Congruences between modular forms and functions and applications to the conjecture of Atkin

By Masao KOIKE

(Communicated by Y. Ihara)

We shall prove some congruence relations mod p^{α} between the Fourier coefficients of cusp forms of weight $p^{\alpha}-p^{\alpha-1}$ with respect to $\Gamma=SL(2, \boldsymbol{Z})$ and those of some modular functions with respect to $\Gamma_0(p)$ (Main Theorem, §6). This generalizes Newman [11] where $p=13$, and $\alpha=1$, and enables us to reduce the conjecture of Atkin [2] on the Fourier coefficients of $J(\tau)$ to the "p-separability" in weight $p-1$, and some "p-vanishing" property in weight $p^{\alpha}-p^{\alpha-1}$ $(\alpha>1)$ of the eigenvalues of the Hecke operator $T(p)$ in the space of cusp forms with respect to Γ (Theorem 3, §8). As a corollary, we can prove some new cases of this conjecture for $\alpha=1$. In §§7, 8, we shall discuss the "p-adic eigenfunctions" of the "p-adic Hecke operators".

Our results are based on the following two facts: (i) there exists an algebraic equivalent of $q^{-1}dq$ $(q=e^{2\pi\sqrt{-1}\tau})$ in the p-adic completion of some unramified algebraic extension of the modular function field, and there is an algebraic formula for $(p^{-1}dq)^{\frac{p-1}{2}}$ (mod. p) (Ihara [8], [9]), (ii) the p-adic rigidity of the function $J(\tau) \to J(p\tau)$, conjectured by Tate and proved by Deligne. Tate predicted that this rigidity might be essential in proving Atkin's conjecture.

Recently, it is reported that Dwork solves the conjecture of Atkin, however, the detail is not known and the relation to this paper is not clear.

The author wishes to express his hearty thanks to Prof. Y. Ihara for suggesting this problem as well as for his encouragement during the preparation of the present paper.

Notations.

$\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$: the rational integers, the rational numbers, the real numbers and the complex numbers.

$\boldsymbol{Q}_p$, $\boldsymbol{Q}_p^{\infty}$, $\mathfrak{o}_p^{\infty}$, $\mathfrak{p}$: the p-adic numbers, the completion of the maximum unramified extension of $\boldsymbol{Q}_p$, the valuation ring of $\boldsymbol{Q}_p^{\infty}$, the maximal ideal of $\mathfrak{o}_p^{\infty}$.

$\boldsymbol{F}_p$, $\bar{\boldsymbol{F}}_p$: the finite field with p elements, the algebraic closure of $\boldsymbol{F}_p$.

Contents

PART I. CONGRUENCES BETWEEN MODULAR FORMS AND FUNCTIONS

1. Statement of Main Theorem

We shall fix a prime number p once and for all. Let $\mathfrak{H}$ be the complex upper half plane; $\mathfrak{H}=\{\tau\in \boldsymbol{C} \mid \operatorname{Im}\tau>0\}$. Denote by $\mathfrak{N}$ the space of all meromorphic functions on $\mathfrak{H}$ that are invariant under the translation $\tau\to\tau+1$. Define the operators $U(p)$ and $T_k(p^n)$ on $\mathfrak{N}$ for each k, $n=0, 1, \cdots$, by

$$(1) \qquad F(\tau)\mid U(p)=p^{-1}\sum_{\lambda=0}^{p-1} F\left(\frac{\tau+\lambda}{p}\right),$$

$$(2) \qquad F(\tau)\mid T_k(p^n)=p^{n(k-1)}\sum_{\substack{ad=p^n\\ d>0\\ b \bmod d}} F\left(\frac{a\tau+b}{d}\right)d^{-k} \quad \text{for} \quad F(\tau)\in\mathfrak{N}\,.$$

It follows immediately from the definitions that

$$(3) \qquad F(\tau)\mid U(p)^n=F(\tau)\mid T_k(p^n)-p^{k-1}(F(\tau)\mid T_k(p^{n-1}))_{\tau\to p\tau}$$

holds for any $F(\tau)\in\mathfrak{N}$.

Let $\Gamma=SL(2, \boldsymbol{Z})$ be the modular group acting on $\mathfrak{H}$ by

$$\tau\to g\cdot\tau=\frac{a\tau+b}{c\tau+d}\,, \quad \text{for} \quad g=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma\,.$$

Let $J(\tau)$ be Klein's modular function. It has a Fourier expansion

$$(4) \qquad J(\tau)=\sum_{n=-1}^{\infty} c(n)\cdot q^n \quad \text{with } c(-1)=1,\ c(n)\in Z, \text{ and } q=e^{2\pi\sqrt{-1}\tau}\,.$$

The modular function field $\mathfrak{M}$ with respect to Γ is the rational function field generated by $J(\tau)$: $\mathfrak{M}=C(J(\tau))$. Put $\Gamma_0(p)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma \mid c\equiv 0 \pmod p\right\}$. Then the modular function field with respect to $\Gamma_0(p)$ is given by $C(J(\tau), J(p\tau))$.

LEMMA 1. *For each $f\in\mathfrak{M}$, $f\mid U(p)^n$ is a modular function with respect to $\Gamma_0(p)$.*

PROOF. Since $\mathfrak{M}=C(J(\tau))$, we may put $f=H(J(\tau))$ with $H(X)\in C(X)$. As is well-known, $T_0(p^n)$ operates on $\mathfrak{M}$; hence $f\mid T_0(p^n)=H_n(J(\tau))$ with some $H_n(X)\in C(X)$. From (3), $f\mid U(p)^n=H_n(J(\tau))-p^{-1}H_{n-1}(J(p\tau))$. q.e.d.

We consider the Z-module M generated by $\{f\mid U(p)^n\,;f\in Z[J(\tau)], n\geqq 0\}$. By Lemma 1, M is a submodule of the modular function field with respect to $\Gamma_0(p)$. Denote by $\mathfrak{S}_k$ the space of cusp forms of weight k with respect to Γ, and by $\mathfrak{S}_{k,Z}$ the submodule of $\mathfrak{S}_k$ consisting of all elements of $\mathfrak{S}_k$ whose Fourier coefficients are rational integers. We define the notion of congruences mod p^α between cusp forms and functions as follows. Let $Q\{q\}$ be the power series field with coefficients in Q, and let $Q\{q\}_Z$ be the set of all elements in $Q\{q\}$ whose coefficients are rational integers. Then two elements $f=\sum_{n\geqq N} a_nq^n$ and $f'=\sum_{n\geqq N} a'_nq^n$ of $Q\{q\}_Z$ will be called congruent modulo p^α if and only if $a_n\equiv a'_n \pmod{p^\alpha}$ hold for all n. By Fourier expansions with respect to q, M and $\mathfrak{S}_{k,Z}$ will be canonically imbedded in $Q\{q\}_Z$.

Now our Main Theorem reads as follows;

MAIN THEOREM. *Let α be a positive integer. Then, for each $g\in M$, there exist $h\in Z[J(\tau)]$ and $F(\tau)\in\mathfrak{S}_{p^\alpha-p^{\alpha-1},Z}$ such that*

$$g-h\equiv F(\tau) \pmod{p^\alpha}\ .$$

These h and $F(\tau)$ are unique up to modulo p^α.

In particular, if we put $p=13$, $\alpha=1$, $g=J(\tau)\mid U(13)=\sum_{n=0}^{\infty} c(13n)\cdot q^n$ in this theorem, we obtain an alternative proof for the classical result of Newman [11]. In fact,

$$g-c(0)\equiv c(13)\Delta(\tau) \pmod{13}\ .$$

Therefore $c(13n)\equiv -\tau(n) \pmod{13}$ for $\Delta(\tau)=\sum_{n=1}^{\infty}\tau(n)\cdot q^n$, since $c(13)\equiv -1 \pmod{13}$.

2. Preliminaries on valued differential fields and associated differentials

Here we explain the general theory of the valued differential fields and the associated differentials with respect to p^f-th Frobenius maps according to Ihara's note [8].

Let K be a field and let $D(K)$ be a one dimensional vector space over K. Let

d be a differentiation from K to $D(K)$ which, by definition, satisfies

$$d(x+y)=dx+dy\ , \qquad d(xy)=ydx+xdy\ , \qquad \text{for } x,\ y\in K.$$

The kernel of d is a subfield of K and it will be denoted by k. Suppose that these objects have the following properties; v is a discrete, additive and normalized valuation of k, and V is a discrete valuation of K extending v, assumed to have the same value group as v. Let $\bar{K}$ denote the residue field of K with respect to V. Also suppose that K and $\bar{K}$ have the unequal characteristics and that d is continuous with respect to the V-adic topology of K and of $D(K)$. We call such a collection of objects $\{K, D(K), d, V\}$ a *valued differential field*. Examples of valued differential fields will be given in §§3, 4. Let $\{K_i, D(K_i), d_i, V_i\}$ $(i=1, 2)$ be valued differential fields. We call $\{K_1, D(K_1), d_1, V_1\}$ is an extension of $\{K_2, D(K_2), d_2, V_2\}$ if the followings are satisfied; K_2 is a subfield of K_1, $D(K_2)$ is a vector subspace of $D(K_1)$, and the restriction of d_1 (resp. V_1) to K_2 coincides with d_2 (resp. V_2).

For each positive integer h, let $D^h(K)$ denote the tensor product of h copies of $D(K)$ over K. Put $D^0(K)=K$. We define a reduction of $D^h(K)$ as follows; $\mathfrak{O}$ will denote the valuation ring of K with respect to V and $\mathfrak{P}$ will denote the maximal ideal of $\mathfrak{O}$. The continuity of d implies that the $\mathfrak{O}$-submodule of $D(K)$ generated by the set $\{dx|x\in\mathfrak{O}\}$ is a free $\mathfrak{O}$-module of rank 1. Denote this module by $D(\mathfrak{O})$. Now we extend the valuation V to a $Z\cup\{\infty\}$ valued function on $\bigcup_{h\geqq 0} D^h(K)$ satisfying the following conditions;

$$V(\xi\otimes\eta)=V(\xi)+V(\eta)\ , \qquad \text{for any } \xi,\ \eta\in \bigcup_{h\geqq 0} D^h(K)\ ,$$

$$V(dx)=0\ , \qquad \text{for any } dx \text{ such that } D(\mathfrak{O})=\mathfrak{O}dx\ .$$

With the above condition, V is uniquely determined. Put $D^h(\mathfrak{O})=\{\xi\in D^h(K)|\ V(\xi)\geqq 0\}$, and $D^h(\mathfrak{P})=\mathfrak{P}D^h(\mathfrak{O})$. Then $D^h(\mathfrak{O})/D^h(\mathfrak{P})$ is a one dimensional vector space over $\bar{K}$. Denote it $D^h(\bar{K})$ and put $D(\bar{K})=D^1(\bar{K})$. Then $D^0(\bar{K})=\bar{K}$ and $D^h(\bar{K})$ $(h\geqq 1)$ can be identified naturally with the tensor product of h copies of $D(\bar{K})$ over $\bar{K}$. For each $\xi\in D^h(\mathfrak{O})$, $\bar{\xi}$ denotes the residue class modulo $D^h(\mathfrak{P})$.

The V-adic completion of $\{K, D(K), d, V\}$ will be defined as follows. Let K_V be the completion of K, and consider K as a subfield of K_V naturally. Put $D(K_V)=D(K)\otimes K_V$ (over K), and identify $\xi\in D(K)$ with $\xi\otimes 1\in D(K_V)$. By the continuity of d, we can extend d to the unique differentiation $d_V: K_V\rightarrow D(K_V)$. Then $\{K_V, D(K_V), d_V, V\}$ is a valued differential field. Let k_V denote the kernel of d_V (in general, k_V does not coincide with the completion of k with respect to v).

Suppose we are given a valued differential field $\{K, D(K), d, V\}$. Let $\mathrm{ch}\,(\bar{K})$

$=p>0$, and let p^f be fixed positive power of p. We shall always consider K as a subfield of K_V, identifying in particular the residue field of K_V with that of K. Now we define a *p^f-th Frobenius map* σ by an injective isomorphism from K to K_V such that the following two conditions are satisfied;

(σ-1) σ is V-preserving and induces the p^f-th power map of the residue field.

(σ-2) σ commutes with the differentiation, namely, $k^\sigma \subset k_V$, $(K-k)^\sigma \subset K_V - k_V$, and

$$\left(\frac{dx}{dy}\right)^\sigma = \left(\frac{d_V x^\sigma}{d_V y^\sigma}\right), \quad \text{for any } x,\ y \in K-k\ .$$

Examples of p^f-th Frobenius map will be given in §§3, 4. For each $h \geqq 0$, $D^h(K)$ is canonically imbedded into $D^h(K_V)$ and σ induces a map from $D(K)$ to $D^h(K_V)$ by $(y(dx)^h)^\sigma = y^\sigma(d_V x^\sigma)^h$. This is well defined by (σ-2).

Let $\sigma: K \to K_V$ be a p^f-th Frobenius map. A differential $\omega \in D(K)$ is called *an associated differential* (with respect to σ) if $\omega^\sigma/\omega \in k^\times$.

About the existence and the uniqueness of ω, the following result is known.

THEOREM A (Ihara). *Let $\{K, D(K), d, V\}$ be a valued differential field. Let k be a kernel of d, and v be a valuation of k induced by V. Let $\sigma: K \to K_V$ be a p^f-th Frobenius map. Then we have the following:*

(i) *The associated differential with respect to σ is at most unique up to $k^\times$-multiples.*

(ii) *Assume that K is complete and $\bar{K}$ is separably closed. Then for any $c \in k$ with $v(c)=\nu$, there exists an associated differential ω such that $\omega^\sigma/\omega = c$. Here ν is a positive integer uniquely determined by σ by the equality $V(\xi^\sigma) = V(\xi) + h\nu$ $(\xi \in D^h(K))$.*

Now we define a certain special element of $D^{p^f-1}(\bar{K})$ under the same situation. Fix $c \in k$ with $v(c)=\nu$. Take $\xi \in D(K)$ with $V(\xi)=0$ and put $\omega_* = c\xi^{p^f}/\xi^\sigma$. Then $\bar{\omega}_* \in D^{p^f-1}(\bar{K})$ is proved to be independent of ξ, since, for $x\xi$ with $V(x)=0$, $\overline{c(x\xi)^{p^f}/(x\xi)^\sigma} = \overline{c\xi^{p^f}/\xi^\sigma} \cdot \overline{x^{p^f}/x^\sigma} = \overline{c\xi^{p^f}/\xi^\sigma}$. Furthermore the following result is known.

THEOREM B (Ihara). *Let σ be a p^f-th Frobenius map of K. If there exists an associated differential with σ which is normalized by the condition $\omega^\sigma/\omega = c$ and $V(\omega)=0$, then we have*

$$\bar{\omega}_* = \bar{\omega}^{p^f-1}\ .$$

Finally, the most important point about the associated differential ω is that $\bar{\omega}$ is characterized by some other conditions and, in some particular cases, $\bar{\omega}$ can be calculated explicitly using these conditions. For details and proofs, we refer to Ihara [7], [8], [9].

3. Valued differential field and associated differential in elliptic modular case

3-1. The Gauss valuation V of $Q(J(\tau))$ with respect to $J(\tau)$ is defined by

$$V\left(p^n \frac{f(J(\tau))}{g(J(\tau))}\right)=n\,, \qquad \text{for } f(X),\ g(X)\in \boldsymbol{Z}[X],\ \in p\boldsymbol{Z}[X].$$

The valuation V is characterized by the following conditions: (i) the restriction on $\boldsymbol{Q}$ is the normalized, additive p-adic valuation ord_p, (ii) $V(J(\tau))=0$, and $J(\tau) \bmod V$ is transcendental over F_p. We give another definition of the valuation V as follows. Let $\mathfrak{R}_0$ be a set of all elements of $\boldsymbol{Q}(J(\tau))$ whose Fourier coefficients with respect to $q=e^{2\pi\sqrt{-1}\tau}$ are bounded from the below in the p-adic sense, namely, $f=\sum_{n\geqq N} a_n q^n \in \boldsymbol{Q}(J(\tau))$ with $a_n\in\boldsymbol{Q}$ belongs to $\mathfrak{R}_0$ if and only if $\mathrm{Min}\,(\mathrm{ord}_p\, a_n)>-\infty$ exists. Then $\mathfrak{R}_0$ is a subring of $\boldsymbol{Q}(J(\tau))$ and its quotient field is $\boldsymbol{Q}(J(\tau))$ itself. We define a $\boldsymbol{Z}\cup\{\infty\}$ valued function V' on $\mathfrak{R}_0$ by

$$V'(f)=\underset{n\geqq N}{\mathrm{Min}}\,(\mathrm{ord}_p\, a_n) \qquad \text{for } f=\sum_{n\leqq N} a_n q^n \in \mathfrak{R}_0\,.$$

It is easily seen that

$$V'(fg)=V'(f)+V'(g),\ \ V'(f+g)\geqq \mathrm{Min}\,\{V'(f),\ V'(g)\} \qquad \text{for } f,\ g\in\mathfrak{R}_0\,.$$

Hence V' can be uniquely extended to a valuation of $\boldsymbol{Q}(J(\tau))$. We show this V' coincides with V; the characterized condition (i) and $V'(J(\tau))=0$ are obviously satisfied. Since $V'(J(\tau)^{p^n}-J(\tau))=V'(q^{-p^n}+\cdots-q^{-1}-\cdots)=0$, $J(\tau) \bmod V'$ is transcendental over F_p. Thus we have another definition of V.

Next we discuss the valuations of $\boldsymbol{Q}(J(\tau), J(p\tau))$ extending V. We can define a valuation V_1 of $\boldsymbol{Q}(J(\tau), J(p\tau))$ using Fourier expansions with respect to q in the same way as above. Then V_1 is an extension of V from the way of definition. We define another valuation V_2 of $\boldsymbol{Q}(J(\tau), J(p\tau))$, which is also proved to be an extension of V. For this purpose, we use some properties of the invariant transformation equation $\Phi_p(X, Y)=0$ of degree p in characteristic 0. As is well-known, $\Phi_p(X, Y)=\Phi_p(Y, X)$, and $\Phi_p(X, Y)$ is irreducible as a polynomial with coefficients in $\boldsymbol{Q}(Y)$, and $\Phi_p(J(\tau), J(p\tau))=0$. Since $\Phi_p(X, Y)=\Phi_p(Y, X)$, we can define an isomorphism ρ of $\boldsymbol{Q}(J(\tau), J(p\tau))$ by

$$\left(\frac{F(J(\tau), J(p\tau))}{G(J(\tau), J(p\tau))}\right)^{\rho}=\frac{F(J(p\tau), J(\tau))}{G(J(p\tau), J(\tau))} \qquad \text{for } F(X, Y),\ G(X, Y)\in\boldsymbol{Z}[X, Y]\,.$$

We define the valuation V_2 of $\boldsymbol{Q}(J(\tau), J(p\tau))$ by $V_2(r)=V_1(r^{\rho})$ for any $r\in\boldsymbol{Q}(J(\tau), J(p\tau))$. Then the residue field of $\boldsymbol{Q}(J(\tau), J(p\tau))$ with respect to V_2 can be identified with that of $\boldsymbol{Q}(J(\tau), J(p\tau))$ with respect to V_1. We show that the restriction of V_2 on $\boldsymbol{Q}(J(\tau))$ coincides with the Gauss valuation V; since ρ is trivial on $\boldsymbol{Q}$, the characterized condition (i) is obviously satisfied. Also it is obvious that $V_2(J(\tau))=0$, since $V_2(J(\tau))=V_1(J(p\tau))=0$. We have $J(p\tau)-J(\tau)^p=\sum_{n=-1}^{\infty} c(n)\cdot q^{np}-(\sum_{n=-1}^{\infty} c(n)\cdot q^n)^p =p(\sum_{n=-p}^{\infty} c'(n)\cdot q^n)$, with some $c'(n)\in \boldsymbol{Z}$. Hence we have $J(p\tau) \bmod V_1=(J(\tau) \bmod V_1)^p$ from the definition of V_1. It follows that $J(\tau) \bmod V_2=J(p\tau) \bmod V_1$, which is transcendental over F_p. Thus V_2 is a valuation of $\boldsymbol{Q}(J(\tau), J(p\tau))$ extending V. Then it is known and is easily proved that V_1 and V_2 are all the valuations of $\boldsymbol{Q}(J(\tau), J(p\tau))$ extending V, and that the ramification degree and the modular degree of V_1 (resp. V_2) over V is equal to 1 and 1 (resp. 1 and p). It follows that $\boldsymbol{Q}(J(\tau))_V$ can be identified with $\boldsymbol{Q}(J(\tau), J(p\tau))_{V_1}$. Hence we can regard that $\boldsymbol{Q}(J(\tau), J(p\tau))$ is contained in $\boldsymbol{Q}(J(\tau))_V$. Then the restriction of V to $\boldsymbol{Q}(J(\tau), J(p\tau))$ coincides with V_1.

