega^{-1})(\sigma))^{-1}\end{cases} \tag{4.2.10}$$

(cf. [**O2**, (5.1.5)]) where ι is the natural inclusion mapping from $1+p\boldsymbol{Z}_p$ to its completed group algebra $\Lambda_{\mathfrak{r}}$.

Noting that

$$\begin{cases}\widetilde{\rho}(\sigma_0)=\begin{bmatrix}\omega^{-i-1}(\sigma_0) & 0\\ 0 & 1\end{bmatrix}\text{ if }i\not\equiv -1\bmod p-1,\\ \widetilde{\rho}(\Phi_p)=\begin{bmatrix}\chi(p)T^*(p)^{-1} & 0\\ 0 & T^*(p)\end{bmatrix}\equiv\begin{bmatrix}\chi(p) & 0\\ 0 & 1\end{bmatrix}\bmod I^*\text{ if }i\equiv -1\bmod p-1\end{cases} \tag{4.2.11}$$

we see that $\{\widetilde{a}(\sigma)-\det\widetilde{\rho}(\sigma)\mid\sigma\in\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})\}$ and $\{\widetilde{d}(\sigma)-1\mid\sigma\in\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})\}$ are contained in I^* and generate the same ideal of $\mathfrak{h}^*$ (cf. [**HP**, Section 3], [**Ku**, Section 3]). This ideal contains $T^*(l)-(1+\vartheta(l)lu(l\omega^{-1}(l)))=T^*(l)-(1+\vartheta(l)A_l(T))$ for any $l\nmid Np$, so that it coincides with I^* by Corollary 4.1.12. It follows that $\widetilde{B}\widetilde{C}=I^*$ for the same reason as [**O1**, (5.3.13)], and furthermore that $\widetilde{B}=I^*$ and $\widetilde{C}=\mathfrak{h}^*$ (cf. [**O4**, (3.4.10)]).

Therefore,

$$\sigma\mapsto\begin{bmatrix}\det\widetilde{\rho}(\sigma)\bmod I^* & \widetilde{b}\bmod I^{*2}\\ 0 & 1\end{bmatrix} \tag{4.2.12}$$

gives a representation of $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$ into the multiplicative group $\{\begin{bmatrix}a & b\\ 0 & 1\end{bmatrix}\mid a\in(\mathfrak{h}/I^*)^\times, b\in I^*/I^{*2}\}$. If $\mathscr{K}$ is the subfield of $\overline{\boldsymbol{Q}}$ corresponding to this representation, we obtain that $\mathrm{Gal}(\mathscr{K}K_\infty/K_\infty)=\mathrm{Gal}(L_\infty/K_\infty)_{(\vartheta\omega)^{-1}}$, and also that this Iwasawa module is isomorphic to $(I^*/I^{*2})^\dagger$ (cf. [**O4**, Theorem 3.4.12]). This settles our Theorem II.

As in [**O4**, Corollary 3.4.14], we obtain the following corollary to this theorem:

COROLLARY 4.2.13. *Let the hypothesis be as in Theorem II, and assume that* $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ *is Gorenstein. Then the following conditions are equivalent*:

(i) $\mathrm{Gal}(L_\infty/K_\infty)_{(\vartheta\omega)^{-1}}$ *is a cyclic* $\Lambda_{\mathfrak{r}}$*-module*;
(ii) $e\,h(N;\mathfrak{r})_{\mathfrak{M}}$ *is a Gorenstein ring*;
(iii) $e\,h(N;\mathfrak{r})_{\mathfrak{M}}$ *is a complete intersection*;
(iv) $\mathscr{I}(\theta,\mathbf{1})_{\mathfrak{M}}$ *is a principal ideal of* $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$;
(v) I *is a principal ideal of* $e\,h(N;\mathfrak{r})_{\mathfrak{M}}$.

PROOF. That (i) $\Rightarrow$ (v) is an immediate consequence of Theorem II. That (iv) $\Leftrightarrow$ (v) $\Rightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) holds without assuming that $e\mathscr{H}(N;\mathfrak{r})_{\mathfrak{M}}$ is Gorenstein.

Here, the only non-trivial implication is "(ii) $\Rightarrow$ (i)", which is essentially due to Harder, Pink and Kurihara. In [**O4**], we derived this using [**O1**, (5.2.16)], i.e. the existence of a $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$- and $\mathfrak{h}^*$-submodule of $X_-/G(T,\vartheta\omega^2)$ isomorphic to $\mathfrak{h}^*/I^* \cong \Lambda_{\mathfrak{r}}/(G(T,\vartheta\omega^2))$, proved when $i \not\equiv 0,\ -1 \bmod p-1$. Although the same proof works in the present case, here is a simpler argument: Consider the exact sequence

$$0 \to X \xrightarrow{i} Y \xrightarrow{\pi} Y/X \to 0$$

of $\mathfrak{H}^*$- and $\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q})$-modules. This sequence splits uniquely as $\mathfrak{H}^*$-modules when tensored with the quotient field $\mathscr{L}_{\mathfrak{r}}$ of $\Lambda_{\mathfrak{r}}$:

$$0 \leftarrow X \otimes_{\Lambda_{\mathfrak{r}}} \mathscr{L}_{\mathfrak{r}} \xleftarrow{t} Y \otimes_{\Lambda_{\mathfrak{r}}} \mathscr{L}_{\mathfrak{r}} \xleftarrow{s} (X/Y) \otimes_{\Lambda_{\mathfrak{r}}} \mathscr{L}_{\mathfrak{r}} \leftarrow 0 \quad \text{(exact)}.$$

