J. Math. Soc. Japan
Vol. 46, No. 2, 1994

Modular construction of normal basis

By Keiichi KOMATSU

(Received Nov. 17, 1992)

We denote by $\boldsymbol{Q}$ the rational number field and $\boldsymbol{Z}$ the integer ring. Let F be an imaginary quadratic field, p an odd prime number which splits in F, and $\mathfrak{p}$ a prime ideal of F dividing p. For a positive integer m, we denote by $k=F \pmod{\mathfrak{p}^m}$ the ray class field of F modulo $\mathfrak{p}^m$ and by O_k the integer ring of k. Let $K=F \pmod{\mathfrak{p}^{2m}}$. In [4], Taylor proved the following striking result:

THEOREM A. *The p-integer ring $O_K[1/p]$ has a normal basis over $O_k[1/p]$.*

The above result represents the first major advance outside cyclotomic case. In this paper, we shall show that we can obtain a better result than Theorem A by a different approach in proving the following theorem:

THEOREM. *Let F be an imaginary quadratic field, p an odd prime number which splits in F, $\mathfrak{p}$ a prime ideal of F dividing p and m a positive integer. Let k and K be the ray class field of F modulo $\mathfrak{p}^m$ and $\mathfrak{p}^{[5m/2]}$, respectively. Then the p-integer ring $O_K[1/p]$ has a normal basis over $O_k[1/p]$.*

This theorem will be proved in two steps, in proving Theorems 1 and 2 stated below. We begin by explaining the notations. We fix a positive integer m, a prime p and put

$$\Gamma=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(\boldsymbol{Z});\ a\equiv d\equiv 1 \pmod{p^m},\ b\equiv 0 \pmod{p^m},\ c\equiv 0 \pmod{p^{2m}}\right\},$$

and

$$S=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma;\ d\not\equiv 1 \pmod{p^{m+1}}\right\}.$$

For an integer n with $n>m$, we put

$$\Gamma_n'=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma;\ a\equiv d\equiv 1 \pmod{p^{m+n}},\ b\equiv 0 \pmod{p^n},\ c\equiv 0 \pmod{p^{m+n}}\right\}.$$

Then Γ and Γ_n' are subgroups of $SL_2(\boldsymbol{Z})$ and Γ_n' is a normal subgroup of Γ. Let $\bar{\boldsymbol{Q}}$ be the algebraic closure of $\boldsymbol{Q}$. An element α of $O_{\bar{\boldsymbol{Q}}}[1/p]$ is said to be a p-unit, if α is an invertible element of $O_{\bar{\boldsymbol{Q}}}[1/p]$. For non-negative integer ν, we put $\zeta_\nu=e^{2\pi i/p^\nu}$.

Now we state our Theorem 1 and 2;

THEOREM 1. *Let F, p, $\mathfrak{p}$, m, n, k, Γ, Γ'_n and $\boldsymbol{S}$ be as above. Let $K=F$ (mod $\mathfrak{p}^{m+n}$) be the ray class field of F modulo $\mathfrak{p}^{m+n}$. We suppose that there exists a modular function f_n with respect to Γ'_n which satisfies the following conditions:*

(i)$_n$ *f_n has no poles or zeros on the upper half plane.*

(ii)$_n$ *The q-expansions of f_n at every cusp have coefficients in $\boldsymbol{Z}[\zeta_{m+n}]$, the leading coefficients q-expansions of f_n are p-units and the q-expansion of f_n at ∞ has coefficients in $\boldsymbol{Z}[\zeta_n]$.*

(iii)$_n$ *For any element A of $\boldsymbol{S}$, f_n^A/f_n is a primitive p^n-th root of* 1.

Then $O_K[1/p]$ has a normal basis over $O_k[1/p]$.

THEOREM 2. *If $m<n\leqq 3m/2$, then there exists a modular function f_n with respect to Γ'_n satisfying the above conditions* (i)$_n$, (ii)$_n$ *and* (iii)$_n$

Theorem 1, 2 will be proved in §1, §2, respectively. In §3, we shall prove the following Theorem 3, which shows, so to speak, the limit of our methods.

THEOREM 3. *If there exists a modular function f_n with respect to Γ'_n satisfying the above conditions* (i)$_n$, (ii)$_n$ *and* (iii)$_n$, *then $n\leqq 3m/2$.*

The author would like to express his hearty thanks to Prof. K. Hashimoto, Prof. S. Iyanaga, Prof. T. Kanno, Dr. F. Kawamoto, Prof. N. Kurokawa, Prof. H. Saito and Prof. T. Takagi for their kind advice and encouragement.