3-2. We shall apply the general theory in § 2 to the elliptic modular case. First, we construct a valued differential field related to the modular function field $\boldsymbol{Q}(J(\tau))$. Let D_0 be the space of differentials of $\boldsymbol{Q}(J(\tau))$ over $\boldsymbol{Q}$, and let $d:\boldsymbol{Q}(J(\tau))\to D_0$ be the usual differentiation. As a discrete valuation of $\boldsymbol{Q}(J(\tau))$, we take the Gauss valuation V defined in § 3-1. Then it is easy to see that $\{\boldsymbol{Q}(J(\tau)), D_0, d, V\}$ is a valued differential field. We also construct a valued differential field related to $\boldsymbol{Q}(J(\tau), J(p\tau))$. Let D_1 be the space of differentials of $\boldsymbol{Q}(J(\tau), J(p\tau))$ over $\boldsymbol{Q}$, and let $d_1:\boldsymbol{Q}(J(\tau), J(p\tau))\to D_1$ be the usual differentiation. As a discrete valuation of $\boldsymbol{Q}(J(\tau), J(p\tau))$, we take the valuation V_1 defined in § 3-1. Then we can also prove that $\{\boldsymbol{Q}(J(\tau), J(p\tau)), D_1, d_1, V_1\}$ is a valued differential field. $\boldsymbol{Q}(J(\tau))$ is a subfield of $\boldsymbol{Q}(J(\tau), J(p\tau))$, and D_0 is canonically imbedded into D_1. Then it is easy to see that $\{\boldsymbol{Q}(J(\tau), J(p\tau)), D_1, d_1, V_1\}$ is an extension of $\{\boldsymbol{Q}(J(\tau)), D_0, d, V\}$. Moreover, from the discussion about the valuation V_1 in § 3-1, the V-adic completion of $\{\boldsymbol{Q}(J(\tau)), D_0, d, V\}$ can be considered as an extension of $\{\boldsymbol{Q}(J(\tau), J(p\tau)), D_1, d_1, V_1\}$.

Next, we define a p-th Frobenius map σ with $\{\boldsymbol{Q}(J(\tau), J(p\tau)), D_0, d, V\}$ by

$$f(J(\tau))^\sigma=f(J(p\tau)) \qquad \text{with } f(X)\in \boldsymbol{Q}(X)\,.$$

From the discussion in § 3-1, σ is in fact an injective isomorphism from $\boldsymbol{Q}(J(\tau))$ to $\boldsymbol{Q}(J(\tau), J(p\tau))\subset \boldsymbol{Q}(J(\tau))_V$. We shall show that σ satisfies (σ-1) and (σ-2). Since $r^\sigma=\sum_{n\geqq N} a_n q^{np}$ for any $r=\sum_{n\geqq N} a_n q^n\in \boldsymbol{Q}(J(\tau))$ with $a_n\in \boldsymbol{Q}$, we have $V(r^\sigma)=V(r)$. Hence σ is V-preserving. From the fact that $\overline{J(p\tau)}=\overline{J(\tau)^p}$, σ induces a p-th power map of the residue field of $\boldsymbol{Q}(J(\tau))$. It is obvious σ satisfies (σ-2). Thus we conclude that σ is a p-th Frobenius map.

The important point is that, in this case, the reduction $\bar{\omega}$ of the associated differential ω with respect to σ is explicitly calculated by Ihara [7]. The result is the following.

THEOREM C (Ihara). *Put* $r=1$ *for* $p=2$ *and* $r=\frac{1}{2}(p-1)$ *for* $p\geqq 3$. *Then*

$$\bar{\omega}^r=\begin{cases}\overline{J(\tau)}^{-1}\overline{d(J(\tau))} & \textit{for } p=2,\ 3\,;\\ \overline{J(\tau)}^{-a}(\overline{J(\tau)}-12^3)^{-b}P(\overline{J(\tau)})\overline{d(J(\tau))}^r & \textit{for } p\geqq 5\,;\end{cases}$$

where $a=\frac{1}{3}(p\mp 1)$ *for* $p\equiv\pm 1$ $(mod\,3)$, $b=\frac{1}{4}(p\mp 1)$ *for* $p\equiv\pm 1$ $(mod\,4)$, *and* S *is the set of all supersingular invariants in characteristic* p, *and* $P(X)=\prod_{\theta\in S}(X-\theta)\in F_p[X]$.

Now using this theorem, we prove the following.

PROPOSITION 1. *Put* $J(p\tau)\equiv J(\tau)^p+pR_1(J(\tau))$ $(mod\ V^2)$ *with* $R_1(J(\tau))$ *in the valuation ring of* $\boldsymbol{Q}(J(\tau))$ *with respect to* V. *Then*

$$\overline{R_1(J(\tau))}=H(\overline{J(\tau)})+\sum_{\theta\in S^*}\frac{\beta_\theta}{\overline{J(\tau)}-\theta}\ ,$$

where S^* *is the subset of* S *excluding* 0 *and* 12^3, *and for* $\theta\in S^*$, β_θ *is a nonzero constant in* F_{p^2}, *and* $H(X)\in F_p[X]$.

PROOF. Since $\dfrac{d_1(J(p\tau))}{d_1(J(\tau))}=(\sum_{n=-1}^{\infty}c(n)\cdot np\cdot q^{np-1})(\sum_{n=-1}^{\infty}c(n)\cdot n\cdot q^{n-1})^{-1}$, we have $V\left(\dfrac{d_1(J(p\tau))}{d_1(J(\tau))}\right)=1$. Hence the constant ν stated in Theorem A is equal to 1, and we can take p as c in Theorem B. Taking $d(J(\tau))$ as ξ and calculating the reduction of ω_*, we have

$$\bar{\omega}_*=(\overline{J(\tau)}^{p-1}+\overline{R_1'(J(\tau))})^{-1}\overline{d(J(\tau))}^{p-1}\ ,$$

where $R_1'(X)$ is a derivative of $R_1(X)$ as a rational function of X. Theorem B implies that $\bar{\omega}_*=\bar{\omega}^{p-1}$ and $\bar{\omega}$ is determined by above Theorem C. Hence the proof is obtained as follows; the proof for $p\geqq 5$ and that for $p=2$, 3 being exactly same, we only prove for $p\geqq 5$. By Theorems B, C, we have

$$\overline{J(\tau)}+\overline{R_1'(J(\tau))}=\overline{J(\tau)}^{2a}(\overline{J(\tau)}-12^3)^{2b}P(\overline{J(\tau)})^{-2}\ . \tag{5}$$

On the other hand, we have $\Phi_p(J(\tau),J(p\tau))=0$ and $\Phi_p(X,Y)=(X^p-Y)(X-Y^p)+p\psi(X,Y)$ with $\psi(X,Y)\in\boldsymbol{Z}[X,Y]$ by the Kronecker congruence relation. Substituting $J(p\tau)\equiv J(\tau)^p+pR_1(J(\tau))$ (mod V^2) in this equation, we have

$$-R_1(J(\tau))\cdot(J(\tau)-J(\tau)^{p^2})+\psi(J(\tau),J(\tau)^p)\equiv 0\quad(\text{mod } V)\ .$$

Hence we have

$$R_1(J(\tau))\equiv-\frac{\psi(J(\tau),J(\tau)^p)}{J(\tau)^{p^2}-J(\tau)}\quad(\text{mod } V)\ . \tag{6}$$

Expanding the right side of (5) into partial fractions and comparing with (6), we obtain Proposition 1. q.e.d.

4. Reduction mod p^a of cusp forms

4-1. We consider another valued differential field. Put $\boldsymbol{Q}_p^\infty(J(\tau))=\boldsymbol{Q}(J(\tau))\otimes\boldsymbol{Q}_p^\infty$ (over $\boldsymbol{Q}$) and $D^\infty=D_0\otimes\boldsymbol{Q}_p^\infty(J(\tau))$ (over $\boldsymbol{Q}(J(\tau))$). $\boldsymbol{Q}(J(\tau))$ and D_0 are canonically imbedded into $\boldsymbol{Q}_p^\infty(J(\tau))$ and D^∞ respectively. Let d^∞ be the unique differentiation extending d with the $\boldsymbol{Q}_p^\infty$-linearity. Let $\boldsymbol{Q}_p^\infty\{q\}$ be the power series field with coefficients in $\boldsymbol{Q}_p^\infty$. For each $r\in\boldsymbol{Q}_p^\infty(J(\tau))$, we can correspond an element of $\boldsymbol{Q}_p^\infty\{q\}$ naturally using the Fourier expansions with respect to q of elements in $\boldsymbol{Q}(J(\tau))$. Call this element also a Fourier expansion of r (with respect to q). This correspondence induces obviously an injective isomorphism from $\boldsymbol{Q}_p^\infty(J(\tau))$ into $\boldsymbol{Q}_p^\infty\{q\}$. By this Fourier expansions, we can define an additive, discrete and normalized valuation V^∞ of $\boldsymbol{Q}_p^\infty(J(\tau))$ in the same way as in the case V in §3-1. It is also proved by the same argument as in §3-2 that $\{\boldsymbol{Q}_p^\infty(J(\tau)), D^\infty, d^\infty, V^\infty\}$ is a valued differential field.

Next we construct another one. Let $\mathfrak{R}$ be the subring of $\boldsymbol{Q}_p^\infty\{q\}$ consisting of all elements $\sum_{n\geqq N} a_n q^n$ in $\boldsymbol{Q}_p^\infty\{q\}$ such that the coefficients a_n are bounded from the below in the $\mathfrak{p}$-adic sense, and let $\mathfrak{K}$ be the quotient field of $\mathfrak{R}$ in $\boldsymbol{Q}_p^\infty\{q\}$. We can define an additive, discrete and normalized valuation $V_\mathfrak{K}$ in the same way as above. Denote by $\tilde{\mathfrak{O}}$ the valuation ring of $V_\mathfrak{K}$ and by $\tilde{\mathfrak{P}}$ the maximal ideal of $\tilde{\mathfrak{O}}$. Let $D(\mathfrak{K})=\mathfrak{K}\cdot d_\mathfrak{K}q$ be a one dimensional vector space generated by $d_\mathfrak{K}q$ over $\mathfrak{K}$. We define a differentiation $d_\mathfrak{K}:\mathfrak{K}\rightarrow D(\mathfrak{K})$ by

$$d_\mathfrak{K}\Bigl(\sum_{n\geqq N} a_n q^n\Bigr)=\Bigl(\sum_{n\geqq N} a_n n\cdot q^{n-1}\Bigr)d_\mathfrak{K}q\ .$$

It is clear that $d_\mathfrak{K}$ is a well defined differentiation and that the kernel of $d_\mathfrak{K}$ is $\boldsymbol{Q}_p^\infty$. We can prove $D(\tilde{\mathfrak{O}})=\tilde{\mathfrak{O}}\cdot d_\mathfrak{K}q$ as follows; take $r=\sum_{n\geqq N} a_n q^n\in\mathfrak{R}$, with $a_n\in\boldsymbol{Q}_p^\infty$. Then $d_\mathfrak{K}r=(\sum a_n n\cdot q^{n-1})d_\mathfrak{K}q$. Hence we have $V_\mathfrak{K}\Bigl(\frac{d_\mathfrak{K}r}{d_\mathfrak{K}q}\Bigr)\geqq V_\mathfrak{K}(r)$ for any $r\in\mathfrak{R}$. It follows that $V_\mathfrak{K}\Bigl(\frac{d_\mathfrak{K}r}{d_\mathfrak{K}q}\Bigr)\geqq V_\mathfrak{K}(r)$ for any $r\in\mathfrak{K}$. Therefore $D(\tilde{\mathfrak{O}})\subset\tilde{\mathfrak{O}}\cdot d_\mathfrak{K}q$. On the other hand, it is obvious $D(\tilde{\mathfrak{O}})\supset\tilde{\mathfrak{O}}\cdot d_\mathfrak{K}q$. From this, it follows that $d_\mathfrak{K}$ is continuous with respect to the $V_\mathfrak{K}$-adic topology of $\mathfrak{K}$ and of $D(\mathfrak{K})$. Hence it is easy to see that $\{\mathfrak{K}, D(\mathfrak{K}), d_\mathfrak{K}, V_\mathfrak{K}\}$ is a valued differential field.

Now we define a p-th Frobenius map $\tilde{\sigma}$ with $\{\mathfrak{K}, D(\mathfrak{K}), d_\mathfrak{K}, V_\mathfrak{K}\}$ by

$$\Bigl(\sum_{n\geqq N} a_n q^n\Bigr)^{\tilde{\sigma}}=\sum_{n\leqq N} a_n q^{np}\ .$$

$\tilde{\sigma}$ is an injective isomorphism from $\mathfrak{K}$ to $\mathfrak{K}$ itself, and it is easily proved that $\tilde{\sigma}$

satisfies the conditions (σ-1), (σ-2).

We note the relationship between these valued differential fields. The fields $\boldsymbol{Q}(J(\tau))$, $\boldsymbol{Q}_p^\infty(J(\tau))$ are imbedded into $\mathfrak{K}$ by the Fourier expansions, and D_0, D^∞ are imbedded into $D(\mathfrak{K})$ by the identification,

$$d(J(\tau))=(\sum_{n=-1}^{\infty} c(n)\cdot n\cdot q^{n-1})d_{\mathfrak{K}}q\ .$$

Under these situations, the restrictions of $d_{\mathfrak{K}}$ and $V_{\mathfrak{K}}$ to $\boldsymbol{Q}(J(\tau))$ (resp. $\boldsymbol{Q}_p^\infty(J(\tau))$) coincide with d and V (resp. d^∞ and V^∞), and $\tilde{\sigma}$ induces σ on $\boldsymbol{Q}(J(\tau))$ defined in § 3-2.

Now we consider associated differentials of $\tilde{\sigma}$. We have the following.

PROPOSITION 2. *The set of all associated differentials with respect to $\tilde{\sigma}$ is* $\{a\cdot q^{-1}d_{\mathfrak{K}}q \mid a\neq 0, \in \boldsymbol{Q}_p^\infty\}$.

PROOF. Since $(q^{-1}d_{\mathfrak{K}}q)^{\tilde{\sigma}}=q^{-p}d_{\mathfrak{K}}(q^p)=p\cdot q^{-1}d_{\mathfrak{K}}q$, $q^{-1}d_{\mathfrak{K}}q$ is an associated differential. By Theorem A about the uniqueness of the associated differentials, we obtain Proposition 2. q.e.d.

On the other hand, taking $d(J(\tau))$ as ξ and calculating $\bar{\omega}_*$ defined in § 2, we attain at the following important identity by Proposition 2, and Theorem B;

$$\overline{(q^{-1}d_{\mathfrak{K}}q)}^{p-1}=(\overline{J(\tau)}^{p-1}+\overline{R_1'(J(\tau))})^{-1}\overline{d(J(\tau))}^{p-1}\ .$$

With this identity and Theorem C, we arrive at the following.

PROPOSITION 3. *Put* $d(J(\tau))=(q\Lambda)^{-1}d_{\mathfrak{K}}q$, *with* $\Lambda\in\mathfrak{K}$. *Then* Λ *belongs to* $\tilde{\mathfrak{O}}$ *and satisfies the following congruences for any rational integer* $\alpha\geqq 1$;

$$(7) \qquad \Lambda^{rp^{\alpha-1}}\equiv(-1)^r W^{p^{\alpha-1}} \quad (mod\ \tilde{\mathfrak{P}}^\alpha)\ ,$$

where

$$W=\begin{cases} J(\tau)^{-1} & for\ \ p=2,\ 3\ ; \\ J(\tau)^{-a}(J(\tau)-12^3)^{-b}\prod_{\theta\in S}(J(\tau)-j_\theta) & for\ \ p\geqq 5. \end{cases}$$

Here the notations are as follows; S, S^*, r, a and b are the same as defined in Theorem C and Proposition 1. For $\theta\in S^*$, j_θ is the unique element in $\mathfrak{o}_p^\infty$ such that $j_\theta^{p^2}=j_\theta$, and $j_\theta \pmod{\mathfrak{p}}=\theta$, and for $\theta=0$, 12^3 in S, j_θ is 0, 12^3 respectively.

PROOF. Since $\Lambda=q^{-1}(\sum_{n=-1}^{\infty} c(n)\cdot n\cdot q^{n-1})^{-1}$ and $c(-1)=1$, we have $V_{\mathfrak{K}}(\Lambda)=0$ by definition; hence Λ belongs to $\tilde{\mathfrak{O}}$. As is remarked above, we have

$$(8) \qquad \overline{(q^{-1}d_{\mathfrak{K}}q)}^{p-1}=(\overline{J(\tau)}^{p-1}+\overline{R_1'(J(\tau))})^{-1}\overline{d(J(\tau))}^{p-1}\ .$$

The right side of (8) is calculated in a more explicit form by Proposition 1. Hence, substituting $\Lambda\cdot d(J(\tau))=q^{-1}d_{\mathfrak{K}}q$ in (8), we obtain

$$\Delta^r \equiv cW \pmod{\tilde{\mathfrak{P}}}\,, \tag{9}$$

with a constant $c\in\mathfrak{o}_p^\infty$. Considering the Fourier expansions of both sides of (9), we have $c=(-1)^r$. Therefore we have

$$\Delta^r=(-1)^r W+p\phi\,, \tag{10}$$

with $\phi\in\tilde{\mathfrak{C}}$. Raising to the $p^{\alpha-1}$-th power of both sides of (10), we have

$$\Delta^{rp^{\alpha-1}}=(-1)^r W^{p^{\alpha-1}}+\sum_{i=1}^{p^{\alpha-1}}\binom{p^{\alpha-1}}{i}p^i\phi^i\,((-1)^r W)^{p^{\alpha-1}-i}\,. \tag{11}$$

Then we shall show

$$\operatorname{ord}_p\left(\binom{p^{\alpha-1}}{i}p^i\right)\geqq\alpha\,, \qquad \text{for any } 1\leqq i\leqq p^{\alpha-1}\,. \tag{12}$$

To begin with, we prove that

$$p^n-(n+1)\geqq 0 \qquad \text{for any } n\geqq 0\,. \tag{13}$$

In the case $n=0$, this is valid since $p^0-(0+1)=0$. Using induction on n, we have

$$p^{n+1}-(n+2)\geqq p(n+1)-(n+2)\geqq n(p-1)+(p-2)\geqq 0\,.$$

Hence (13) is proved to be valid. From (13), we have

$$i-\operatorname{ord}_p i-1\geqq 0 \qquad \text{for any } i\geqq 1.$$

Therefore we have

$$\begin{aligned}\operatorname{ord}_p\left(\binom{p^{\alpha-1}}{i}p^i\right)-\alpha &\geqq i+\operatorname{Max}\{0,\alpha-1-\operatorname{ord}_p i\}-\alpha\,,\\ &=\operatorname{Max}\{i-\alpha,\, i-\operatorname{ord}_p i-1\}\geqq 0\,.\end{aligned}$$

Considering (11) in modulo $\tilde{\mathfrak{P}}^\alpha$ with this result, we obtain (7). q.e.d.

REMARK. As for the known facts about supersingular invariants in characteristic p, we refer to Deuring [4]. Here, we briefly recall some facts which are needed later; the cardinal number of S^* is equal to $\left[\dfrac{p}{12}\right]$. For $p\geqq 5$, 0 belongs to S if and only if $p\equiv 5$, 11 (mod 12), and 12^3 belongs to S if and only if $p\equiv 7$, 11 (mod 12). Hence W is rewritten as follows;

$$W=J(\tau)^{-m_1}(J(\tau)-12^3)^{-m_2}\prod_{\theta\in S^*}(J(\tau)-j_\theta)\,,$$

with $m_1=\left[\dfrac{1}{3}(p-1)\right]$, $m_2=\left[\dfrac{1}{4}(p-1)\right]$.

4-2. Reduction mod p^α of cusp forms of weight $k(p^\alpha-p^{\alpha-1})$. Let $\tilde{Q}\subset C$ be the algebraic closure of $\boldsymbol{Q}$. Fix a divisor $\mathbf{p}$ of $\bar{\boldsymbol{Q}}$ extending p of $\boldsymbol{Q}$, and denote by $\bar{\boldsymbol{Q}}_T$ the inertia field of $\mathbf{p}$. Then $\mathbf{p}$ determines an unramified valuation of $\bar{\boldsymbol{Q}}_T$. Hence $\bar{\boldsymbol{Q}}_T$ can be imbedded in $\boldsymbol{Q}_p^{\infty}$. Henceforth we fix one imbedding. Thus, as far as the elements of $\bar{\boldsymbol{Q}}_T$ are concerned, they can be regarded as $\mathfrak{p}$-adic numbers. Denote by $\mathfrak{o}_T$ the subring of $\bar{\boldsymbol{Q}}_T$ consisting of all elements of $\bar{\boldsymbol{Q}}_T$ which belong to $\mathfrak{o}_p^{\infty}$ as $\mathfrak{p}$-adic numbers.

Let $k\geqq 1$, and $\alpha\geqq 1$ be rational integers. If $p=2$ and $\alpha=1$, we assume k is even. We denote by $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$ the space of cusp forms of weight $k(p^\alpha-p^{\alpha-1})$ with respect to $\Gamma=SL(2, \boldsymbol{Z})$. As is well-known, we can take the following elements as a basis of $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$; let

$$\Delta=q\prod_{n=1}^{\infty}(1-q^n)^{24},$$

$$G_4=1+240\sum_{n=1}^{\infty}\sigma_3(n)\cdot q^n,$$

$$G_6=1-504\sum_{n=1}^{\infty}\sigma_5(n)\cdot q^n,$$

with $\sigma_i(n)=\sum_{\substack{d\mid n\\ d>0}} d^i$. Put $G_0=1$, $G_8=G_4^2$, $G_{10}=G_4G_6$, $G_{12}=G_4^3$, and $G_{14}=G_4^2G_6$. Put $s=\left[\dfrac{1}{12}k(p^\alpha-p^{\alpha-1})\right]$, and $t=k(p^\alpha-p^{\alpha-1})-12s$. If $s>0$ except $s=1$ and $t=2$, a basis of $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$ is given by the followings $\{F_i(\tau)\}$ such that,

Case 1. If $t\neq 2$,

$$F_i(\tau)=\Delta^i G_{12}^{s-i}G_t \qquad \text{for } 1\leqq i\leqq s,$$

Case 2. If $t=2$,

$$F_i(\tau)=\Delta_i G_{12}^{s-i-1}G_{14} \qquad \text{for } 1\leqq i\leqq s-1.$$

Call this basis a *canonical basis* of $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$. The canonical basis $\{F_i(\tau)\}$ satisfies following two properties;

(i) The Fourier coefficients of $F_i(\tau)$ with respect to q are rational integers, and the first coefficient which is not zero is equal to 1.