By the uniqueness, this latter sequence is also compatible with the Galois action. The associated congruence module:

$$t(Y)/X \underset{\sim}{\xleftarrow{t}} Y/(i(X) + Y \cap s(X/Y)) \underset{\sim}{\xrightarrow{\pi}} (Y/X)/\pi(Y \cap s(X/Y))$$

(cf. [**O3**, (1.1.4)]) is isomorphic to $\mathfrak{h}^*/I^*$ ([**O3**, (1.5.5)]), and $\sigma_0 \in I_p$ (resp. Φ_p such that $\kappa(\Phi_p) = 1$) acts as $\omega^{-i-1}(\sigma_0)$ (resp. $\chi(p)T^*(p)^{-1}$) when $i \not\equiv -1 \bmod p-1$ (resp. $i \equiv -1 \bmod p-1$) on this module ([**O3**, 3.4]). Since $t(Y)$, being a submodule of $X \otimes_{\Lambda_{\mathfrak{r}}} \mathscr{L}_{\mathfrak{r}}$, is $\Lambda_{\mathfrak{r}}$-torsion free, our claim follows from the snake lemma applied to the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X & \longrightarrow & t(Y) & \longrightarrow & t(Y)/X & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \times G(T,\vartheta\omega^2)} & & \downarrow{\scriptstyle \times G(T,\vartheta\omega^2)} & & \downarrow{\scriptstyle \times 0} & & \\
0 & \longrightarrow & X & \longrightarrow & t(Y) & \longrightarrow & t(Y)/X & \longrightarrow & 0.
\end{array}$$

We can then proceed in the same way as in [**O4**] to show that (ii) $\Rightarrow$ (i). $\square$

References

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

[Go] F. Gouvêa, On the ordinary Hecke algebra, J. Number Theory, **41** (1992), 178–198.

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

[HP] G. Harder and R. Pink, Modular konstruierte unverzweigte abelsche p-Erweiterungen von $\boldsymbol{Q}(\zeta_p)$ und die Struktur ihrer Galoisgruppen, Math. Nachr., **159** (1992), 83–99.

[Hi] H. Hida, Iwasawa modules attached to congruences of cusp forms, Ann. Sci. École Norm. Sup. (4), **19** (1986), 231–273.

[Ka1] 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.

[Ka2] N. Katz, A result on modular forms in characteristic p, In: Modular functions of one variable V, Lecture Notes in Math., **601** (1977), 53–61.

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

[Ku] M. Kurihara, Ideal class groups of cyclotomic fields and modular forms of level 1, J. Number Theory, **45** (1993), 281–294.

[L] R. P. Langlands, Modular forms and ℓ-adic representations, In: Modular functions of one variable II, Lecture Notes in Math., **349** (1973), 361–500.

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of **Q**, Invent. Math., **76** (1984), 179–330.

[O1] M. Ohta, Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves, Compos. Math., **115** (1999), 241–301.

[O2] M. Ohta, Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves. II, Math. Ann., **318** (2000), 557–583.

[O3] M. Ohta, Congruence modules related to Eisenstein series, Ann. Sci. École Norm. Sup. (4), **36** (2003), 225–269.

[O4] M. Ohta, Companion forms and the structure of p-adic Hecke algebras, J. Reine Angew. Math., **585** (2005), 141–172.

[R] G. Robert, Congruences entre séries d'Eisenstein, dans le cas supersingulier, Invent. Math., **61** (1980), 103–158.

[S1] J.-P. Serre, Résumé des cours de 1987–1988, Annuaire du Collège de France (1988), 79–82 (Œuvres IV, No. 145).

[S2] J.-P. Serre, Two letters on quaternions and modular forms (mod p), Israel J. Math., **95** (1996), 281–299 (Œuvres IV, No. 169).

[SW] C. Skinner and A. Wiles, Ordinary representations and modular forms, Proc. Natl. Acad. Sci. USA, **94** (1997), 10520–10527.

[U1] D. Ulmer, p-descent in characteristic p, Duke Math. J., **62** (1991), 237–265.

[U2] D. Ulmer, On the Fourier coefficients of modular forms. II, Math. Ann., **304** (1996), 363–422.

[Wa] L. Washington, Introduction to cyclotomic fields, Grad. Texts in Math., **83** (1982).

[Wi1] A. Wiles, On ordinary λ-adic representations associated to modular forms, Invent. Math., **94** (1988), 529–573.

[Wi2] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2), **141** (1995), 443–551.

Masami Ohta

Department of Mathematics
Faculty of Science
Tokai University
Hiratsuka, Kanagawa, 259-1292, Japan
E-mail: ohta@sm.u-tokai.ac.jp