(ii) Let $F(\tau)=\sum_{n=N}^{\infty}A_nq^n\neq 0$, with $A_n\in \boldsymbol{C}$, be any modular form with respect to Γ. Denote by $\mathrm{ord}_\infty(F)$ the first n such that $A_n\neq 0$. Then we have $\mathrm{ord}_\infty(F_i)=i$.

Now we define the reduction mod p^α of cusp forms of weight $k(p^\alpha-p^{\alpha-1})$. Let $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1}),\mathfrak{o}_T}$ denote the submodule of $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$ consisting of all elements in $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$ whose Fourier coefficients all belong to $\mathfrak{o}_T$. Then $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1}),\mathfrak{o}_T}$ is a free $\mathfrak{o}_T$-module with the canonical basis as its free basis by the properties (i), (ii). From definition, $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1}),\mathfrak{o}_T}$ is canonically imbedded in $\tilde{\mathfrak{O}}$ by the Fourier expansions. Hence, for $F\in\mathfrak{S}_{k(p^\alpha-p^{\alpha-1}),\mathfrak{o}_T}$, $F\,(\mathrm{mod}\,\tilde{\mathfrak{P}}^\alpha)$ is well defined. Call $F\,(\mathrm{mod}\,\tilde{\mathfrak{P}}^\alpha)$ *the reduction mod* p^α *of cusp form* F.

PROPOSITION 4. *Let* $p\geqq 5$. *Let* $\alpha\geqq 1$ *and* $k\geqq 1$ *be rational integers. Then, for each* $F\in\mathfrak{S}_{k(p^\alpha-p^{\alpha-1}),\mathfrak{o}_T}$, *we have the following congruence;*

$$F\equiv\frac{H(J(\tau))}{J(\tau)^{M_1-m_1kp^{\alpha-1}}(J(\tau)-12^3)^{M_2-m_2kp^{\alpha-1}}(\prod_{\theta\in S^*}J(\tau)-j_\theta)^{kp^{\alpha-1}}}\quad(\mathrm{mod}\,\tilde{\mathfrak{P}}^\alpha)\,,\tag{14}$$

with $H(X)\in\mathfrak{o}_T[X]$, *where* $M_1=\left[\frac{1}{3}k(p^\alpha-p^{\alpha-1})\right]$, $M_2=\left[\frac{1}{4}k(p^\alpha-p^{\alpha-1})\right]$, $m_1=\left[\frac{1}{3}(p-1)\right]$, $m_2=\left[\frac{1}{4}(p-1)\right]$, *and* S^* *and* j_θ *are the same as in Proposition* 3, §4-1. *Moreover, the polynomial degree of* $H(X)$ *is smaller than* $\dim_C\mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$, *and while* F *varies in* $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1}),\mathfrak{o}_T}$, *all polynomials in* $\mathfrak{o}_T[J(\tau)]$ *satisfying above condition about the polynomial degree can appear as* $H(J(\tau))$ *in* (14), *and, for each* F, $H(J(\tau))$ *is unique up to modulo* $\tilde{\mathfrak{P}}^\alpha$.

For $p=2$, 3, we have the following;

PROPOSITION 5. *Let* $p=2$, 3. *Let* $\alpha\geqq 1$ *and* $k\geqq 1$ *be rational integers. Put* $d=\dim_C\mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$. *Then, if* $d\neq 0$, *for each* $F\in\mathfrak{S}_{k(p^\alpha-p^{\alpha-1}),\mathfrak{o}_T}$, *the following congruence is valid;*

$$F\equiv\frac{H(J(\tau))}{J(\tau)^d}\quad(\mathrm{mod}\,\tilde{\mathfrak{P}}^\alpha)\tag{15}$$

with $H(X)\in\mathfrak{o}_T[X]$ *whose polynomial degree is smaller than* d. *Moreover, while* F *varies in* $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1}),\mathfrak{o}_T}$, *all polynomials in* $\mathfrak{o}_T[J(\tau)]$ *satisfying the above condition about the polynomial degree can appear as* $H(J(\tau))$ *in* (15), *and, for each* F, $H(J(\tau))$ *is unique up to modulo* $\tilde{\mathfrak{P}}^\alpha$.

REMARK 1. By definition of $\tilde{\mathfrak{P}}^\alpha$, (14) and (15) mean that the Fourier coefficients of both sides are congruent in modulo $\mathfrak{p}^\alpha$. Hence this definition of the reduction mod p^α coincides with that defined in §1 for the elements in $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1}),Z}$.

REMARK 2. The same argument of the proof of this proposition enables us to consider the reduction mod p^α of the entire forms of weight $k(p^\alpha-p^{\alpha-1})$, where the entire forms mean the modular forms which are holomorphic on $\mathfrak{H}$. The result is as follows. Let $F(\tau)$ be an entire form of weight $k(p^\alpha-p^{\alpha-1})$ with respect to Γ whose Fourier coefficients all belong to $\mathfrak{o}_T$. Then there exists $H(X)\in\mathfrak{o}_T[X]$ such that

$$F(\tau)\equiv\frac{H(J(\tau))}{J(\tau)^{M_1-m_1kp^{\alpha-1}}(J(\tau)-12^3)^{M_2-m_2kp^{\alpha-1}}(\prod_{\theta\in S^*}J(\tau)-j_\theta)^{kp^{\alpha-1}}}\quad(\mathrm{mod}\,\tilde{\mathfrak{P}}^\alpha)\,.$$

Here $H(X)$ is unique up to modulo $p^\alpha\cdot\mathfrak{o}_T[X]$ and its polynomial degree satisfies the following relation,

$$\deg H = \dim_C \mathfrak{S}_{k(p^{\alpha}-p^{\alpha-1})} - \mathrm{ord}_{\infty}(F) .$$

This fact is used in §7, but we do not give its proof, the argument being entirely similar.

Remark 3. We have the following table;

p; prime	$M_1 - m_1kp^{\alpha-1}$	$M_2 - m_2kp^{\alpha-1}$
$p\equiv 1 \pmod{12}$	0	0
$p\equiv 5 \pmod{12}$	$\left[\frac{1}{3}kp^{\alpha-1}\right]$	0
$p\equiv 7 \pmod{12}$	0	$\left[\frac{1}{2}kp^{\alpha-1}\right]$
$p\equiv 11 \pmod{12}$	$\left[\frac{1}{3}kp^{\alpha-1}\right]$	$\left[\frac{1}{2}kp^{\alpha-1}\right]$

The proofs being similar, we only prove for $p\equiv 11 \pmod{12}$. Put $p=12t+11$. Then we have $m_1=\left[4t+\frac{10}{3}\right]=4t+3$, and $m_2=\left[3t+\frac{5}{2}\right]=3t+2$. On the other hand, we have $M_1=\left[kp^{\alpha-1}\left(4t+\frac{10}{3}\right)\right]=kp^{\alpha-1}(4t+3)+\left[\frac{1}{3}kp^{\alpha-1}\right]$, and $M_2=\left[kp^{\alpha-1}\left(3t+\frac{5}{2}\right)\right]$ $=kp^{\alpha-1}(3t+2)+\left[\frac{1}{2}kp^{\alpha-1}\right]$. q.e.d.

Hence from Remark of Proposition 3, if 0 (resp. 12^3) is not contained in S, $M_1-m_1kp^{\alpha-1}$ (resp. $M_2-m_2kp^{\alpha-1}$) is always zero.

Proof of Propositions 4, 5. The proofs of both propositions being similar, we prove only Proposition 4.

As is mentioned in §1, Γ acts on $\mathfrak{H}$. Put $\mathfrak{H}^*=\mathfrak{H}\cup\{\infty\}\cup \boldsymbol{Q}$. We extend the action of Γ on $\mathfrak{H}$ to that on $\mathfrak{H}^*$ by,

$$g\cdot x=\begin{cases}(cx+d)^{-1}(ax+b) & \text{if } cx+d\neq 0 ,\\ \infty & \text{if } cx+d=0 ,\end{cases}$$

$$g\cdot\infty=\begin{cases}c^{-1}a & \text{if } c\neq 0 ,\\ \infty & \text{if } c=0 ,\end{cases}$$

for $x\in \boldsymbol{Q}$, $g=\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in\Gamma$. As is well-known, $\Gamma\backslash\mathfrak{H}$ and $\Gamma\backslash\mathfrak{H}^*$ can be considered as a complex manifold of dimension 1 and a compact Riemann surface of genus zero respectively. $\Gamma\backslash\mathfrak{H}$ is canonically imbedded into $\Gamma\backslash\mathfrak{H}^*$, and this imbedding is holomorphic with the above structures. As a set, we have $\Gamma\backslash\mathfrak{H}^*=\Gamma\backslash\mathfrak{H}\cup\{\text{one point}\}$. Let $\pi:\mathfrak{H}\rightarrow\Gamma\backslash\mathfrak{H}$ be a natural projection. Then π is holomorphic and is ramified at $\pi(i)$ and $\pi(e^{\frac{2\pi\sqrt{-1}}{3}})$ with the ramification order 2 and 3 respectively. $J(\tau)$ is considered as a meromorphic function on $\Gamma\backslash\mathfrak{H}^*$ and, then, generates the function field of $\Gamma\backslash\mathfrak{H}^*$ over C. Hence, we take $J(\tau)$ as a local coordinates of $\Gamma\backslash\mathfrak{H}^*$, and also as a coordinate of $\Gamma\backslash\mathfrak{H}$. Then π is ramified at the point of $J(\tau)=0$ and $J(\tau)=12^3$ with the ramification order 3 and 2 respectively.

Let k be a rational positive integer. Let $F(\tau)$ be a modular form of weight $2k$ with respect to Γ. Then $F(\tau)\left(\frac{dJ(\tau)}{d\tau}\right)^{-k}$ is a modular function with respect to Γ by definition of modular forms. Put $F(\tau)\left(\frac{dJ(\tau)}{d\tau}\right)^{-k}=T(J(\tau))$, with $T(X)\in C(X)$. This implies that the differential $T(J(\tau))\cdot d(J(\tau))^k$ on $\Gamma\backslash\mathfrak{H}$ of degree k induces a differential $F(\tau)\cdot(d\tau)^k$ on $\mathfrak{H}$ by the covering map π. In general, let ω be a differential on $\Gamma\backslash\mathfrak{H}$ of degree k and let ω' be a differential on $\mathfrak{H}$ induced by ω by the covering map $\pi:\mathfrak{H}\rightarrow\Gamma\backslash\mathfrak{H}$. Denote by (ω) and (ω') the divisor of ω on $\Gamma\backslash\mathfrak{H}$ and that of ω' on $\mathfrak{H}$ respectively. Take any point $P'\in\mathfrak{H}$, and put $\pi(P')=P$, and denote by e the ramification order of π at P'/P. Then we have the well-known formula;

$$\operatorname{ord}_{P'}(\omega')+k=e(\operatorname{ord}_P(\omega)+k)\ . \tag{16}$$

Apply this formula to $\omega'=F(\tau)\cdot(d\tau)^k$ and $\omega=T(J(\tau))\cdot d(J(\tau))^k$. If we assume that $F(\tau)$ is a cusp form, we have $\operatorname{ord}_{P'}(\omega')\geqq 0$ for any $P'\in\mathfrak{H}$. Hence, by (16), we have the following;

$$\operatorname{ord}_P(\omega)\geqq\begin{cases} 0 & \text{if } P \text{ is not equal to the point of } J(\tau)=0 \text{ or } J(\tau)=12^3, \\ -\left[\frac{2}{3}k\right] & \text{if } P \text{ is the point of } J(\tau)=0, \\ -\left[\frac{1}{2}k\right] & \text{if } P \text{ is the point of } J(\tau)=12^3. \end{cases}$$

It follows that $T(X)=X^{-\left[\frac{2}{3}k\right]}(X-12^3)^{-\left[\frac{1}{2}k\right]}\cdot S(X)$, with some $S(X)\in C[X]$. Therefore if we take $F(\tau)\in\mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$, we have

$$F(\tau)\left(\frac{dJ(\tau)}{d\tau}\right)^{-\frac{1}{2}k(p^\alpha-p^{\alpha-1})}=\frac{S(J(\tau))}{J(\tau)^{M_1}(J(\tau)-12^3)^{M_2}}$$

with $S(X)\in C[X]$. Since $\frac{dq}{d\tau}=2\pi iq$, we have

$$F(\tau)\left(\frac{qdJ(\tau)}{dq}\right)^{-\frac{1}{2}k(p^\alpha-p^{\alpha-1})}=\frac{H(J(\tau))}{J(\tau)^{M_1}(J(\tau)-12^3)^{M_2}} \tag{17}$$

with $H(X)=(2\pi i)^{\frac{1}{2}k(p^\alpha-p^{\alpha-1})}\cdot S(X)\in C[X]$. Moreover, if we assume $F(\tau)\in\mathfrak{S}_{k(p^\alpha-p^{\alpha-1}),\mathfrak{o}_T}$, we conclude that $H(X)\in\mathfrak{o}_T[X]$; because all the Fourier coefficients of $F(\tau)J(\tau)^{M_1}(J(\tau)-12^3)^{M_2}\left(\frac{qdJ(\tau)}{dq}\right)^{-\frac{1}{2}k(p^\alpha-p^{\alpha-1})}$ belong to $\mathfrak{o}_T$. Hence, for each $F(\tau) \in \mathfrak{S}_{k(p^\alpha-p^{\alpha-1}),\mathfrak{o}_T}$, we can regard that (17) holds in $\tilde{\mathfrak{O}}_T$ with the identification $\frac{qdJ(\tau)}{dq} = \frac{qdJ(\tau)}{d_{\mathfrak{K}}q}$. Therefore, with Proposition 3 where we calculated $\left(\frac{qdJ(\tau)}{d_{\mathfrak{K}}q}\right)^{\frac{1}{2}(p^\alpha-p^{\alpha-1})}$ $(\bmod \tilde{\mathfrak{P}}^\alpha)$ explicitly, we conclude that,

$$F(\tau) \equiv (-1)^{k\frac{p-1}{2}} \frac{H(J(\tau))}{J(\tau)^{M_1}(J(\tau)-12^3)^{M_2}} W^{-kp^{\alpha-1}} \quad (\bmod \tilde{\mathfrak{P}}^\alpha) .$$

And, from Remark of the same proposition, we have

$$(18) \qquad F(\tau) \equiv (-1)^{k\frac{p-1}{2}} \frac{H(J(\tau))}{J(\tau)^{M_1-m_1kp^{\alpha-1}}(J(\tau)-12^3)^{M_2-m_2kp^{\alpha-1}}(\prod_{\theta \in S^*} J(\tau)-j_\theta)^{kp^{\alpha-1}}} \quad (\bmod \tilde{\mathfrak{P}}^\alpha) .$$

Now we discuss on the polynomial degree of the polynomial $H(X)$. In the equality (17), considering the Fourier expansions of both sides, we obtain the following equality;

$$(19) \qquad \mathrm{ord}_\infty (F) + \frac{1}{2} k(p^\alpha - p^{\alpha-1}) = M_1 + M_2 - \deg H ,$$

where $\deg H$ is the polynomial degree of $H(X) \in \mathfrak{o}_T[X]$. From the well-known dimension formula of $\mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$, we have, if $k(p^\alpha-p^{\alpha-1})>2$,

$$(20) \qquad \begin{aligned} \dim_C \mathfrak{S}_{k(p^\alpha-p^{\alpha-1})} &= -\{k(p^\alpha-p^{\alpha-1})-1\} + \left\{\frac{1}{2} k(p^\alpha-p^{\alpha-1})-1\right\} \\ &\quad + \left[\frac{1}{3} k(p^\alpha-p^{\alpha-1})\right] + \left[\frac{1}{4} k(p^\alpha-p^{\alpha-1})\right] , \\ &= M_1 + M_2 - \frac{1}{2} k(p^\alpha-p^{\alpha-1}) . \end{aligned}$$

In particular, if we put $k=1$, $\alpha=1$ in (20), we have $\dim_C \mathfrak{S}_{p-1} = m_1+m_2-\frac{1}{2}(p-1)$. On the other hand, it is well-known that $\dim_C \mathfrak{S}_{p-1} = \left[\frac{p}{12}\right]$ for any prime $p \geqq 3$. Hence we have

$$(21) \qquad m_1+m_2-\frac{1}{2}(p-1) = \left[\frac{p}{12}\right] .$$

From (20), (21), we have $\dim_C \mathfrak{S}_{k(p^\alpha-p^{\alpha-1})} = (M_1-m_1kp^{\alpha-1}) + (M_2-m_2kp^{\alpha-1}) + \left[\frac{p}{12}\right]$. Therefore, we conclude that the denominator of the right side of (18) is the polynomial of $J(\tau)$ whose polynomial degree is equal to $\dim_C \mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$, and that $\deg H$ is smaller than $\dim_C \mathfrak{S}_{k(p^\alpha-p^{\alpha-1})}$, since $\mathrm{ord}_\infty(F)>0$ for any $F(\tau) \in$

$\mathfrak{S}_{k(p^{\alpha}-p^{\alpha-1}),\mathfrak{o}_T}$.

Finally, we prove that if $F(\tau)$ varies in $\mathfrak{S}_{k(p^{\alpha}-p^{\alpha-1}),\mathfrak{o}_T}$, all $H(J(\tau))\in\mathfrak{o}_T[J(\tau)]$ whose polynomial degree is smaller than $\dim_C\mathfrak{S}_{k(p^{\alpha}-p^{\alpha-1})}$ can appear in the right side of (14) for some $F(\tau)$. Put $d=\dim_C\mathfrak{S}_{k(p^{\alpha}-p^{\alpha-1})}$. Take the canonical basis $\{F_i(\tau)\}_{i=1}^{d}$ of $\mathfrak{S}_{k(p^{\alpha}-p^{\alpha-1})}$. For $F_i(\tau)$, let $H_i(X)\in\mathfrak{o}_T[X]$ be such that

$$F_i(\tau)\left(\frac{q\cdot dJ(\tau)}{dq}\right)^{-\frac{1}{2}k(p^{\alpha}-p^{\alpha-1})}=\frac{(-1)^{-\frac{1}{2}k(p-1)}H_i(J(\tau))}{J(\tau)^{M_1}(J(\tau)-12^3)^{M_2}} .$$

holds. Since $\mathrm{ord}_{\infty}(F_i)=i$, we have $\deg H_i=d-i$. Considering the Fourier expansions, we see that $H_i(X)$ is a monic polynomial because of the property (i). Hence all $H(X)\in\mathfrak{o}_T[X]$ whose polynomial degree is smaller than d is a linear sum of $H_i(X)$, $1\leqq i\leqq d$ with coefficients in $\mathfrak{o}_T$. q.e.d.

5. Reduction mod p^{α} of some modular functions

Here we prove a certain proposition, which is needed to connect the Fourier coefficients of some modular functions with respect to $\Gamma_0(p)$ with those of cusp forms with respect to Γ.

5-1. We need the following lemma.

LEMMA 2. *Let $l\geqq 0$, $n\geqq 1$ be rational integers. Let m be a rational integer such that $m\not\equiv 0$ (mod p). Let $T_0(p^n)$ be the same as defined in* §1. *Then we have*

$$p^n\cdot e^{2\pi\sqrt{-1}mp^l\tau}|T_0(p^n)=\sum_{i=0}^{\mathrm{Min}(n,l)}p^i\cdot e^{2\pi\sqrt{-1}mp^{n+l-2i}\tau} .$$

PROOF. The left side equals to $\sum\limits_{\substack{ad=p^n\\ d>0}}e^{2\pi\sqrt{-1}mp^l\cdot\frac{a}{d}\cdot\tau}\Big(\sum\limits_{b\bmod d}e^{2\pi\sqrt{-1}m\cdot p^l\cdot\frac{b}{d}}\Big)$, and the second sum takes the value 0 (if $d\nmid mp^l$), d (if $d|mp^l$). q.e.d.

Since $(n+l-2i)-(n-i)=l-i\geqq 0$ for $0\leqq i\leqq\mathrm{Min}(n,l)$, we notice the following fact from this lemma; if we put $e^{2\pi\sqrt{-1}mp^l\tau}|T_0(p^n)=\sum\limits_{j\geqq N}a_je^{2\pi\sqrt{-1}j\tau}$, with $a_j\in\boldsymbol{Q}$, then $j\cdot a_j$ are all rational integers.

5-2. We also need some elementary congruence properties of the combination number $\binom{n}{r}$. Let $t\geqq 1$ be a rational integer and take $t+1$ positive rational integers r_0, $r_1,\cdots,r_t$ with $r_0>r_1>\cdots>r_t$. Put $(r_0,\cdots,r_t)=\prod\limits_{i=0}^{t-1}\binom{r_i}{r_{i+1}}$. Then we have;

LEMMA 3. *Put* $\mathrm{ord}_p r_i=l_i$ *and* $L=\mathrm{Min}_{0\leqq i\leqq t}(l_i)$. *Then* (i) $(r_0,\cdots,r_t)$ *is divisible* *by* p^{l_0-L}. (ii) *If* $L\geqq 1$, *then*

$$p^{-(l_0-L)}(r_0,\cdots,r_t)\equiv p^{-(l_0-L)}(p^{-1}r_0,\cdots,p^{-1}r_t)\quad (mod\ p^L)\ . \tag{22}$$

PROOF. Since $\binom{r_i}{r_{i+1}}=\frac{r_i}{r_{i+1}}\cdot\binom{r_i-1}{r_{i+1}-1}$, we have $\mathrm{ord}_p\binom{r_i}{r_{i+1}}\geqq \mathrm{Max}\,\{0,l_i-l_{i+1}\}$. Hence $\mathrm{ord}_p(r_0,\cdots,r_t)\geqq\sum_{i=0}^{t-1}\mathrm{Max}\,\{0,l_i-l_{i+1}\}\geqq l_0-L$. (ii) By definition, $\binom{r_i}{r_{i+1}}=\prod_{s=0}^{r_{i+1}-1}\frac{r_i-s}{r_{i+1}-s}$. If $(s,p)=1$, $\frac{r_i-s}{r_{i+1}-s}\equiv 1\ (\mathrm{mod}\ p^L)$, and if $(s,p)=p$, $\frac{r_i-s}{r_{i+1}-s}=\frac{p^{-1}r_i-p^{-1}s}{p^{-1}r_{i+1}-p^{-1}s}$. Hence we have $p^{-\mathrm{Max}\,\{0,l_i-l_{i+1}\}}\cdot\binom{r_i}{r_{i+1}}\equiv p^{-\mathrm{Max}\,\{0,l_i-l_{i+1}\}}\cdot\binom{p^{-1}r_i}{p^{-1}r_{i+1}}$ $(\mathrm{mod}\ p^L)$, which implies $p^{-(l_0-L)}(r_0,\cdots,r_t)\equiv p^{-(l_0-L)}(p^{-1}r_0,\cdots,p^{-1}r_t)\ (\mathrm{mod}\ p^L)$.

q.e.d.

5-3. Let $\boldsymbol{Q}[[q]]$ be the formal power series ring with coefficients in $\boldsymbol{Q}$. Let $\boldsymbol{Q}\{q\}$ be its quotient field. By the Fourier expansion with respect to q, each element of $\boldsymbol{Q}(J(\tau))$ corresponds to an element of $\boldsymbol{Q}\{q\}$. Then it is easily proved that the restriction to $\boldsymbol{Q}[J(\tau)]$ of this correspondence gives an isomorphism of $\boldsymbol{Q}[J(\tau)]$ as $\boldsymbol{Q}$-module onto the residue class $\boldsymbol{Q}$-module of $\boldsymbol{Q}\{q\}$ modulo $q\cdot\boldsymbol{Q}[[q]]$. Denote this isomorphism by ι. The set $\{\sum_{i=0}^{m}a_iq^{-i}|a_i\in\boldsymbol{Q},m\geqq 0\}$ gives a full set of representatives of the residue class of $\boldsymbol{Q}\{q\}$ modulo $q\cdot\boldsymbol{Q}[[q]]$.

Let $d\geqq 1$ be a rational integer such that $d\not\equiv 0\ (\mathrm{mod}\ p)$, and let $n\geqq 0$ be a rational integer. Put $\iota^{-1}(p^{-n}\cdot q^{-dp^n})=H_{p,d,n}(J(\tau))$. We prove:

PROPOSITION 6. *Let* $n\geqq 1$. *Then,*

$$H_{p,d,n}(J(\tau))\equiv p^{-1}H_{p,d,n-1}(J(\tau)^p)\quad (mod\ \boldsymbol{Z}[J(\tau)])\ . \tag{23}$$

PROOF. We note that $\iota^{-1}(\sum_{i=0}^{m}a_i\cdot q^{-i})$ belongs to $\boldsymbol{Z}[J(\tau)]$ if and only if all a_i belong to $\boldsymbol{Z}$. Put

$$\iota(H_{p,d,n}(J(\tau))-p^{-n}\cdot J(\tau)^{dp^n})=\sum_{\substack{m>0\\(m,p)=1\\l\geqq 0\\0<mp^l<dp^n}}(-a_{mp^l}^{(d,n)}\cdot q^{-mp^l})-a_0^{(d,n)} \tag{24}$$

with $a_i^{(d,n)}\in\boldsymbol{Q}$, $0\leqq i<dp^n$. Let the Fourier expansion of $J(\tau)$ be $J(\tau)=\sum_{n=-1}^{\infty}c(n)\cdot q^n$, with $c(n)\in\boldsymbol{Z}$. Then, we have

$$a_{mp^l}^{(d,n)}=\sum_{\substack{t\geqq 0\\dp^n=r_0>r_1>\cdots>r_t>r_{t+1}=0\\n_t>\cdots>n_1>n_0\geqq -1\\\sum_{i=0}^{t}(r_i-r_{i+1})n_i=-mpl}}p^{-n}\cdot c(n_0)^{r_0-r_1}\cdots c(n_t)^{r_t}\cdot\binom{r_0}{r_0-r_1}\cdot\binom{r_1}{r_1-r_2}\cdots \tag{25}$$

$$\cdots\binom{r_{t-1}}{r_{t-1}-r_t}=\sum p^{-n}\cdot c(n_0)^{r_0-r_1}\cdots c(n_t)^{r_t}\cdot(r_0,\cdots,r_t)\ .$$

By using Lemma 3, we see that if at least one r_i is prime to p the corresponding term in (25) is a rational integer. Therefore, when we consider $H_{p,d,n}(J(\tau))$ modulo $\boldsymbol{Z}[J(\tau)]$, we can omit that term. For $l \geqq 1$, put

$$(26)\quad a'^{(d,n)}_{mp^l} = \sum_{\substack{t \geqq 0 \\ dp^n = r_0p > r_1p > \cdots > r_tp > r_{t+1} = 0 \\ n_t > \cdots > n_1 > n_0 \geqq -1 \\ \sum_{i=0}^{t} (r_i - r_{i+1}) n_i = -mp^{l-1}}} p^{-n} \cdot c(n_0)^{r_0p - r_1p} \cdots c(n_t)^{r_tp} \cdot (r_0p, \cdots, r_tp) .$$

Then, from the above we have

$$(27)\quad H_{p,d,n}(J(\tau)) - p^{-n}J(\tau)^{dp^n} \equiv \iota^{-1}\{ \sum_{\substack{m>0 \\ (m,p)=1 \\ l \geqq 1 \\ 0 < mp^l < dp^n}} (a'^{(d,n)}_{mp^l} q^{mp^l}) - a'^{(d,n)}_0 \} \quad (\mathrm{mod}\ \boldsymbol{Z}[J(\tau)]) .$$

It is well-known that, for any rational integer a,

$$(28)\quad a^{mp^l} \equiv a^{mp^{l-1}} \quad (\mathrm{mod}\ p^l)$$

holds. We apply this to $a'^{(d,n)}_{mp^l}$; put $L = \operatorname*{Min}_{0 \leqq i \leqq t} (\mathrm{ord}_p (r_ip))$. Then from (28), we have

$$(29)\quad c(n_i)^{r_ip - r_{i+1}p} \equiv c(n_i)^{r_i - r_{i+1}} \quad (\mathrm{mod}\ p^L) .$$

From (22) in Lemma 3, we have

$$(30)\quad p^{-(n-L)}(dp^n, r_1p, \cdots, r_tp) \equiv p^{-(n-L)}(dp^{n-1}, r_1, \cdots, r_t) \quad (\mathrm{mod}\ p^L) .$$

Hence, we have from (29), (30),

$$\begin{aligned} &p^{-n}c(n_0)^{dp^n - pr_1} \cdots c(n_t)^{pr_t} \cdot (dp^n, \cdots, r_tp) \\ &\quad \equiv p^{-n} \cdot c(n_0)^{dp^{n-1} - r_1} \cdots c(n_t)^{r_t} \cdot (dp^{n-1}, \cdots, r_t) \quad (\mathrm{mod}\ 1) . \end{aligned}$$

It follows that

$$(31)\quad a'^{(d,n)}_{mp^l} \equiv p^{-1} a^{(d,n-1)}_{mp^{l-1}} \quad (\mathrm{mod}\ 1) .$$

And, also we have

$$(32)\quad a'^{(d,n)}_{mp^l} \cdot p^l \in \boldsymbol{Z} ;$$

since, $-mp^l = \sum_{i=0}^{t} (pr_i - pr_{i+1}) n_i$ and $l \geqq L$, the p^L-multiple of the corresponding term in $a'^{(d,n)}_{mp^l}$ belongs to $\boldsymbol{Z}$.

With these preparations, the proof proceeds as follows by using induction on $N = d \cdot p^n$; it is easily seen that $H_{p,1,0}(J(\tau)) = \iota^{-1}(q^{-1}) = J(\tau) - 744$, and, $H_{p,1,1}(J(\tau)) = \iota^{-1}(p^{-1} \cdot q^{-1}) \equiv p^{-1}J(\tau)^p - p^{-1} \cdot 744$ (mod $\boldsymbol{Z}[J(\tau)]$). Hence, in case $dp^n = 1 \cdot p^1$, the proposition is valid. From (27), it follows that,

$$H_{p,d,n}(J(\tau))-p^{-n}J(\tau)^{dp^n}\equiv\iota^{-1}\Big(\sum_{\substack{m>0\\(m,p)=1\\l\geqq 1\\mp^l<dp^n}}(-a'^{(d,n)}_{mp^l}\cdot q^{-mp^l})-a'^{(d,n)}_0\Big)\quad(\bmod\ \boldsymbol{Z}[J(\tau)])$$

$$\equiv\sum_{\substack{m>0\\(m,p)=1\\l\geqq 1\\mp^l<dp^n}}-a'^{(d,n)}_{mp^l}\cdot p^l\cdot H_{p,m,l}(J(\tau))-a'^{(d,n)}_0\quad(\bmod\ \boldsymbol{Z}[J(\tau)])\,.$$

From (31), (32) and the induction assumption, we have

$$H_{p,d,n}(J(\tau))-p^{-n}J(\tau)^{dp^n}\equiv\sum_{\substack{m>0\\(m,p)=1\\l\geqq 1\\mp^l<dp^n}}-a^{(d,n-1)}_{mp^{l-1}}\cdot p^{l-1}\cdot p^{-1}H_{p,m,l-1}(J(\tau)^p)-p^{-1}a_0^{(d,n)}\quad(\bmod\ \boldsymbol{Z}[J(\tau)])\,.$$

$$\equiv p^{-1}H_{p,d,n-1}(J(\tau)^p)-p^{-1}\cdot p^{-(n-1)}\cdot J(p\tau)^{d\cdot p^{n-1}\cdot p}\quad(\bmod\ \boldsymbol{Z}[J(\tau)])\,.\qquad\text{q.e.d.}$$

COROLLARY. *Let* $H_{p,d,n}(J(\tau))=\sum_{\substack{m>0\\(m,p)=1\\l\geqq 0\\mp^l<dp^n}}b^{(d,n)}_{mp^l}J(\tau)^{mp^l}+b_0^{(d,n)}$, *with* $b_i^{(d,n)}\in\boldsymbol{Q}$, $0\leqq i\leqq dp^n$. *Then* $p^l\cdot b^{(d,n)}_{mp^l}$ *belongs to* $\boldsymbol{Z}$.

PROOF. We shall use induction on n with $N=d\cdot p^n$. By the above proposition, we have for any $n\geqq 1$,

$$H_{p,d,n}(X)\equiv p^{-1}\cdot H_{p,d,n-1}(X^p)\quad(\bmod\ \boldsymbol{Z}[X])\,.\tag{33}$$

Hence, if $l\geqq 1$, we have $b^{(d,n)}_{mp^l}\equiv p^{-1}\cdot b^{(d,n-1)}_{mp^{l-1}}$ (mod $\boldsymbol{Z}$). It follows that, $l\geqq 1$, $p^l\cdot b^{(d,n)}_{mp^l}\equiv p^{l-1}\cdot b^{(d,n-1)}_{mp^{l-1}}$ (mod $\boldsymbol{Z}$). If $l=0$, from (33), $b_m^{(d,n)}$ belongs to $\boldsymbol{Z}$. Since it is obvious that $H_{p,d,0}(J(\tau))=\iota^{-1}(q^{-d})\in\boldsymbol{Z}[J(\tau)]$, the induction assumption for $N=d\cdot p^0$ holds.

q.e.d.

5 4. From these facts, we shall prove the following.

PROPOSITION 7. *Let* $m\geqq 1$ *and* $n\geqq 1$ *be rational integers. Then the following congruence is valid;*

$$J(\tau)^d\,|\,U(p)^n\equiv\sum_{\substack{0<mp^l<dp^n\\(m,p)=1\\l\geqq 1}}a_{m,l,d,n}\cdot p^{-l}(J(\tau)^{mp^l}-J(p\tau)^{mp^{l-1}})\quad(\bmod\ \boldsymbol{Z}[J(\tau)])\,,$$

with $a_{m,l,d,n}\in\boldsymbol{Z}$.

PROOF. It is well-known that $J(\tau)^d|T_0(p^n)$ belongs to $\boldsymbol{Q}[J(\tau)]$. Let $J(\tau)^d\equiv\sum_{\substack{0<mp^l<d\\(m,p)=1\\l\geqq 0}}c_{mp^l}\cdot q^{-mp^l}+c_0$ (mod $q\cdot\boldsymbol{Q}[[q]]$), with $c_{mp^l}\in\boldsymbol{Z}$. Then, we have

$$J(\tau)^d|T_0(p^n)=\sum_{\substack{0<mp^l<d\\(m,p)=1\\l\geqq 0}}c_{mp^l}\,\iota^{-1}(q^{-mp^l}|T_0(p^n))+c_0|T_0(p^n)\,.$$

From (3) in § 1, we have

$$J(\tau)^d|U(p)^n=\sum_{\substack{0<mp^l<d\\(m,p)=1\\l\geqq 0}} c_{mp^l}\{\iota^{-1}(q^{-mp^l}|T_0(p^n))-p^{-1}\iota^{-1}(q^{-mp^l}|T_0(p^{n-1}))_{\tau\to p\tau}\}$$
$$+c_0|T_0(p^n)-p^{-1}c_0|T_0(p^{n-1}) .$$

Using Lemma 2, $q^{-mp^l}|T_0(p^n)=\sum_{i=0}^{\mathrm{Min}\,(n,l)} p^{-n+i}\cdot q^{-m\cdot p^{l+n-2i}}=\sum_{i=0}^{\mathrm{Min}\,(n,l)} p^{l-i}\cdot p^{-(l+n-2i)}\cdot$ $\cdot q^{-mp^{l+n-2i}}$. Hence, we have

$$J(\tau)^d|U(p)^n=\sum_{\substack{0<mp^l<d\\(m,p)=1\\l\geqq 0}} c_{mp^l}\{\sum_{i=0}^{\mathrm{Min}\,(n,l)} p^{l-i}\cdot H_{p,m,l+n-2i}(J(\tau))$$
$$-p^{-1}\sum_{i=0}^{\mathrm{Min}\,(n-1,l)} p^{l-i}\cdot H_{p,m,l+n-1-2i}(J(p\tau))\}+c_0 .$$

By Proposition 6,

$$J(\tau)^d|U(p)^n=\sum_{\substack{0<mp^l<d\\(m,p)=1\\n-1\geqq l\geqq 0}} c_{mp^l}\{\sum_{i=0}^{\mathrm{Min}\,(n-1,l)} p^{l-1-i}(H_{p,m,l+n-1-2i}(J(\tau)^p)$$
$$-H_{p,m,l+n-1-2i}(J(p\tau)))\}+\sum_{\substack{0<mp^l<d\\(m,p)=1\\l\geqq n}} c_{mp^l}\cdot p^{l-n}\cdot H_{p,m,l-n}(J(\tau))$$
$$(\mathrm{mod}\ \boldsymbol{Z}[J(\tau)]) . \tag{34}$$

Since $p^{l-n}\cdot H_{p,m,l-n}(J(\tau))=\iota^{-1}(q^{-mp^{l-n}})$, the last sum of (34) belongs to $\boldsymbol{Z}[J(\tau)]$. So by using Corollary of Proposition 6, we obtain Proposition 7. q.e.d.

6. Proof of Main Theorem.

Here we shall prove Theorem 1 which is a slightly extended form of the Main Theorem stated in § 1.

THEOREM 1. *Denote by M^∞ the $\mathfrak{o}_p^\infty$-module in $\boldsymbol{Q}_p^\infty(J(\tau))_{V^\infty}$ generated by $\{f\,|\,U(p)^n;$ $f\in\boldsymbol{Z}[J(\tau)], n\geqq 0\}$. Let $\alpha\geqq 1$ be a rational integer. Then for each $g\in M^\infty$, there exist $h\in\mathfrak{o}_T[J(\tau)]$, and $F(\tau)\in\mathfrak{S}_{p^\alpha-p^{\alpha-1},\mathfrak{o}_T}$ such that*

$$g-h\equiv F(\tau)\quad(\mathrm{mod}\ \tilde{\mathfrak{P}}^\alpha) . \tag{35}$$

These h and $F(\tau)$ are unique up to modulo $\tilde{\mathfrak{P}}^\alpha$.

To begin with, we show that Theorem 1 implies the Main Theorem; put $d=\dim_C\mathfrak{S}_{p^\alpha-p^{\alpha-1}}$, and let $\{F_i(\tau)\}_{i=1}^d$ be the canonical basis of $\mathfrak{S}_{p^\alpha-p^{\alpha-1}}$. Take $g\in$ M. Then, we have the following congruence by Theorem 1;

$$g-h\equiv F(\tau)\quad(\mathrm{mod}\ \tilde{\mathfrak{P}}^\alpha) ,$$

with $h\in\mathfrak{o}_T[J(\tau)]$ and $F(\tau)\in\mathfrak{S}_{p^\alpha-p^{\alpha-1},\mathfrak{o}_T}$. As the Fourier coefficients of g are all rational integers, we can take h from $\boldsymbol{Z}[J(\tau)]$ by the fact $J(\tau)=\sum_{n=-1}^{\infty}c(n)q^n$, with $c(-1)=1$ and $c(n)\in\boldsymbol{Z}$. It follows that the Fourier coefficients of $(g-h)$ are rational integers. Hence, by the properties of the canonical basis stated in § 4-2, we can take $F(\tau)$ from $\mathfrak{S}_{(p^\alpha-p^{\alpha-1}),Z}$. q.e.d.

We prove this theorem using Propositions 4, 5 and 7, and the theorem of Deligne about the p-adic rigidity of the map $J(\tau)\to J(p\tau)$. Deligne's theorem reads as follows; we showed that $J(p\tau)$ belongs to $\boldsymbol{Q}(J(\tau))_V$, therefore, to $\boldsymbol{Q}_p^\infty(J(\tau))_{V^\infty}$. Hence $J(p\tau)$ has a V^∞-adic expansion. Deligne's theorem gives this V^∞-adic expansion of $J(p\tau)$ explicitly in the following form,

$$J(p\tau)=J(\tau)^p+p\cdot H+\sum_{\theta\in S}\sum_{n=1}^{\infty}A_n^{(\theta)}(J(\tau)-j_\theta)^{-n}\,, \tag{36}$$

with $H\in\boldsymbol{Z}[J(\tau)]$ such that $J(\tau)|T_0(p)=p^{-1}J(\tau)^p+H$, and $A_n^{(\theta)}\in\mathfrak{o}_p^\infty$, S and j_θ being the same as in Proposition 3. Furthermore, Deligne's theorem gives the evaluation of $\mathrm{ord}_p A_n^{(\theta)}$ as follows; for $p\geqq5$, and $n\geqq1$, we have

$$\mathrm{ord}_p A_n^{(\theta)}\geqq\begin{cases}\dfrac{1}{p+1}+\dfrac{np}{p+1} & \text{if } \theta\in S^*\,,\\[2mm] \dfrac{1}{p+1}+\dfrac{3np}{p+1} & \text{if } \theta=0\in S\,,\\[2mm] \dfrac{1}{p+1}+\dfrac{2np}{p+1} & \text{if } \theta=12^3\in S\,.\end{cases} \tag{37}$$

For $p=2$, 3, and $n\geqq1$, we have

$$\mathrm{ord}_p A_n\geqq\begin{cases}\dfrac{11}{2}+\dfrac{13}{2}n & \text{for } p=2\,,\\[2mm] \dfrac{5}{2}+\dfrac{7}{2}n & \text{for } p=3\,.\end{cases} \tag{38}$$

As for Deligne's theorem, we refer to Dwork [5] (p. 80).

Proof of Theorem 1. First, we briefly sketch the proof; for any $F(\tau)\in\mathfrak{S}_{p^\alpha-p^{\alpha-1},\mathfrak{o}_T}$, in Propositions 4, 5, we calculated $F(\tau)\pmod{\mathfrak{P}^\alpha}$ to be a rational function of $J(\tau)\pmod{\mathfrak{P}^\alpha}$ in a definite form. On the other hand, by Proposition 7 and Deligne's theorem, we shall show that, for each $g\in M^\infty$, $g\pmod{\tilde{\mathfrak{P}}^\alpha}$ can be calculated to be a sum of some $h\in\mathfrak{o}_T[J(\tau)]$ and of some rational function of $J(\tau)$ in the same definite type as above modulo $\tilde{\mathfrak{P}}^\alpha$. Hence we obtain Theorem 1 by the 'surjectivity' of the reduction mod p^α of cusp forms in Propositions 4, 5.

To begin with, we need the following elementary lemma.

LEMMA 4. *Let K be a field with an additive, discrete valuation V. Let $\mathfrak{O}$ be the valuation ring of V and let π be a prime element of V. Let $r \in K(X)$ be such an element that*

$$r=\frac{b\cdot F(X)}{\prod_{i=1}^{m}(X-a_i)^{e_i}}, \tag{39}$$

with $m\geqq 1$, $e_i\geqq 1$ $(i=1,\cdots,m)$, and b, $a_i\in\mathfrak{O}$ $(i=1,\cdots,m)$, and $F(X)\in\mathfrak{O}[X]$. Assume that $V(a_i-a_j)=0$ for any $1\leqq i<j\leqq m$. Then we have the following, unique partial fractional expansion of r;

$$r=\sum_{i=1}^{m}\sum_{j=1}^{e_i}\frac{b_{ij}}{(X-a_i)^j}+G(X)$$

with $b_{ij}\in\mathfrak{O}$ $(i=1,\cdots,m, j=1,\cdots,e_i)$, and $G(X)\in\mathfrak{O}[X]$ such that $V(b_{ij})\geqq V(b)$ and $G(X)\in\pi^{V(b)}\mathfrak{O}[X]$.

PROOF. Since the uniqueness of the partial fractional expansions is well-known, we only prove that the evaluation of the coefficients b_{ij} and of $G(X)$ with respect to V are given by the above. In case $m=1$, the assertion is obviously valid since, for each $F(X)\in\mathfrak{O}[X]$, we have $F(X)=\sum_{l=0}^{N}c_l(X-a_1)^l$ with some N and $c_l\in\mathfrak{O}$ $(i=1,\cdots,N)$. In general case, we use induction on m and e_m; we may assume $F(a_i)\neq 0$ for $i=1,\cdots,m$. Let $m_0>1$ be a rational integer. Assume that the assertion is valid for any $1\leqq m<m_0$. From (39), we have $r\cdot(X-a_{m_0})^{e_{m_0}}|_{X=a_{m_0}}=b_{m_0\cdot m_0}$. On the other hand, $r\cdot(X-a_{m_0})^{e_{m_0}}|_{X=a_{m_0}}=\dfrac{b\cdot F(a_{m_0})}{\prod_{i=1}^{m_0-1}(a_{m_0}-a_i)^{e_i}}$. Since $V(a_{m_0}-a_i)=0$ for $1\leqq i<m_0$, $\prod_{i=1}^{m_0-1}(a_{m_0}-a_i)^{e_i}$ is a V-adic unit; it followst hat $V(b_{m_0\cdot e_{m_0}})\geqq V(b)$. Hence we have

$$r-\frac{b_{m_0\cdot e_{m_0}}}{(X-a_{m_0})^{e_{m_0}}}=\frac{b\cdot F_1(X)}{(\prod_{i=1}^{m_0-1}(X-a_i)^{e_i})(X-a_{m_0})^{e_{m_0}-1}},$$

with $F_1(X)\in\mathfrak{O}[X]$. Therefore, using induction on e_{m_0}, we conclude the assertion is valid in $m=m_0$. q.e.d.

Hereafter, since the proof for $p\geqq 5$ and that for $p=2$, 3 are entirely similar, we prove only for $p\geqq 5$ and we write only the results for $p=2$, 3. Now the first step of the proof is to give the following; let $m\geqq 1$ be a rational integer. Then we have

$$J(p\tau)^m=J(\tau)^{mp}+ph_1+\sum_{\theta\in S}\sum_{n=1}^{\infty}B_n^{(\theta)}(J(\tau)-j_\theta)^{-n},$$

with $h_1 \in \mathfrak{o}_p^\infty[J(\tau)]$ and $B_n^{(\theta)} \in \mathfrak{o}_p^\infty$. Moreover, the evaluation of $\mathrm{ord}_p B_n^{(\theta)}$ is given by the same equation as $\mathrm{ord}_p A_n^{(\theta)}$ in (37); namely, for $p \geqq 5$, $n \geqq 1$ we have

$$\mathrm{ord}_p B_n^{(\theta)} \geqq \begin{cases} \dfrac{1}{p+1} + \dfrac{np}{p+1} & \text{if } \theta \in S^*, \\[2ex] \dfrac{1}{p+1} + \dfrac{3np}{p+1} & \text{if } \theta = 0 \in S, \\[2ex] \dfrac{1}{p+1} + \dfrac{2np}{p+1} & \text{if } \theta = 12^3 \in S, \end{cases} \tag{40}$$

and for $p=2$, 3 so on. Put $J(p\tau)=J(\tau)^p+pR$ with $R \in \boldsymbol{Q}(J(\tau))_V$. Then, R is the sum of infinite terms which consist of $\{p^{-1}\cdot A_n^{(\theta)}\cdot(J(\tau)-j_\theta)^{-n}\}$ with $\theta \in S$, $n \geqq 1$, and of a polynomial $H \in \boldsymbol{Z}[J(\tau)]$. Hence, we have

$$J(p\tau)^m = J(\tau)^{mp} + \sum_{s=1}^{m} p^s \cdot \binom{m}{s} \cdot R^s \cdot J(\tau)^{p(m-s)} .$$

Then R^s is the sum of infinite terms which consist of $\{\prod_{i=1}^{s'} p^{-1}\cdot A_{n_i}^{(\theta_i)}\cdot(J(\tau)-j_{\theta_i})^{-n_i}\cdot \cdot H^{s-s'}\}$ with $1 \leqq s' \leqq s$, and of H^s. By the above lemma, the evaluation with respect to ord_p of the coefficients of the partial fractional expansion of $p^s\cdot\binom{m}{s}\cdot \prod_{i=1}^{s'} p^{-1}\cdot A_{n_i}^{(\theta_i)}\cdot(J(\tau)-j_{\theta_i})^{-n_i}\cdot H^{s-s'}\cdot J(\tau)^{p(m-s)}$ is given by the following; if $B_n'^{(\theta)}$ is the coefficient of $(J(\tau)-j_\theta)^{-n}$ in this partial fractional expansion, we have $\mathrm{ord}_p B_n'^{(\theta)} \geqq s+\sum_{i=1}^{s'}(\mathrm{ord}_p A_{n_i}^{(\theta_i)}-1)$ and $n \leqq \sum_{i=1}^{s'} n_i$. Moreover, the ord_p of the coefficients of the polynomial part is not smaller than $s+\sum_{i=1}^{s'}(\mathrm{ord}_p A_{n_i}^{(\theta_i)}-1)$, and its polynomial degree is bounded by pm. Hence, we have for $\theta \in S^*$,

$$\begin{aligned} \mathrm{ord}_p B_n'^{(\theta)} &\geqq s+\sum_{i=1}^{s'}(\mathrm{ord}_p A_{n_i}^{(\theta_i)}-1) \geqq (s-s')+\frac{s'}{p+1}+\frac{p}{p+1}\sum_{i=1}^{s'} n_i , \\ &\geqq \frac{1}{p+1}+\frac{np}{p+1} . \end{aligned}$$

Similarly, if 0 (resp. 12^3) is contained in S, we have $\mathrm{ord}_p B_n'^{(0)} \geqq \dfrac{1}{p+1}+\dfrac{3np}{p+1}$ $\left(\text{resp. } \mathrm{ord}_p B_n'^{(12^3)} \geqq \dfrac{1}{p+1}+\dfrac{2np}{p+1}\right)$. Since $B_n^{(\theta)}$ is the sum of these $B_n'^{(\theta)}$, we obtain the equation (40). Concerning to the polynomial part h_1, h_1 is the sum of the polynomial part of each partial fractional expansions of $\left\{p^s\cdot\binom{m}{s}\cdot\prod_{i=1}^{s'} p^{-1}A_{n_i}^{(\theta_i)}(J(\tau)-j_{\theta_i})^{-n_i} \cdot H^{s-s'}\cdot J(\tau)^{p(m-s)}\right\}$ with $1 \leqq s \leqq m$, and $1 \leqq s' \leqq s$, and of H^s with $1 \leqq s \leqq m$. Since the polynomial degree of each polynomial part is bounded and the ord_p of its coefficients is not smaller than $s+\sum_{i=1}^{s'}(\mathrm{ord}_p A_{n_i}^{(\theta_i)}-1)$, h_1 becomes an element of

$\mathfrak{o}_p^\infty[J(\tau)]$.

Next step is to show the following; Let $m \geqq 1$ be rational integer such that $(m, p)=1$ and let $l \geqq 1$ be a rational integer. Then we have

$$p^{-l}(J(\tau)^{mp^l} - J(p\tau)^{mp^{l-1}}) = h_2 + \sum_{\theta \in S} \sum_{n=1}^{\infty} C_n^{(\theta)} (J(\tau) - j_\theta)^{-n}\,, \tag{41}$$

with $h_2 \in \mathfrak{o}_p^\infty[J(\tau)]$ and $C_n^{(\theta)} \in \mathfrak{o}_p^\infty$. Moreover the evaluation of the coefficients $C_n^{(\theta)}$ with respect to ord_p is given by, for $p \geqq 5$,

$$\mathrm{ord}\, C_n^{(\theta)} \geqq \begin{cases} \dfrac{np}{p+1} - \dfrac{1}{p+1} - 1 & \text{if } \theta \in S^*\,, \\[2ex] \dfrac{3np}{p+1} - \dfrac{1}{p+1} - 1 & \text{if } \theta = 0 \in S\,, \\[2ex] \dfrac{2np}{p+1} - \dfrac{1}{p+1} - 1 & \text{if } \theta = 12^3 \in S\,, \end{cases} \tag{42}$$

and for $p=2$, 3,

$$\mathrm{ord}\, C_n \geqq \begin{cases} \dfrac{13}{2} n + \dfrac{11}{2} - 1 & \text{for } p=2\,, \\[2ex] \dfrac{5}{2} n + \dfrac{5}{2} - 1 & \text{for } p=3\,. \end{cases} \tag{43}$$

We make the similar argument to the first step. Put $J(p\tau)^m = J(\tau)^{mp} + pR_1$ with $R_1 \in \boldsymbol{Q}_p(J(\tau))_{V^\infty}$. Then we have

$$J(\tau)^{mp^{l-1}} = J(\tau)^{mp^l} + \sum_{s=1}^{p^{l-1}} p^s \cdot \binom{p^{l-1}}{s} R_1^s \cdot J(\tau)^{mp(p^{l-1}-s)}\,.$$

R_1 is the sum of infinite terms which consist of $\{p^{-1} \cdot B_n^{(\theta)} \cdot (J(\tau) - j_\theta)^{-n}\}$ with $\theta \in S$, $n \geqq 1$, and of $h_1 \in \mathfrak{o}_p^\infty[J(\tau)]$. Hence R_1^s, for $1 \leqq s \leqq p^{l-1}$, is also the sum of infinite terms which consist of $\{\prod_{i=1}^{s'} p^{-1} \cdot B_{n_i}^{(\theta_i)} \cdot (J(\tau) - j_{\theta_i})^{-n_i} \cdot h_1^{s-s'}\}$ with $1 \leqq s' \leqq s$, and of h_1^s. By Lemma 4, the evaluation with respect to ord_p of the coefficients in the partial fractional expansions of $p^s \cdot \binom{p^{l-1}}{s} \cdot \prod_{i=1}^{s'} p^{-1} \cdot B_{n_i}^{(\theta_i)} \cdot (J(\tau) - j_{\theta_i})^{-n_i} \cdot h_i^{s-s'}$ is given by the following; if $C_n'^{(\theta)}$ is the coefficient of $(J(\tau) - j_\theta)^{-n}$ in this partial fractional expansion, we have $\mathrm{ord}_p\, C_n'^{(\theta)} \geqq s + \mathrm{ord}_p \binom{p^{l-1}}{s} + \sum_{i=1}^{s'} (\mathrm{ord}_p\, B_{n_i}^{(\theta_i)} - 1)$ and $n \leqq \sum_{i=1}^{s'} n_i$. Moreover the ord_p of the coefficient of the polynomial part is not smaller than $s + \mathrm{ord}_p \binom{p^{l-1}}{s} + \sum_{i=1}^{s'} (\mathrm{ord}_p\, B_{n_i}^{(\theta_i)} - 1)$ and the polynomial degree is bounded by $p^l \cdot m$. Hence, by Lemma 3, we have

$$\mathrm{ord}_p\, C_n'^{(\theta)} \geqq s + l - 1 - \mathrm{ord}_p\, s + \sum_{i=1}^{s'} (\mathrm{ord}_p\, B_{n_i}^{(\theta_i)} - 1)$$

$$\geqq (s-s')+l-1-\operatorname{ord}_p s+\frac{s'}{p+1}+\frac{np}{p+1}$$

$$\geqq \frac{np}{p+1}+\frac{s}{p+1}+l-1-\operatorname{ord}_p s\,.$$

Therefore, for (42), it is sufficient to prove

$$\frac{s}{p+1}-\operatorname{ord}_p s-1\geqq -\frac{1}{p+1}-1\,,\quad \text{for } s\geqq 1\,. \tag{44}$$

This is equivalent to show that,

$$p^t+1-(p+1)t\geqq 0\,,\qquad \text{for } t\geqq 0\,.$$

If $t=0$, we have $p^0+1-(p+1)\cdot 0=2$, and if $t=1$, we have $p^1+1-(p+1)=0$. For $t\geqq 2$ we use induction on t; if $t=2$, we have $p^2+1-2(p+1)=(p-1)^2-2>0$ since $p\geqq 5$. We have $p^{t+1}+1-(p+1)(t+1)\geqq p\{(p+1)t-1\}+1-(p+1)(t+1)=p^2t-2p-t=t(p^2-1)-2p\geqq p^2-1-2p=(p-1)^2-2>0$. From (44) we have $s+\operatorname{ord}_p\binom{p^{l-1}}{s}+\sum_{i=1}^{s'}(\operatorname{ord}_p B_{n_i}^{(\theta_i)}-1)-l\geqq\frac{np}{p+1}-\frac{1}{p+1}-1=-\frac{2}{p+1}>-1$. Hence the polynomial part of each partial fractional expansions in (41) belongs to $\mathfrak{o}_p^\infty[J(\tau)]$. Therefore we obtain the second step.

Put $n_\alpha=[p^{-1}\{\alpha(p+1)+1\}]$, $n'_\alpha=[(3p)^{-1}\{\alpha(p+1)+1\}]$ and $n''_\alpha=[(2p)^{-1}\{\alpha(p+1)+1\}]$. We prove that,

$$n_\alpha\leqq p^{\alpha-1}\,,\quad n'_\alpha\leqq\left[\frac{1}{3}\,p^{\alpha-1}\right]\ \text{and}\ n''_\alpha\leqq\left[\frac{1}{2}\,p^{\alpha-1}\right]. \tag{45}$$

If $\alpha=1$, we have $n_1=[p^{-1}(p+2)]=1$, and $n'_1=n''_2=0$; hence (45) is valid for $\alpha=1$. For $\alpha\geqq 2$, we shall prove that $p^\alpha-\alpha(p+1)+1\geqq 0$; from this, (45) is obviously valid. If $\alpha=2$, we have $p^2-2(p+1)-1=(p-1)^2-4>0$ since $p\geqq 5$. For $\alpha\geqq 3$, we use induction on α; $p^{\alpha+1}-\{(\alpha+1)(p+1)+1\}\geqq p\{\alpha(p+1)+1\}-\{(\alpha+1)(p+1)+1\}\geqq\alpha(p^2-1)-2>0$.

Finally we prove Theorem 1. For this, it is sufficient to prove (14) only for $g=J(\tau)^d\,|\,U(p)^n$. By Proposition 7 and (41), we have

$$g\equiv h+\sum_{\theta\in S}\sum_{n=1}^{n^{(\theta)}}a_n^{(\theta)}(J(\tau)-j_\theta)^{-n}\qquad(\operatorname{mod}\tilde{\mathfrak{P}}^\alpha)\,,$$

with $h\in\mathfrak{o}_T[J(\tau)]$, and $a_n^{(\theta)}\in\mathfrak{o}_T$. Here for $\theta\in S^*$ $n^{(\theta)}$ is the maximum integer such that $\frac{n^{(\theta)}}{p+1}-\frac{1}{p+1}-1\leqq\alpha-1$, and $n^{(0)}$, $n^{(12^3)}$ are the maximum integer such that $\frac{3n^{(0)}}{p+1}-\frac{1}{p+1}-1\leqq\alpha-1$, $\frac{2n^{(12^3)}}{p+1}-\frac{1}{p+1}-1\leqq\alpha-1$ respectively. Hence we have $n^{(\theta)}=n_\alpha$ for $\theta\in S^*$, $n^{(0)}=n'_\alpha$ and $n^{(12^3)}=n''_\alpha$. Therefore from (45) and Proposition 4, we obtain (14). q.e.d.

PART II. APPLICATIONS TO THE CONJECTURE OF ATKIN

7. p-adic Hecke operators

Now in the following sections we deal with the applications of the facts we proved so far, mainly Propositions 4, 5 and Theorem 1, to the conjecture of Atkin. It is performed as follows. Atkin asserts in [1] the following:

Conjecture. Let $p\leqq 23$ be a prime number and l be a prime other than p. Put $t_\alpha(n)=c(p^\alpha n)/c(p^\alpha)$ with the Fourier coefficients $c(n)$ of $J(\tau)$ in (4). Then it holds that,

$$t_\alpha(nl)-t_\alpha(n)t_\alpha(l)+l^{-1}t_\alpha\left(\frac{n}{l}\right)\equiv 0 \qquad (\mathrm{mod}\ p^\alpha)\,,$$

$$t_\alpha(np)-t_\alpha(n)t_\alpha(p)\equiv 0 \qquad (\mathrm{mod}\ p^\alpha)\,,$$

where $t_\alpha\left(\frac{n}{l}\right)$ is defined to be zero if n is not divisible by l. Moreover, examining the case for large primes by the aid of a computer, he asserts a conjecture of similar type for general primes. Atkin says in [1] that he proved this conjecture for $p=2, 3, 5, 7, 13$, but it seems that they are not published yet.

First we define certain p-adic Banach spaces and p-adic Hecke operators acting on them. The conjecture of Atkin is closely connected with the existence and the construction of simultaneous eigenfunctions of p-adic Hecke operators on the space $\mathscr{S}^{(0)}$. Secondly, we shall prove the conjecture of Atkin for $p=13$ completely, studying eigenfunctions of a p-adic Hecke operator $\tilde{U}_0(13)$ on $\mathscr{S}^{(0)}$ by the result of Atkin and O'Brien on modular functions with respect to $\Gamma_0(13)$ ([3]). At last, we shall show that, if we assume certain assertions, the same procedure of the proof in the case $p=13$ is applicable to the general case. However, new assumptions themselves have not been proved yet.

7-1. Let $p\geqq 5$ be a prime number, and let λ be an even rational integer. For any positive integer α, put $V_\alpha^{(\lambda)}=\mathfrak{S}_{\lambda+p^\alpha-p^{\alpha-1},\mathfrak{o}_T}$ and put $d_\alpha^{(\lambda)}=\dim_C\mathfrak{S}_{\lambda+p^\alpha-p^{\alpha-1}}$.

PROPOSITION 8. *Let $\alpha'>\alpha$ be two positive rational integers. Then for each $F\in V_\alpha^{(\lambda)}$, there exists $F'\in V_{\alpha'}^{(\lambda)}$ such that,*

$$F'\equiv F \quad (\mathrm{mod}\ \tilde{\mathfrak{P}}^\alpha)\,,$$

and F' is unique up to modulo $\tilde{\mathfrak{P}}^\alpha$.

PROOF. From Remark 2 of Proposition 4, it follows that there exists a regular form G of weight $(p^{\alpha'-\alpha}-1)(p^\alpha-p^{\alpha-1})$ with respect to Γ whose Fourier coefficients are all rational integers, satisfying $G\equiv 1 \pmod{\widetilde{\mathfrak{P}}^{\alpha}}$. Put $F'=F\cdot G$. Then F' belongs to $V_{\alpha}^{(\lambda)}$ and it holds that $F'\equiv F \pmod{\widetilde{\mathfrak{P}}^{\alpha}}$. q.e.d.

From this proposition, it follows that there exists a system of free basis $\{F_{\alpha,i}^{(\lambda)}\}_{i=1}^{d_{\alpha}^{(\lambda)}}$ of $V_{\alpha}^{(\lambda)}$ over $\mathfrak{o}_T$ such that $F_{\alpha,i}^{(\lambda)}\equiv F_{\alpha',i}^{(\lambda)} \pmod{\widetilde{\mathfrak{P}}^{\alpha}}$ for any $\alpha'>\alpha$. Hence the sequence $\{F_{\alpha,i}^{(\lambda)}\}_{\alpha=1}^{\infty}$ has a $\widetilde{\mathfrak{P}}$-adic limit in $q\cdot\mathfrak{o}_p^{\infty}[[q]]$, and it will be denoted by $\widetilde{F}_i^{(\lambda)}$. We call this system of free basis of $V_{\alpha}^{(\lambda)}$ *the compatible system of free basis of* $V_{\alpha}^{(\lambda)}$. Let $\mathscr{S}^{(\lambda)}$ be a p-adic Banach space admitting the orthonormal basis $\{\widetilde{F}_i^{(\lambda)}\}_{i=1}^{\infty}$ over $\boldsymbol{Q}_p^{\infty}$. For the definition of a p-adic Banach space with an orthonormal basis, we refer to Serre [12]. Namely, by definition, $\mathscr{S}^{(\lambda)}$ consists of all the elements $\sum_{i=1}^{\infty} a_i\widetilde{F}_i^{(\lambda)}$ with $a_i\in\boldsymbol{Q}_p^{\infty}$, such that there are only finitely many a_i with $\mathrm{ord}_p\, a_i<t$ for any positive number t. Therefore $\mathscr{S}^{(\lambda)}$ is contained in $q\cdot\boldsymbol{Q}_p^{\infty}[[q]]$.

Proposition 9. (1) $\mathscr{S}^{(\lambda)}$ *does not depend on the choice of the compatible system of free basis of* $V_{\alpha}^{(\lambda)}$. (2) $\mathfrak{S}_{\lambda,\mathfrak{o}_T}$ *is contained in* $\mathscr{S}^{(\lambda)}$. (3) *For each* $F\in\mathscr{S}^{(\lambda)}$, $F'\in\mathscr{S}^{(\lambda')}$, $F\cdot F'$ *belongs to* $\mathscr{S}^{(\lambda+\lambda')}$. *Especially* $\mathscr{S}^{(0)}$ *is a ring.* (4) $\{(J(\tau)-j_{\theta})^{-n}\}_{\substack{1\leqq n<\infty\\ \theta\in S}}$ *forms an orthonormal basis of* $\mathscr{S}^{(0)}$.

Proof. (1) Let $\{F_{\alpha,i}'^{(\lambda)}\}$ be another compatible system of free basis of $V_{\alpha}^{(\lambda)}$ over $\mathfrak{o}_T$. Put $\widetilde{F}_i'^{(\lambda)}=\lim\limits_{\alpha\to\infty} F_{\alpha,i}'^{(\lambda)}$. Then for any α, there exist $a_{ij}\in\mathfrak{o}_T$, $1\leqq j\leqq d_{\alpha}^{(\lambda)}$, such that $F_{\alpha,i}'^{(\lambda)}=\sum_{j=1}^{d_{\alpha}^{(\lambda)}} a_{ij}F_{\alpha,j}^{(\lambda)}$. Hence we have $\widetilde{F}_i'^{(\lambda)}\equiv\sum_{j=1}^{d_{\alpha}^{(\lambda)}} a_{ij}\widetilde{F}_j^{(\lambda)} \pmod{\widetilde{\mathfrak{P}}^{\alpha}}$, so $\widetilde{F}_i'^{(\lambda)}$ belongs to $\mathscr{S}^{(\lambda)}$.

(2) By the same reason of the proof of Proposition 8, it is proved that there exists a certain regular form G_{α} of weight $p^{\alpha}-p^{\alpha-1}$ with respect to Γ whose Fourier coefficients are rational integers satisfying $G_{\alpha}\equiv 1 \pmod{\widetilde{\mathfrak{P}}^{\alpha}}$. Therefore, for any $F\in\mathfrak{S}_{\lambda,\mathfrak{o}_T}$, $F\cdot G_{\alpha}$ belongs to $V_{\alpha}^{(\lambda)}$ and it holds that $\lim\limits_{\alpha\to\infty} F\cdot G_{\alpha}=F$.

(3) Let $\{F_{\alpha,i}^{(\lambda)}\}$, $\{F_{\alpha,j}^{(\lambda')}\}$, $\{F_{\alpha,l}^{(\lambda+\lambda')}\}$ be each compatible systems of free basis. For each $F_{\alpha,i}^{(\lambda)}\in V_{\alpha}^{(\lambda)}$, $F_{\alpha,j}^{(\lambda')}\in V_{\alpha}^{(\lambda')}$, $F_{\alpha,i}^{(\lambda)}\cdot F_{\alpha,j}^{(\lambda')}$ belongs to, $\mathfrak{S}_{\lambda+\lambda'+2(p^{\alpha}-p^{\alpha-1})}$. By Proposition 4, there exist $a_l\in\mathfrak{o}_T$, for $1\leqq l\leqq d_{\alpha+1}^{(\lambda+\lambda')}$, such that $F_{\alpha,i}^{(\lambda)}\cdot F_{\alpha,j}^{(\lambda')}\equiv\sum_{l=1}^{d_{\alpha+1}^{(\lambda+\lambda')}} a_lF_{\alpha+1,l}^{(\lambda+\lambda')} \pmod{\widetilde{\mathfrak{P}}^{\alpha}}$, so that we have $\widetilde{F}_i^{(\lambda)}\cdot\widetilde{F}_j^{(\lambda')}\equiv\sum_{l=1}^{d_{\alpha+1}^{(\lambda+\lambda')}} a_l\widetilde{F}_l^{(\lambda+\lambda')} \pmod{\widetilde{\mathfrak{P}}^{\alpha}}$. Hence $\widetilde{F}_i^{(\lambda)}\cdot\widetilde{F}_j^{(\lambda')}$ belongs to $\mathscr{S}^{(\lambda+\lambda')}$.

(4) By Proposition 4, we can choose a compatible system of free basis $\{F_{\alpha,i}^{(0)}\}$ of $V_{\alpha}^{(0)}$ such that $F_{\alpha,i}^{(0)}\equiv(J(\tau)-j_{\theta})^{-k} \pmod{\widetilde{\mathfrak{P}}^{\alpha}}$ with some k, $\theta\in S$, and by its Remark 3, for any $(J(\tau)-j_{\theta})^{-k}$, there exist some α and i such that $F_{\alpha,i}^{(0)}\equiv(J(\tau)-j_{\theta}{}^{-k}) \pmod{\widetilde{\mathfrak{P}}^{\alpha}}$. Hence we have $\lim\limits_{\alpha\to\infty} F_{\alpha,i}^{(0)}=(J(\tau)-j_{\theta})^{-k}$. q.e.d.

An element $\sum_{i=1}^{\infty} a_i\widetilde{F}_i$ in $\mathscr{S}^{(\lambda)}$ such that all a_i belong to $\mathfrak{o}_p^{\infty}$ will be called an integral element. This does not depend on the choice of the compatible system of free basis of $V_{\alpha}^{(\lambda)}$.

7-2. We shall define the p-adic Hecke operators on $\mathscr{S}^{(\lambda)}$, which are seemed to be the counterpart of the classical Hecke operators in this case. Before this, we recall briefly the classical Hecke operator theory. Let $k \geqq 12$ be an even rational integer and let l be any prime number. Denote by $\mathfrak{S}_k$ the space of cusp forms of weight k with respect to Γ. The Hecke operators $T_k(l)$ on $\mathfrak{S}_k$ are defined by

$$F(\tau)\,|\,T_k(l) = \sum_{n=1}^{\infty} \left\{ a(nl) + l^{k-1} a\left(\frac{n}{l}\right) \right\} \cdot q^n ,$$

for $F(\tau) = \sum_{n=1}^{\infty} a(n) \cdot q^n \in \mathfrak{S}_k$, with $a(n) \in \boldsymbol{C}$. Here $a\left(\frac{n}{l}\right)$ is defined to be zero if n is not divisible by l. $T_k(l)$ are mutually commutative.

PROPOSITION 10. *Let l be any prime other than p. Then for any $\tilde{F} = \sum_{n=1}^{\infty} A(n) \cdot q^n \in \mathscr{S}^{(\lambda)}$ with $A(n) \in Q_p^{\infty}$, both $\sum_{n=1}^{\infty} A(np) \cdot q^n$ and $\sum_{n=1}^{\infty} \left\{ A(nl) + l^{\lambda-1} A\left(\frac{n}{l}\right) \right\} q^n$ belong to $\mathscr{S}^{(\lambda)}$.*

PROOF. Let $\{F_{\alpha,i}^{(\lambda)}\}$ be the compatible system of free basis of $V_\alpha^{(\lambda)}$. We may assume that $\tilde{F}$ is integral, namely $\tilde{F} = \sum_{i=1}^{\infty} a_i \tilde{F}_i$ with $a_i \in \boldsymbol{Q}_p^{\infty}$. Then $\tilde{F}$ is congruent modulo $\mathfrak{P}^\alpha$ to a finite sum of these $a_i \tilde{F}_i$. It follows that, by Proposition 4, there exist some rational integer k_α and $F_\alpha(\tau) \in \mathfrak{S}_{\lambda+k_\alpha(p^\alpha-p^{\alpha-1}),\,\mathfrak{o}_T}$ such that $\tilde{F} \equiv F_\alpha(\tau)$ (mod $\tilde{\mathfrak{P}}^\alpha$). Put $F_\alpha(\tau) = \sum_{n=1}^{\infty} A_\alpha(n) \cdot q^n$. By definitions of Hecke operators, $T_{\lambda+k_\alpha(p^\alpha-p^{\alpha-1})}(l)$ and $T_{\lambda+k_\alpha(p^\alpha-p^{\alpha-1})}(p)$ act on $\mathfrak{S}_{\lambda+k_\alpha(p^\alpha-p^{\alpha-1}),\,\mathfrak{o}_T}$. Since $l^{\lambda+k_\alpha(p^\alpha-p^{\alpha-1})} \equiv l^\lambda \pmod{p^\alpha}$ for any prime l other than p, we have

$$\begin{aligned} F_\alpha(\tau)\,|\,T_{\lambda+k_\alpha(p^\alpha-p^{\alpha-1})}(l) &= \sum_{n=1}^{\infty} \left\{ A_\alpha(nl) + l^{\lambda+k_\alpha(p^\alpha-p^{\alpha-1})-1} A_\alpha\left(\frac{n}{l}\right) \right\} \cdot q^n \\ &\equiv \sum_{n=1}^{\infty} \left\{ A_\alpha(nl) + l^{\lambda-1} \cdot A_\alpha\left(\frac{n}{l}\right) \right\} \cdot q^n \quad (\operatorname{mod} \tilde{\mathfrak{P}}^\alpha) . \end{aligned}$$

Putting $\tilde{F}_l = \sum_{n=1}^{\infty} \left\{ A(nl) + l^{\lambda-1} \cdot A\left(\frac{n}{l}\right) \right\} \cdot q^n$, we have

$$\tilde{F}_l \equiv F_\alpha(\tau)\,|\,T_{\lambda+k_\alpha(p^\alpha-p^{\alpha-1})}(l) \qquad (\operatorname{mod} \tilde{\mathfrak{P}}^\alpha) .$$

Therefore $\tilde{F}_l$ belongs to $\mathscr{S}^{(\lambda)}$. Put $\tilde{F}_p = \sum_{n=1}^{\infty} A(np) q^n$. As for $\tilde{F}_p$, we can take sufficiently large k_α satisfying $\lambda + k_\alpha(p^\alpha - p^{\alpha-1}) - 1 - \alpha \geqq 0$. Then we have

$$\begin{aligned} F_\alpha(\tau)\,|\,T_{\lambda+k_\alpha(p^\alpha-p^{\alpha-1})}(p) &= \sum_{n=1}^{\infty} \left\{ A_\alpha(np) + p^{\lambda+k_\alpha(p^\alpha-p^{\alpha-1})-1} A_\alpha\left(\frac{n}{p}\right) \right\} \cdot q^n \\ &\equiv \sum_{n=1}^{\infty} A_\alpha(np) \cdot q^n \qquad (\operatorname{mod} \tilde{\mathfrak{P}}^\alpha) , \end{aligned}$$

so $\tilde{F}_p$ belongs to $\mathscr{S}^{(\lambda)}$. q.e.d.

By this, we can define the p-adic Hecke operators as follows.

Definition. Let l be any prime other than p. We define the p-adic Hecke operators $\tilde{U}_\lambda(p)$ and $\tilde{T}_\lambda(l)$ on $\mathscr{S}^{(\lambda)}$ by

$$\tilde{F}|\tilde{U}_\lambda(p)=\sum_{n=1}^{\infty} A(np)\cdot q^n ,$$

$$\tilde{F}|\tilde{T}_\lambda(l)=\sum_{n=1}^{\infty}\left\{A(nl)+l^{\lambda-1}A\left(\frac{n}{l}\right)\right\}\cdot q^n ,$$

for $\tilde{F}=\sum_{n=1}^{\infty} A(n)\cdot q^n\in\mathscr{S}^{(\lambda)}$. Here $A\left(\frac{n}{l}\right)$ is defined to be zero if n is not divisible by l. It is clear that $\tilde{U}_\lambda(p)$, $\tilde{T}_\lambda(l)$ are mutually commutative.

8. The conjecture of Atkin

8-1. In this section we discuss the case $p=13$ using the results of Atkin and O'Brien [3]. Put $f(\tau)=\prod_{n=1}^{\infty}(1-q^n)$, and $g(\tau)=q\{f(13\tau)/f(\tau)\}^2$. Then it is well-known that the modular function field with respect to $\Gamma_0(13)$ is generated by $g(\tau)$ over $\boldsymbol{C}$.

Proposition 11. *$\{g(\tau)^k\}_{k=1}^{\infty}$ forms an orthonormal basis of $\mathscr{S}^{(0)}$ as a p-adic Banach space over $\boldsymbol{Q}_p^{\infty}$.*

Proof. Put $J^0(\tau)=J(\tau)-744$. By Lemma 5 in [3], it holds that

$$J^0(\tau)|U(13)=-g(\tau)+13^2 g(\tau)|U(13)^2 . \tag{46}$$

From the above equality, it is easily seen that $g(\tau)$ is p-adically approximated by the sequence $\{-\sum_{i=0}^{n} 13^{2i}J^0(\tau)|U(13)^{2i+1}\}_{n=1}^{\infty}$. On the other hand, it follows from Theorem 1 and Proposition 9 that $J^0(\tau)|U(13)^n$, for $n\geqq 1$, belong to $\mathscr{S}^{(0)}$. Moreover, using the fact that there exists only one supersingular invariant in characteristic $p=13$ and that it is 5, we have by Theorem 1,

$$J^0(\tau)|U(13)\equiv-(J(\tau)-j_5)^{-1}\qquad(\bmod\tilde{\mathfrak{P}}) ,$$

with $j_5\in\mathfrak{o}_p^{\infty}$ such that $j_5^4=1$, $j_5\ (\bmod\mathfrak{p})=5$. Therefore $g(\tau)$ belongs to $\mathscr{S}^{(0)}$ and it holds that,

$$g(\tau)^k\equiv(J(\tau)-j_5)^{-k}\qquad(\bmod\tilde{\mathfrak{P}}) . \tag{47}$$

With this and the fact that $\{(J(\tau)-j_5)^{-k}\}_{k=1}^{\infty}$ forms an orthonormal basis, the proposition is completely proved. q.e.d.

Denote by $\bar{\mathfrak{S}}_{k(p-1)}$ the residue class module of $\mathfrak{S}_{k(p-1),\mathfrak{o}_T}$ modulo $\tilde{\mathfrak{P}}$. Then $\bar{\mathfrak{S}}_{k(p-1)}$ is the vector space over $\bar{F}_p$. Denote by $\bar{T}_{k(p-1)}(p)$ the induced operator on $\bar{\bar{\mathfrak{S}}}_{k(p-1)}$ from $T_{k(p-1)}(p)$ on $\mathfrak{S}_{k(p-1),c_T}$. By definition, for any $F\in\mathfrak{S}_{k(p-1),c_T}$, we have

$$F|T_{k(p-1)}(p)(\bmod\,\tilde{\mathfrak{P}})=F(\bmod\,\tilde{\mathfrak{P}})|\bar{T}_{k(p-1)}(p)\ . \tag{48}$$

By Proposition 4, it can be considered that $\bar{\bar{\mathfrak{S}}}_{k(p-1)}$ is contained in $\bar{\bar{\mathfrak{S}}}_{k'(p-1)}$ with $k'>k$, and that $\bar{T}_{k'(p-1)}(p)$ induces $\bar{T}_{k(p-1)}(p)$ on $\bar{\bar{\mathfrak{S}}}_{k(p-1)}$. For each integral element f of $\mathscr{F}^{(0)}$, there exists some k such that $f(\bmod\,\tilde{\mathfrak{P}})\in\bar{\bar{\mathfrak{S}}}_{k(p-1)}$, and then we have

$$f|\tilde{U}_0(p)(\bmod\,\tilde{\mathfrak{P}})=f(\bmod\,\tilde{\mathfrak{P}})|\bar{T}_{k(p-1)}(p)\ . \tag{49}$$

In the case $p=13$, Atkin and O'Brien determined the action of $U(13)$ on each element of $\{g(\tau)^k\}_{k=1}^{\infty}$ in [3]. By definition, it is clear that $g(\tau)^k|\tilde{U}_0(13)=g(\tau)^k|U(13)$, so that their result gives a certain explicit representation of $\tilde{U}_0(13)$ with respect to the orthonormal basis $\{g(\tau)^k\}_{k=1}^{\infty}$ of $\mathscr{F}^{(0)}$. This fact is crucial to the proof of Atkin's conjecture.

PROPOSITION 12. *There exists only one non-zero eigenvalue of* $\bar{T}_{12k}(13)$ *and its eigenspace is of dimension one.*

PROOF. It is well known $\Delta(\tau)|T_{12}(13)=\tau(13)\cdot\Delta(\tau)$, and the fact $\tau(13)=-577738$ $\not\equiv 0 \pmod{13}$ is easily checked. From Proposition 4, it follows that $\bar{\bar{\mathfrak{S}}}_{12k}$ is the vector space with a basis $\{(\overline{J(\tau)-j^5})^{-1}\}_{i=1}^{k}$ over $\bar{F}_p$. Put $\bar{g}=g(\tau)\ (\bmod\,\tilde{\mathfrak{P}})$. Since $\bar{g}=(\overline{J(\tau)-j^5})^{-1}$, we have $\bar{\bar{\mathfrak{S}}}_{12k}=\sum_{i=1}^{k}\bar{F}_p\cdot\bar{g}^i$. By Lemma 4 in [3], we have for $k\geqq 1$,

$$g(\tau)^k|U_0(13)=\sum_{r=1}^{\infty}c_{k.r}g(\tau)^r\ , \tag{50}$$

where $c_{k.r}$ are integers satisfying $\operatorname{ord}_p c_{k.r}\geqq[13r-k-1/14]$. Hence the representation matrix of $\bar{T}_{12k}(13)$ with respect to $\{\bar{g}^i\}_{i=1}^{k}$ is given by $[c_{i.j}(\bmod\,13)]_{1\leqq i,j\leqq k}$. For any positive integer k, let denote by r_k the maximal integer such that $[13r_k-k-1/14]<1$. Then it is easily proved that r_k is smaller than k except $k=1$. Therefore $[c_{i.j}(\bmod\,13)]_{1\leqq i,j\leqq k}$ is a lower triangular matrix whose diagonal elements are all zero but one. q.e.d.

Denote by $\mathscr{T}$ the submodule of $\mathscr{F}^{(0)}$ consisting of all elements $\sum_{r=1}^{\infty}a_rg(\tau)^r$ with $a_r\in\mathfrak{o}_p^{\infty}$ satisfying $\operatorname{ord}_p a_r\geqq[13r-2/14]$. Lemma 6 in [3] says that $J^0(\tau)|U(13)^{\alpha}$ all belong to $\mathscr{T}$ for $\alpha\geqq 1$. We extend this lemma as follows;

PROPOSITION 13. *For each* $f\in M^{\infty}$, *there exist a unique* $h\in\mathfrak{o}_p^{\infty}[J(\tau)]$ *and* $\tilde{F}\in\mathscr{T}$ *such that* $f=h+\tilde{F}$.

PROOF. By Theorem 1, we have the following unique decomposition of f; $f=h+\tilde{F}$ with $h\in\mathfrak{o}_p^{\infty}[J(\tau)]$, and $\tilde{F}\in\mathscr{F}^{(0)}$. We shall show that $\tilde{F}$ belongs to $\mathscr{T}$. By the same argument of the proof of Lemma 6 in [11], it is easily proved that $U(13)$

operates on $\mathscr{T}$. Hence it is sufficient to prove that the proposition is valid for $J(\tau)^m | U(13)$ with $m \geqq 1$. We use induction on m; for $m=1$, Lemma 6 is our proposition itself. We assume that our proposition is valid for $J(\tau)^i | U(13)$ with $1 \leqq i < m$. It is easily seen that

$$(51) \qquad 13^m \left\{ g\left(-\frac{1}{13\tau}\right)^m + 13 g(\tau)^m | \tilde{U}_0(13) \right\} = g(\tau)^{-m} + 13^{m+1} g(\tau)^m | \tilde{U}_0(13)$$

is an entire modular function with respect to Γ, so that we have

$$(52) \qquad g(\tau)^{-m} + 13^{m+1} g(\tau)^m | \tilde{U}_0(13) = J(\tau)^m + \sum_{i=0}^{m-1} b_i J(\tau)^i ,$$

with $b_i \in Z$. Here we use the fact that $13 g\left(-\dfrac{1}{13\tau}\right) = g(\tau)^{-1}$. Also we have

$$(53) \qquad g\left(-\frac{1}{13\tau}\right)^{-m} + 13 g(\tau)^{-m} | \tilde{U}_0(13) = 13^m g(\tau)^m + 13 \cdot g(\tau)^{-m} | \tilde{U}_0(13) ,$$

$$= 13 \sum_{i=1}^{\left[\frac{m}{13}\right]} c_i J(\tau)^i ,$$

with $c_i \in Z$. From (52), (53), it follows that,

$$(54) \qquad \{J(\tau)^m + \sum_{i=1}^{m-1} b_i J(\tau)^i\} | U(13) = \sum_{i=1}^{\left[\frac{m}{13}\right]} c_i J(\tau)^i$$
$$- 13^{m-1} \{ g(\tau)^m - 13^2 g(\tau)^m | \tilde{U}_0(13)^2 \} .$$

Using Lemma 4 in [3], it is easily seen that $13^{m+1} g(\tau)^m | \tilde{U}_0(13)^2$ belongs to $\mathscr{T}$. Therefore the proposition is proved to be valid for $J(\tau)^m | U(13)$. q.e.d.

Now we discuss the eigenfunctions of $\tilde{U}_0(13)$.

Proposition 14. *The eigenfunction of $\tilde{U}_0(13)$ in $\mathscr{S}^{(0)}$ whose eigenvalue is not zero modulo $\mathfrak{p}$ exists and is unique up to $\boldsymbol{Q}_p^{\infty\times}$-multiples.*

Proof. We may assume that an eigenfunction F is integral and is not zero modulo $\tilde{\mathfrak{P}}$. We shall show this F exists and is unique up to $\mathfrak{o}_p^{\infty\times}$-multiples. For the purpose, it is enough to find a sequence $\{F_\alpha\}_{\alpha=1}^\infty$ of integral elements in $\mathscr{S}^{(0)}$ such that $F_{\alpha+1} \equiv F_\alpha \pmod{\tilde{\mathfrak{P}}^\alpha}$, and that $F_\alpha | \tilde{U}_0(13) \equiv k_\alpha F_\alpha \pmod{\tilde{\mathfrak{P}}^\alpha}$ with $k_\alpha \in \mathfrak{o}_p^{\infty\times}$, and to show these F_α are unique up to $\mathfrak{o}_p^{\infty\times} \cdot \{1+\tilde{\mathfrak{P}}^\alpha\}$-multiples. By Proposition 12, this is valid for $\alpha=1$. Suppose that $\{F_i\}_{i=1}^\alpha$, $\{k_i\}_{i=1}^\alpha$ are already found and that their uniqueness is already proved. Let us denote by n_α the maximal integer such that $[13n_\alpha - n_\alpha - 1/14] \leqq \alpha - 1$. Then we may put $F_\alpha = g + \sum_{i=2}^{n_\alpha} c_i g^i$ with $c_i \in \mathfrak{o}_p^\infty$, where we denote simply g^i for $g^i(\tau)$. Since $F_\alpha \equiv g \pmod{\tilde{\mathfrak{P}}}$, we have $c_i \equiv 0 \pmod{\mathfrak{p}}$ for $2 \leqq i \leqq n_\alpha$. We may also put

$$F_\alpha | \tilde{U}_0(13) \equiv k_\alpha F_\alpha + p^\alpha \sum_{i=1}^{n_{\alpha+1}} b_i g^i \pmod{\tilde{\mathfrak{P}}^{\alpha+1}},$$

with $b_i \in \mathfrak{o}_p^\infty$. Put $F_{\alpha+1} = F_\alpha + p^\alpha \sum_{i=2}^{n_{\alpha+1}} d_i g^i$, and $k_{\alpha+1} = k_\alpha + p^\alpha t$, with d_i, $t \in \mathfrak{o}_p^\infty$. Then, in order that $F_{\alpha+1} | \tilde{U}_0(13) \equiv k_{\alpha+1} F_{\alpha+1} \pmod{\tilde{\mathfrak{P}}^{\alpha+1}}$, it is necessary and sufficient that

$$\begin{aligned}(55)\qquad &[b_1, \cdots, b_{n_{\alpha+1}}] + [0, d_2, \cdots, d_{n_{\alpha+1}}][c_{ij}]_{1\leqq i,j\leqq n_{\alpha+1}} \\ &\equiv t[1, 0, \cdots, 0] + k_\alpha [0, d_2, \cdots, d_{n_{\alpha+1}}] \pmod{\mathfrak{p}}.\end{aligned}$$

Hence we have

$$(56)\qquad [0, d_2, \cdots, d_{n_{\alpha+1}}][c_{ij} - k_\alpha \delta_{ij}]_{1\leqq i,j\leqq n_{\alpha+1}} \equiv [t + b_1, b_2, \cdots, b_{n_{\alpha+1}}] \pmod{\mathfrak{p}},$$

where $\delta_{ii} = 1$, and $\delta_{ij} = 0$ if $i \neq j$. Since $k_\alpha \not\equiv 0 \pmod{\mathfrak{p}}$, the rank of the matrix $[\bar{c}_{ij} - \bar{k}_\alpha \delta_{ij}]_{1\leqq i,j\leqq n_{\alpha+1}}$ is $n_{\alpha+1} - 1$ by Proposition 12. Hence in order that the congruence equation (56) has solutions $[0, d_2, \cdots, d_{n_{\alpha+1}}]$ and t, it is necessary and sufficient that the rank of the matrix $\begin{bmatrix} [\bar{c}_{ij} - \bar{k}_\alpha \delta_{ij}]_{1\leqq i,j\leqq n_{\alpha+1}} \\ \bar{t} + \bar{b}_1, \bar{b}_2, \cdots, \bar{b}_{n_{\alpha+1}} \end{bmatrix}$ is $n_{\alpha+1} - 1$. By Proposition 12, the solution t is uniquely determined up to modulo $\mathfrak{p}$ and the d_i, $2 \leqq i \leqq n_{\alpha+1}$, also are uniquely determined up to modulo $\mathfrak{p}$. q.e.d.

Moreover, Atkin and O'Brien proved the following fact in [3] (Theorem 1). Put $J_1(\tau) = J^0(\tau) = J_1(\tau) | U(13)$ and $J_\alpha(\tau) = J_1(\tau) | \tilde{U}_0(13)^{\alpha-1}$. Then there exists $k_\alpha \in \boldsymbol{Z}$ not divisible by 13 such that $J_{\alpha+1}(\tau) \equiv k_\alpha J_\alpha(\tau) \pmod{\tilde{\mathfrak{P}}^\alpha}$. By the same argument of this proof and with Proposition 13, we obtain the following;

PROPOSITION 15. *For each* $f \in M^\infty$ *such that* $f = \sum_{n=1}^\infty a(n) \cdot q^n$ *with* $a(1) \not\equiv 0 \pmod{\mathfrak{p}}$, *put* $f_\alpha = f | \tilde{U}_0(13)^{\alpha-1}$ *for* $\alpha \geqq 1$. *Then there exists a constant* $k_\alpha \in \mathfrak{o}_p^\infty$ *with* $k_\alpha \not\equiv 0 \pmod{\mathfrak{p}}$ *such that,*

$$f_{\alpha+1} \equiv k_\alpha f_\alpha \pmod{\tilde{\mathfrak{P}}^\alpha}.$$

The proof is exactly the same as that in [3], so we omit this.

Now we prove the conjecture of Atkin in the case $p = 13$. The author does not know the proof of Atkin, but perhaps the following proof is the same as that of Atkin.

PROPOSITION 16. *Let* l *be a prime other than* 13. *For each* $f \in M^\infty$ *such that* $f = \sum_{n=1}^\infty a(n) \cdot q^n$ *with* $a(1) \not\equiv 0 \pmod{\mathfrak{p}}$, *put* $t_\alpha(n) = a(13^{\alpha-1} \cdot n)/a(13^{\alpha-1})$. *Then we have, for any* $n \geqq 1$,

$$(57)\qquad t_\alpha(nl) - t_\alpha(n) t_\alpha(l) + l^{-1} t_\alpha\left(\frac{n}{l}\right) \equiv 0 \pmod{\mathfrak{p}^\alpha}.$$

PROOF. By Proposition 15, we have $f_\alpha = \sum_{n=1}^\infty a(13^{\alpha-1} n) \cdot q^n \equiv k_{\alpha-1} \cdots k_1 f \pmod{\tilde{\mathfrak{P}}}$.

Since $k_i \not\equiv 0 \pmod{\mathfrak{p}}$, we have $a(13^{\alpha-1}) \not\equiv 0 \pmod{\mathfrak{p}}$. Hence $t_\alpha(n)$ are well defined and belongs to $\mathfrak{o}_p^\infty$, and we have $f_\alpha = a(13^{\alpha-1}) \sum_{n=1}^{\infty} t_\alpha(n) \cdot q^n$. The congruence relations (57) are equivalent to the following congruence,

$$f_\alpha | \tilde{T}_0(l) \equiv t_\alpha(l) \cdot f_\alpha \qquad (\mathrm{mod}\ \tilde{\mathfrak{P}}^\alpha) . \tag{58}$$

Put $f'_\alpha = \sum_{n=1}^{\infty} t_\alpha(n) \cdot q^n$. Then we have $f'_{\alpha+1} \equiv f'_\alpha \ (\mathrm{mod}\ \tilde{\mathfrak{P}}^\alpha)$ by Proposition 15, so that $\{f'_\alpha\}_{\alpha=1}^{\infty}$ has a $\tilde{\mathfrak{P}}$-adic limit $\tilde{f}'$ in $\mathscr{S}^{(0)}$. It is clear that $\tilde{f}' | \tilde{U}_0(13) = \tilde{k} \cdot \tilde{f}'$ with $\tilde{k} \in \mathfrak{o}_p^{\infty\times}$. Since $\tilde{U}_0(13)$, $\tilde{T}_0(l)$ are mutually commutative, we have

$$\begin{aligned}(f' | \tilde{T}_0(l)) | \tilde{U}_0(13) &= (f' | \tilde{U}_0(13)) | \tilde{T}_0(l) ,\\ &= \tilde{k} \cdot \tilde{f}' | \tilde{T}_0(l) .\end{aligned}$$

By Proposition 14, we have $\tilde{f}' | \tilde{T}_0(l) = \tilde{t}(l) \tilde{f}'$ with $\tilde{t}(l) \in \mathfrak{o}_p^\infty$. Since $\tilde{f}' \equiv f'_\alpha \ (\mathrm{mod}\ \tilde{\mathfrak{P}}^\alpha)$, we have $\tilde{t}(l) \equiv t_\alpha(l) \ (\mathrm{mod}\ \mathfrak{p}^\alpha)$, so that we obtain (58). (q.e.d.)

Especially applying Propositions 15 and 16 to $f = J_1(\tau)$, we obtain the following;

Theorem 2. *The conjecture of Atkin is valid for all α in the case $p = 13$.*

8-2. Let $p \geqq 13$ be a prime number. We shall prove that, assuming the following assertions (H-1), (H-2), the conjecture of Atkin is proved to be valid. The process to the proof is similar to that in the case $p = 13$, namely, corresponding propositions to Propositions 12, 13, 14, 15, and 16, which are slightly modified, will be proved. However we do not know whether Proposition 11 has any correspondent in the general case or not.

(H-1) The eigenvalues of $\bar{T}_{p-1}(p)$ are not zero and are not equal to each other.

(H-2) For each positive rational integer n, we put $n_\theta = n$ for $\theta \in S^*$, $n_0 = 3n$, and $n_{12^3} = 2n$. Then we have

$$(J(\tau) - j_\theta)^{-i} | \tilde{U}_0(p) = \sum_{\theta' \in S} \sum_{r=1}^{\infty} c'_{ir.\theta\theta'} (J(\tau) - j_{\theta'})^{-r} ,$$

where $c'_{ir.\theta\theta'} \in \mathfrak{o}_p^\infty$ satisfying,

$$\mathrm{ord}_{\mathfrak{p}}\, c'_{ir.\theta\theta'} \geqq [p r_{\theta'} - i_\theta - 1/p + 1] . \tag{59}$$

From (H-1), it follows that there exist $G_\theta = \sum_{\theta' \in S^*} a_{\theta.\theta'} (J(\tau) - j_{\theta'})^{-1}$ with $\theta \in S^*$ and $a_{\theta.\theta'} \in \mathfrak{o}_p^\infty$ such that $G_\theta | \tilde{U}_0(p) \equiv k_\theta G_\theta \ (\mathrm{mod}\ \tilde{\mathfrak{P}})$ with $k_\theta \not\equiv 0 \ (\mathrm{mod}\ \mathfrak{p})$, and that det $[a_{\theta.\theta'}]_{\theta,\theta' \in S^*}$ is not zero mod $\mathfrak{p}$. Put $G_{1.\theta} = G_\theta$, and $G_{n.\theta} = (J(\tau) - j_\theta)^{-n}$ for $n \geqq 2$, $\theta \in S^*$ and for $n \geqq 1$, $\theta \in S - S^*$. Then $\{G_{i.\theta}\}_{\theta \in S, 1 \leqq i < \infty}$ also forms an orthonormal basis of $\mathscr{S}^{(0)}$. If we represent the operator $\tilde{U}_0(p)$ with respect to $\{G_{i.\theta}\}$, we have by (H-2),

$$G_{i,\theta}|\tilde{U}_0(p)=\sum_{\theta'\in S}\sum_{r=1}^{\infty}c_{ir,\theta\theta'}G_{r,\theta'}\ ,$$

where $c_{ir,\theta\theta'}\in\mathfrak{o}_p^{\infty}$ satisfying,

$$\text{ord}_p\, c_{ir,\theta\theta'}\geqq[pr_{\theta'}-i_\theta-1/p+1]\ . \tag{60}$$

Moreover we have $\text{ord}_p\, c_{11,\theta\theta}=0$ and $\text{ord}_p\, c_{11,\theta\theta'}\geqq 1$ for $\theta\neq\theta'$.

PROPOSITION 17. *Assume* $p\geqq 13$. *If we suppose* (H-1) *and* (H-2), *there exist only* $\left[\dfrac{p}{12}\right]$ *non-zero eigenvalues of* $\bar{T}_{k(p-1)}(p)$ *and each eigenspace is of dimension one.*

FROOF. We saw in 4-2 $\dim_{F_p}\bar{\mathfrak{S}}_{p-1}=\left[\dfrac{p}{12}\right]$. From the assumption (H-1), the eigenvalues of $\bar{T}_{p-1}(p)$ are not zero. By Proposition 4, we have $\bar{\mathfrak{S}}_{k(p-1)}=\sum_{\theta\in S}\sum_{1\leqq i\leqq k^{(\theta)}}\bar{F}_p\overline{(J(\tau)-j_\theta)}^{-i}$ with $k^{(\theta)}=k$ for $\theta\in S^*$, $k^{(0)}=\left[\dfrac{k}{3}\right]$, and $k^{(1728)}=\left[\dfrac{k}{2}\right]$. Since we have $(J(\tau)-j_\theta)^{-i}|\tilde{U}_0(p)\ (\text{mod}\,\tilde{\mathfrak{P}})=\overline{(J(\tau)-j_\theta)}^{-i}|\bar{T}_{k(p-1)}(p)$, the representation matrix of $\bar{T}_{k(p-1)}(p)$ with respect to the basis $\{\overline{(J(\tau)-j_\theta)}^{-i}\}_{\theta\in S,1\leqq i\leqq k^{(\theta)}}$ is given by $[c_{ir,\theta\theta'}(\text{mod}\,\mathfrak{o})]_{\theta,\theta'\in S,1\leqq i\leqq k^{(\theta)},1\leqq r\leqq k^{(\theta')}}$. Using (59), it is easily proved that $\bar{\mathfrak{S}}_{k(p-1)}|\bar{T}_{k(p-1)}(p)\subset\bar{\mathfrak{S}}_{(k-1)(p-1)}$. Hence the eigenvalues of $\bar{T}_{k(p-1)}(p)$ which do not come from those of $\bar{T}_{(k-1)(p-1)}(p)$ are all zero. q.e.d.

Denote by $\mathscr{T}$ the submodule of $\mathscr{S}^{(0)}$ consisting of all elements $\sum_{r,\theta}a_{r,\theta}(J(\tau)-j_\theta)^{-r}$ with $a_{r,\theta}\in\mathfrak{o}_p^{\infty}$ satisfying $\text{ord}_p\, a_{r,\theta}\geqq[pr_\theta-2/p+1]$. Then we have the following;

PROPOSITION 18. *Assume* $p\geqq 5$. *For each* $f\in M^{\infty}$, *there exist* $h\in\mathfrak{o}_p^{\infty}[J(\tau)]$ *and* $\tilde{F}\in\mathscr{T}$ *uniquely such that* $f=h+\tilde{F}$.

REMARK. Here, we obtain another proof of Proposition 13. The method of that proof is not applicable to the general case, because we do not have enough facts on modular functions with respect to $\Gamma_0(p)$.

PROOF. This follows essentially from Theorem 1. We proved there in (42) that we have

$$p^{-l}(J(\tau)^{mpl}-J(p\tau)^{mpl-1})=h_2+\sum_{\theta\in S}\sum_{n=1}^{\infty}C_n^{(\theta)}(J(\tau)-j_\theta)^{-n}\ ,$$

with some $h_2\in\mathfrak{o}_p^{\infty}[J(\tau)]$ and $C_n^{(\theta)}\in\mathfrak{o}_p^{\infty}$ satisfying,

$$\text{ord}_p\, C_n^{(\theta)}\geqq(np_\theta-1-p-1)/p+1\ .$$

Since $\text{ord}_p\, C_n^{(\theta)}$ is a rational integer, we have $\text{ord}_p\, C_n^{(\theta)}\geqq[pn_\theta-2-p+p/p+1]=[pn_\theta-2/p+1]$. q.e.d.

PROPOSITION 19. *Let* ρ_i, $1\leqq i\leqq\left[\dfrac{p}{12}\right]$, *be the eigenvalues of* $\bar{T}_{p-1}(p)$. *If we assume* (H-1) *and* (H-2), *for each* ρ_i *there exists an eigenfunction* $\tilde{F}$ *of* $\tilde{U}_0(p)$

in $\mathscr{S}^{(0)}$, *such that* $\tilde{F}|\tilde{U}_0(p)=\tilde{k}\tilde{F}$ *with* $\tilde{k}\in\mathfrak{o}_p^{\infty}$ *satisfying* $\tilde{k}(\mathrm{mod}\,\mathfrak{p})=\rho_i$. *For each* ρ_i, *this* $\tilde{F}$ *is unique up to* $\boldsymbol{Q}_p^{\infty}$*-multiples. Moreover any eigenfunction of* $\tilde{U}_0(p)$ *in* $\mathscr{S}^{(0)}$ *whose eigenvalue is not congruent to zero* mod $\mathfrak{p}$, *coincides with one of the above eigenfunctions.*

The proof, being entirely similar to that of Proposition 14, is omitted.

Put $N^{\infty}=M^{\infty}\cap q\cdot\mathfrak{o}_T[[q]]$. N^{∞} and $\mathfrak{S}_{p-1,\mathfrak{o}_T}$ have not any intersection in $q\cdot\mathfrak{o}_T[[q]]$, but, if we consider the reduction modulo $\tilde{\mathfrak{P}}$, the residue class module of N^{∞} mod $\tilde{\mathfrak{P}}$ can be considered to be contained in that of $\mathfrak{S}_{p-1,\mathfrak{o}_T}$ mod $\tilde{\mathfrak{P}}$. Moreover we have the following;

PROPOSITION 20. *Let* $p\geqq 13$, *and let* M^{∞} *be the same as is defined in* § 6-1. *Put* $N^{\infty}=M^{\infty}\cap q\cdot\mathfrak{o}_T[[q]]$. *Then the residue class module of* N^{∞} mod $\tilde{\mathfrak{P}}$ *coincides with that of* $\mathfrak{S}_{p-1,\mathfrak{o}_T}$ mod $\tilde{\mathfrak{P}}$.

PROOF. From Proposition 4, it follows that the residue class module of $\mathfrak{S}_{p-1,\mathfrak{o}_T}$ mod $\tilde{\mathfrak{P}}$ is the vectors pace over $\bar{F}_p$ with the basis $\{(\overline{J(\tau)-j_\theta})^{-1}\}_{\theta\in S^*}$. Hence, it is enough to show that for any $\theta\in S^*$ there exists some $f\in N^{\infty}$ such that $f(\mathrm{mod}\,\tilde{\mathfrak{P}})=(\overline{J(\tau)-j_\theta})^{-1}$. Let m be a rational integer with $1\leqq m\leqq\left[\frac{p}{12}\right]$. Then, by Theorem 1, we have

$$J(\tau)^m|U(p)\equiv b_m+\sum_{\theta\in S^*}a_{m.\theta}(J(\tau)-j_\theta)^{-1}\qquad(\mathrm{mod}\,\tilde{\mathfrak{P}})\,,$$

with b_m, $a_{m.\theta}\in\mathfrak{o}_p^{\infty}$ for $1\leqq m\leqq\left[\frac{p}{12}\right]$, $\theta\in S^*$, where b_m is the constant term of the Fourier expansions of $J(\tau)^m$. On the other hand, we have

$$\begin{aligned}J(\tau)^m|U(p)&=J(\tau)^m|T_0(p)-p^{-1}J(p\tau)^m\,,\\&\equiv p^{-1}\{J(\tau)^{mp}-J(p\tau)^m\}\qquad(\mathrm{mod}\,\boldsymbol{Z}[J(\tau)]\,,\\&\equiv p^{-1}\{J(\tau)^p-J(p\tau)\}\cdot\{\sum_{i=0}^{m-1}J(\tau)^{ip}J(p\tau)^{m-i-1}\}\qquad(\mathrm{mod}\,\boldsymbol{Z}[J(\tau)])\,.\end{aligned}$$

Since $J(p\tau)\equiv J(\tau)^p$ (mod $\tilde{\mathfrak{P}}$), we have

$$a_{m.\theta}\equiv ma_{1.\theta}j_\theta^{(m-1)p}\qquad(\mathrm{mod}\,\mathfrak{p})\,.$$

Moreover, from Proposition 1, it follows that $a_{1.\theta}$ is not congruent to zero mod $\mathfrak{p}$. Hence the determinant of the matrix $\{a_{m.\theta}\}_{\substack{1\leqq m\leqq\left[\frac{p}{12}\right]\\ \theta\in S^*}}$ is not congruent to zero mod $\mathfrak{p}$, so that we have

$$(J(\tau)-j_\theta)^{-1}\equiv\sum_{m=1}^{\left[\frac{p}{12}\right]}c_m(J(\tau)^m-b_m)|U(p)\qquad(\mathrm{mod}\,\tilde{\mathfrak{P}})\,,$$

with some $c_m \in \mathfrak{o}_p^\infty$. q.e.d.

Let $p \geqq 13$ be a prime. Assuming (H-1) and (H-2), we showed in Proposition 19 that, for each $\theta \in S^*$, there exists $\tilde{F} \in \mathscr{F}^{(0)}$ satisfying $\tilde{F} \equiv G_\theta \pmod{\tilde{\mathfrak{P}}}$ and $\tilde{F} | \tilde{U}_0(p) = \tilde{k}_\theta \tilde{F}$ with $\tilde{k}_\theta \in \mathfrak{o}_p^\infty$, and that this $\tilde{F}$ is unique up to $\{1 + p\mathfrak{o}_p^\infty\}$-multiples. Fix one of these $\tilde{F}$ and denote it by $\tilde{F}_\theta$.

PROPOSITION 21. *Assume* (H-1) *and* (H-2). *Take any element* $H \in N^\infty$ *satisfying* $H \equiv G_\theta \pmod{\tilde{\mathfrak{P}}}$ *with some* $\theta \in S^*$. *Then* $H | \tilde{U}_0(p)^{a-1}$ *is congruent modulo* $\tilde{\mathfrak{P}}^a$ *to a linear sum of* $\tilde{F}_\theta$, $\theta \in S^*$, *with coefficients in* $\mathfrak{o}_p^\infty$.

PROOF. By Proposition 20, for any $\theta \in S^*$, there exists a $H_\theta \in N^\infty$ such that $H_\theta \equiv G_\theta \pmod{\tilde{\mathfrak{P}}}$. We may put $H_\theta = \sum_{\theta' \in S, 1 \leqq i < \infty} a^{(\theta)}_{i.\theta'} G_{i.\theta'}$, with $a^{(\theta)}_{i.\theta'} \in \mathfrak{o}_p^\infty$. Since $H_\theta \equiv G_\theta$ $(\mathrm{mod}\, \mathfrak{P})$, we have $\mathrm{ord}_\mathfrak{p}\, a^{(\theta)}_{1.\theta'} \geqq 1$ for $\theta' \neq \theta \in S^*$. Moreover, by Proposition 18, H_θ belongs to $\mathscr{T}$, so that we have $\mathrm{ord}_\mathfrak{p}\, a^{(\theta)}_{i.\theta'} \geqq [pi_{\theta'} - 2/p+1]$. Now fix one of the elements in S^* and denote it by θ_0. Take any $H \in N^\infty$ satisfying $H \equiv G_{\theta_0} \pmod{\tilde{\mathfrak{P}}}$. Put $F_1 = H = \sum_{i,\theta} a^1_{i.\theta} G_{i.\theta}$ with $a_{i,\theta} \in \mathfrak{o}_p^\infty$, $F'_2 = F_1 | \tilde{U}_0(p) = \sum_{i,\theta} a'^2_{i.\theta} G_{i.\theta}$ and $F_2 = F'_2 + p \sum_{\theta^1 \in S^*, \theta^1 \neq \theta_0} b^1_{\theta^1} H_{\theta^1} = \sum a^2_{i.\theta} G_{i.\theta}$ with $a'^2_{i.\theta}$, $b^1_{\theta^1}$, $a^2_{i.\theta} \in \mathfrak{o}_p^\infty$. Define $\gamma'^1_{ij.\theta\theta'} = a'^2_{i.\theta} a^1_{j.\theta'} - a^1_{i.\theta} a'^2_{j.\theta'}$ for $1 \leqq i$, $j < \infty$ and θ, $\theta' \in S$ and also $\gamma^1_{ij.\theta\theta'} = a^2_{i.\theta} a^1_{j.\theta'} - a^1_{i.\theta} a^2_{j.\theta'}$. Then we have

$$(61) \qquad \begin{cases} \mathrm{ord}_\mathfrak{p}\, \gamma'^1_{11.\theta\theta'} \geqq 1 & \text{for } \theta,\ \theta' \in S^*\,, \\ \mathrm{ord}_\mathfrak{p}\, \gamma'^1_{ij.\theta\theta'} \geqq 1 + [pi_\theta + pj_{\theta'} - 6 - 2p/p+1] & \text{for otherwise}\,. \end{cases}$$

This follows from the facts that $F_1 | \tilde{U}_0(p) \equiv \tilde{k}_{\theta_0} F_1 \pmod{\tilde{\mathfrak{P}}}$, and that F_1, F'_2 belongs to $\mathscr{T}$. Since $a^2_{i.\theta} = a'^2_{i.\theta} + p \sum_{\substack{\theta^1 \in S^* \\ \theta^1 \neq \theta_0}} b^1_{\theta^1} a^{(\theta^1)}_{i.\theta}$, we have

$$\gamma^1_{ij.\theta\theta'} = \gamma'^1_{ij\theta\theta'} + p \cdot a^1_{j.\theta'} \sum_{\theta^1} b^1_{\theta^1} a^{(\theta^1)}_{i.\theta} - p \cdot a^1_{i\theta} \sum_{\theta^1} b^1_{\theta^1} a^{(\theta^1)}_{j.\theta'}\,,$$

so that $\mathrm{ord}_\mathfrak{p}\, \gamma^1_{ij.\theta\theta'}$ satisfies the same inequality as (61). Put $F'_3 = F_2 | \tilde{U}_0(p) = \sum_{i,\theta} a'^3_{i.\theta} G_{i.\theta}$, and $\gamma'^2_{ij.\theta\theta'} = a'^3_{i\theta} a^2_{j.\theta'} - a^2_{i.\theta} a'^3_{j.\theta'}$. Then we shall show that there exist some $b^1_{\theta^1} \in \mathfrak{o}_p^\infty$ for $\theta^1 \in S^*$, $\theta^1 \neq \theta_0$, which is unique up to modulo $\mathfrak{p}$, such that $\mathrm{ord}_\mathfrak{p}\, \gamma'^2_{ij.\theta\theta'}$ satisfies the following inequality;

$$(62) \qquad \begin{cases} \mathrm{ord}_\mathfrak{p}\, \gamma'^2_{11.\theta\theta'} \geqq 2 & \text{for } \theta,\ \theta' \in S^*\,, \\ \mathrm{ord}_\mathfrak{p}\, \gamma'^2_{ij.\theta\theta'} \geqq 2 + [pi_\theta + pj_{\theta'} - 6 - 2p/p+1] & \text{for otherwise}\,. \end{cases}$$

Since we have $a'^3_{i.\theta} = \sum_{r.\theta_1} a^2_{r.\theta_1} c_{ri.\theta_1\theta}$, and $a^2_{j.\theta'} = \sum_{s,\theta_2} a^1_{s.\theta_2} c_{sj.\theta_2\theta'} + p \sum_{\substack{\theta^1 \in S^* \\ \theta^1 \neq \theta_0}} b^1_{\theta^1} a^{(\theta^1)}_{j.\theta'}$, so that we have

$$\gamma'^2_{ij.\theta\theta'} = \sum_{r,\theta_1} \sum_{s,\theta_2} \gamma'^1_{rs.\theta_1\theta_2} c_{ri.\theta_1\theta} c_{sj.\theta_2\theta'}$$

$$+\Big(\sum_{\theta^1\in S^*,\theta^1\neq\theta_0} p\cdot b^1_{\theta^1}a^{(\theta^1)}_{j\cdot\theta'}\Big)\Big(\sum_{r,\theta_1} a^2_{r\cdot\theta_1}c_{ri\cdot\theta_1\theta}\Big)$$
$$-\Big(\sum_{\theta^1\in S^*,\theta^1\neq\theta_0} p\cdot b^1_{\theta^1}a^{(\theta^1)}_{i\cdot\theta}\Big)\Big(\sum_{s,\theta_2} a^2_{s\cdot\theta_2}c_{sj\cdot\theta_2\theta'}\Big)\ .$$

If follows that, for $\theta\in S^*$, $\theta\neq\theta_0$, we have

$$\gamma'^2_{11\cdot\theta\theta_0}\equiv\gamma'^1_{11\cdot\theta\theta_0}\cdot c_{11\cdot\theta\theta}c_{11\cdot\theta_0\theta_0}-p\cdot b^1_{\theta^1}a^{(\theta)}_{1\cdot\theta}\cdot a^2_{1\cdot\theta_0}\cdot c_{11\cdot\theta_0\theta_0}\quad(\operatorname{mod}\mathfrak{p}^2)\ .$$

Hence, for $\theta\in S^*$, $\theta\neq\theta_0$, b^1_θ is uniquely determined up to mod $\mathfrak{p}$ such that $\operatorname{ord}_\mathfrak{p}\gamma'^2_{11\cdot\theta\theta_0}\geqq 2$. The second inequalities are obtained as follows; we have

$$\operatorname{ord}_\mathfrak{p}(\gamma'^1_{11\cdot\theta_1\theta_2}c_{1i\cdot\theta_1\theta}\cdot c_{1j\cdot\theta_2\theta'})\geqq 1+[pi_\theta-1-1/p+1]+[pj_{\theta'}-1-1/p+1]\ ,$$
$$\geqq 2+[pi_\theta+pj_{\theta'}-5-2p/p+1]\quad\text{for } \theta,\ \theta'\in S^*\ ,$$

and,

$$\operatorname{ord}_\mathfrak{p}(\gamma'^1_{rs\cdot\theta_1\theta_2}c_{ri\cdot\theta_1\theta}c_{sj\cdot\theta_2\theta'})\geqq 1+[pr_{\theta_1}+ps_{\theta_2}-6-2p/p+1]+[pi_\theta-r_{\theta_1}-1/p+1]$$
$$+[pj_{\theta'}-s_{\theta_2}-1/p+1]\ ,$$
$$\geqq 1+[pi_\theta+pj_{\theta'}-5-p/p+1]\quad\text{for otherwise}\ .$$

Also we have

$$\operatorname{ord}_\mathfrak{p}(pa^{(\theta^1)}_{j\cdot\theta'}a^2_{r\cdot\theta_1}c_{ri\cdot\theta_1\theta})\geqq 1+[pj_{\theta'}-2/p+1]+[pr_{\theta_1}-2/p+1]$$
$$+[pi_\theta-r_{\theta_1}-1/p+1]\ ,$$
$$\geqq 1+[pi_\theta+pj_{\theta'}-4-p/p+1]\ .$$

From (62), it follows that $F_2|\tilde{U}_0(p)\equiv\tilde{k}_{\theta_0}F_2$ (mod $\tilde{\mathfrak{P}}^2$), so that it holds $F_2\equiv a_1\tilde{F}_{\theta 0}$ (mod $\tilde{\mathfrak{P}}^2$) with $a_1\in\mathfrak{o}_p^\infty$ by Proposition 19. Therefore we have

$$F_1|\tilde{U}_0(p)\equiv a_1\cdot\tilde{F}_{\theta_0}-p\sum_{\substack{\theta^1\in S^*\\ \theta^1\neq\theta_0}} b^1_{\theta^1}\tilde{F}_{\theta^1}\qquad(\operatorname{mod}\tilde{\mathfrak{P}}^2)\ ,$$

so that our proposition is valid for $\alpha=2$.

For $\alpha=3$, by the same argument, it can be proved that there exist some $b^2_{\theta 1}\in\mathfrak{o}_p^\infty$ for $\theta^1\in S^*$, $\theta^1\neq\theta_0$, which is unique up to mod $\mathfrak{p}$ such that,

$$F_2|\tilde{U}_0(p)\equiv a_2\tilde{F}_{\theta_0}-p\sum_{\substack{\theta^1\in S^*\\ \theta^1\neq\theta_0}} b^1_{\theta 1}H_{\theta 1}|\tilde{U}_0(p)-p^2\sum_{\substack{\theta^1\in\theta^*\\ \theta^1\neq\theta_0}} b^2_{\theta 1}H_{\theta^1}\qquad(\operatorname{mod}\tilde{\mathfrak{P}}^3)\ ,$$

with $a_2\in\mathfrak{o}_p^\infty$. Since $H_{\theta^1}|\tilde{U}_0(p)$ is already proved to be congruent mod $\tilde{\mathfrak{P}}^2$ to a linear sum of $\tilde{F}_\theta$ with $\theta\in S^*$, our proposition is valid for $\alpha=3$. Proceeding the same argument, we obtain the complete proof of this proposition. q.e.d.

Corollary. *Put* $J^0(\tau)=J(\tau)-744$, *and* $J_1(\tau)=J^0(\tau)|U(p)$. *Then, for* $\alpha\geqq 1$, $J_1(\tau)|\tilde{U}_0(p)^{\alpha-1}$ *is congruent modulo* $\tilde{\mathfrak{P}}^\alpha$ *to a linear sum of* $\tilde{F}_\theta,\theta\in S^*$, *with coef-*

ficients in $\mathfrak{o}_p^\infty$.

PROOF. From Proposition 20, it follows that there exist some $H_\theta \in N^\infty$ with $\theta \in S^*$ satisfying $H_\theta \equiv G_\theta \pmod{\tilde{\mathfrak{P}}}$ such that,

$$J_1(\tau) = \sum_{\theta \in S^*} a_\theta H_\theta\ ,$$

with $a_\theta \in \mathfrak{o}_p^\infty$. Hence the corollary follows from the above proposition. q.e.d.

8-3. With these preliminaries, we discuss the conjecture of Atkin. First, we shall write down a slightly modified (stronger) version of the conjecture of Atkin, as follows. Let p be a prime number, and let α, n be any positive integers, and put $t_\alpha(n) = c(p^\alpha n)/c(p^\alpha)$. Then the conjecture asserts first that $c(p^\alpha) \neq 0$, and that $t_\alpha(n)$ are p-adic integers. Now put $d = \mathrm{Max}\left\{1, \left[\frac{p}{12}\right]\right\}$. Then it asserts secondly that for each $1 \leqq i \leqq d$ there exists a sequences $\{t^{(i)}(n)\}_{n=1}^\infty$ in $\mathfrak{o}_p^\infty$ and for each α an element $a_\alpha^{(i)}$ of $\mathfrak{o}_p^\infty$, satisfying the following congruences and the identities;

$$(1) \qquad t_\alpha(n) \equiv \sum_{i=1}^{d} a_\alpha^{(i)} t^{(i)}(n) \qquad \pmod{\mathfrak{p}^\alpha}\ ,$$

(2) let l be any prime number other than p. Then for all i, l, and n it holds that,

$$t^{(i)}(nl) = t^{(i)}(n) \cdot t^{(i)}(l) - l^{-1} t^{(i)}\left(\frac{n}{l}\right),$$

$$t^{(i)}(np) = t^{(i)}(n) \cdot t^{(i)}(p).$$

Here, $t^{(i)}\left(\frac{n}{l}\right)$ is defined to be zero if n is not divisible by l.

Now we assume,

(H-3) for $\alpha \geqq 1$, $c(p^\alpha)$ is a p-adic unit.

Then we have following;

THEOREM 3. *Let* $p \geqq 13$ *be a prime number. Assume* (H-1), (H-2) *and* (H-3). *Let* l *be any prime other than* p. *Put* $J_\alpha(\tau) = c(p^\alpha)^{-1} J_1(\tau) \mid \tilde{U}_0(p)^{\alpha-1} = \sum_{i=1}^{\infty} t_\alpha(n) \cdot q^n$. *Then, for each* $1 \leqq i \leqq d$, *there exists* $\tilde{F}_i$ *in* $\mathscr{T}^-$ *which is a simultaneous eigenfunction of* $\tilde{U}_0(p)$ *and* $\tilde{T}_0(l)$, *and some* $a_\alpha^{(i)} \in \mathfrak{o}_p^\infty$ *for* $\alpha \geqq 1$, *such that,*

$$J_\alpha(\tau) \equiv \sum_{i=1}^{d} a_\alpha^{(i)} \cdot \tilde{F}_i \qquad \pmod{\tilde{\mathfrak{P}}^\alpha}\ ,$$

holds.

PROOF. With (H-3), this follows immediately from Corollary of Proposition 21. q.e.d.

Therefore we have the following;

Corollary. *Let* $p \geqq 13$ *be a prime number, and assume* (H-1), (H-2), *and* (H-3). *Then the conjecture of Atkin is valid.*

§9. Numerical examples

9-1. By the aid of a computer, we can compute the eigenvalues of $\tilde{T}_{k(p-1)}(p)$ for some small p. The obtained results are as follows.

(1) the case $p=17$.

For $1 \leqq m \leqq 4$, we have $\tilde{\mathfrak{S}}_{16m} | \tilde{T}_{16m}(17) = \tilde{\mathfrak{S}}_{16}$.

(2) the case $p=19$.

For $1 \leqq m \leqq 2$, we have $\tilde{\mathfrak{S}}_{18m} | \tilde{T}_{18m}(19) = \tilde{\mathfrak{S}}_{18}$.

(3) the case $p=23$.

For $1 \leqq m \leqq 2$, we have $\tilde{\mathfrak{S}}_{22m} | \tilde{T}_{22m}(23) = \tilde{\mathfrak{S}}_{22}$.

(4) the case $p=29$, 31.

For $1 \leqq m \leqq 2$, we have $\tilde{\mathfrak{S}}_{m(p-1)} | \tilde{T}_{m(p-1)}(p) = \tilde{\mathfrak{S}}_{p-1}$, and the characteristic polynomial of $\tilde{T}_{p-1}(p)$ is irreducible over F_p.

(5) the case $p=37$, 41, 47.

The characteristic polynomial of $\tilde{T}_{(p-1)}(p)$ is not irreducible over F_p, but has only one root in F_p, which is not zero.

(6) the case $p=43$.

The characteristic polynomial of $\tilde{T}_{(p-1)}(p)$ is irreducible over F_p.

From these results, it follows.

Proposition 22. (H-1) *is valid for* $13 \leqq p \leqq 47$.

9-2. As for (H-2), we have a certain result for $p=5$, 7. Let $f(\tau)=\prod_{n=1}^{\infty}(1-q^n)$ and $g_5(\tau)=q\{f(5\tau)/f(\tau)\}^6$, $g_7(\tau)=q\{f(7\tau)/f(\tau)\}^4$. Then it is well-known that the modular function field with respect to $\Gamma_0(p)$ is generated by $g_p(\tau)$ over $\boldsymbol{C}$. Also, it is well-known that 0 and 12^3 respectively is the only supersingular invariant in characteristic $p=5$ and 7.

Proposition 23. (1) *We have* $g_p(\tau) \equiv (J(\tau)-j_\theta)^{-1}$ (mod $\tilde{\mathfrak{P}}$) *with* $\theta=0$ *for* $p=5$, $\theta=12^3$ *for* $p=7$.

(2) $\{g_p(\tau)^k\}_{k=1}^{\infty}$ *forms an orthonomal basis of* $\mathscr{F}^{(0)}$.

(3) *Put* $g_p(\tau)^k | \tilde{U}_0(p) = \sum_{r=1}^{\infty} c_{k,r} g_p(\tau)^r$. *Then* $c_{k,r}$ *are rational integers satisfying* $\mathrm{ord}_p\, c_{kr} \geqq [pr_\theta - k_\theta - 1/p + 1]$.

Proof. With the results of Lehner about the coefficients of the modular

The author wishes to acknowledge his gratitude to Mr. Machida for making the program to compute the eigenvalues of $\tilde{T}_{k(p-1)}(p)$.

equation ([10], 145, 147), the proof is easily obtained by the same method of that of Propositions 11, 12, and that of Lemma 4 in [3].

9-3. Concerning to the assertion (H-3), we have a following result.

PROPOSITION 24. (1) *The assertion* (H-3) *is valid for* $13 \leqq p \leqq 23$. (2) *For* $13 \leqq p \leqq 97$, *$c(p)$ is not divisible by p.*

PROOF. (1) Put $J_\alpha(\tau) = J_1(\tau) | \tilde{U}_0(p)^{\alpha-1}$, for $\alpha \geqq 1$, and denote by F the generator of the free module $\mathfrak{S}_{p-1, \mathfrak{o}_T}$ over $\mathfrak{o}_T$. Then, from Proposition 1 and Theorem 1, it follows that $J_1(\tau) \equiv c(p) \cdot (J(\tau) - j_\theta)^{-1} \pmod{\tilde{\mathfrak{P}}}$ $\theta \in S^*$, and it is seen that $c(p)$ is not divisible by p. Also we have, by Proposition 4, $J_1(\tau) \equiv c(p) \cdot F \pmod{\tilde{\mathfrak{P}}}$. Since $J_\alpha(\tau) = J_1(\tau) | \tilde{U}_0(p)^{\alpha-1} \equiv c(p) \cdot F | T_{p-1}(p)^{\alpha-1} \pmod{\tilde{\mathfrak{P}}}$, our proposition follows from Proposition 22.

(2) By Proposition 1, it is seen that $c(p) (\text{mod } p) = -\sum_{\theta \in S^*} \beta_\theta$. Also, by Proposition 1, it is seen that $\beta_\theta = -\{\theta^{m_1} (\theta - 12^3)^{m_2} \prod_{\theta \neq \theta' \in S^*} (\theta - \theta')^{-1}\}^2$. We can check the assertion (2) using the table of the supersingular invariants in characteristic p in Deuring [4]. q.e.d.

References

[1] A. O. L. Atkin, Congruences for modular forms, Proc. IBM Conf. on computers mathematical research, Blaricum 1966, published North Holland, 1967.

[2] A. O. L. Atkin, Congruence Hecke operators, Proc. Symp. Pure Math., vol. 12, 33-40.

[3] A. O. L. Atkin and J. N. O'Brien, Some properties of $p(n)$ and $c(n)$ modulo powers of 13, Trans. Amer. Math. Soc. **126** (1967), 442-459.

[4] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg, 14 (1941), 197-272.

[5] B. Dwork, p-adic cycles, Publ. Math I.H.E.S., N° **37** (1969), 27-115.

[6] Y. Ihara, An invariant multiple differential attached to the field of elliptic modular functions of characteristic p, Amer. J. Math., **78** (1971), 137-147.

[7] Y. Ihara, Schwartzian Equations, mimeographed note (1971, unpublished).

[8] Y. Ihara, Non abelian invariant differentials, mimeographed note (1971, unpublished).

[9] Y. Ihara, A Letter to Prof. Serre, July 31, 1971.

[10] J. Lehner, Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$, Amer. J. Math. **71** (1949), 136-148.

[11] M. Newman, Congruences for the coefficients of modular forms and for the coefficients of $j(\tau)$, Proc. Amer. Math. Soc. **9** (1958), 609-612.

[12] J.-P. Serre, Endomorphismes complètement continus des espaces de Banach p-adiques, Publ. Math. I.H.E.S., N° **12** (1962).

(Received October 24, 1972)

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo
113 Japan