§1. Proof of Theorem 1.

Let k be an algebraic number field and O_k the integer ring of k. For a finite algebraic extension K over k, we denote by $(K: k)$ the degree of K over k, by $\mathrm{Tr}_{K/k}$ the trace of K over k and $N_{K/k}$ the norm of K over k. We assume that K is a Galois extension of k with the Galois group $G(K/k)$. If the set $\{\theta^\sigma\}_{\sigma\in G(K/k)}$ of conjugate of an element θ of the ring $O_K[1/p]$ is a basis of $O_K[1/p]$ over $O_k[1/p]$, we say: θ generates a normal basis of $O_K[1/p]$ over $O_k[1/p]$. Let $\zeta_j=e^{2\pi\sqrt{-1}/p^j}$ for a positive integer j. First, we prove the following algebraic Lemma:

LEMMA 1. *Let n be a positive integer and k an algebraic number field with $k\cap\boldsymbol{Q}(\zeta_n)=\boldsymbol{Q}$. We put $k_j=k(\zeta_j)$ for $j=1, 2, \cdots, n$. Let K be a cyclic extension of k of degree p^n with $K\cap k_n=k$. We denote by K_j an intermediate field between k and K with $(K_j: k)=p^j$. If there exists an invertible element θ_n of $O_{k_nK}[1/p]^\times$ with $k_nK=k_n(\theta_n)$ and $\theta_n^{p^n}\in k_n$, then $\theta_j=N_{k_nK/k_jK}(\theta_n)$ belongs to k_jK_j and*

$$\theta = 1+\sum_{j=1}^{n} \mathrm{Tr}_{k_jK_j/K_j}(\theta_j)$$

generates a normal basis of $O_K[1/p]$ *over* $O_k[1/p]$.

PROOF. Let γ be a generator of the Galois group $G=G(Kk_n/k_n)$ with $\theta_n^{\gamma}=\zeta_n\theta_n$. Since $\theta_j^{\gamma}=\zeta_j\theta_j$ implies $\theta_j^{\gamma^{p^j}}=\theta_j$, we have $\theta_j\in k_jK_j$. Hence, in order to prove our Lemma, it is sufficient to show that $\sum_{\sigma\in G}\chi(\sigma)\theta^{\sigma}$ is an invertible element of $O_{k_nK}[1/p]$ for every character χ of G. Since $\theta_j^{p^j}$ is in k_j, we can define a character φ_j of G by

$$\varphi_j(\sigma)=\frac{\theta_j^{\sigma}}{\theta_j} \qquad \text{for every element } \sigma \text{ of } G.$$

Then we have

$$\sum_{\sigma\in G}\chi(\sigma)\theta^{\sigma} = \sum_{\sigma\in G}\chi(\sigma)\Big(1+\sum_{j=1}^{n}\mathrm{Tr}_{k_jK_j/K_j}(\theta_j)\Big)^{\sigma}$$

$$= \sum_{\sigma\in G}\chi(\sigma)+\sum_{j=1}^{n}\sum_{\sigma\in G}\chi(\sigma)\mathrm{Tr}_{k_jK_j/K_j}(\theta_j)^{\sigma}$$

and

$$\sum_{\sigma\in G}\chi(\sigma)\mathrm{Tr}_{k_jK_j/K_j}(\theta_j)^{\sigma} = \sum_{\sigma\in G}\chi(\sigma)\sum_{\rho\in G(k_jK_j/K_j)}\theta_j^{\rho\sigma}$$

$$= \sum_{\sigma\in G}\chi(\sigma)\sum_{\rho\in G(k_jK_j/K_j)}\varphi_j(\sigma)^{\rho}\theta_j^{\rho}$$

$$= \sum_{\rho\in G(k_jK_j/K_j)}\theta_j^{\rho}\sum_{\sigma\in G}\chi(\sigma)\varphi_j(\sigma)^{\rho}\,.$$

Suppose that the order of χ is p^j $(1\leqq j\leqq n)$. Then there exists a unique element ρ of $G(k_jK_j/K_j)$ with $\varphi_j^{\rho}=\chi^{-1}$, which shows $\sum_{\sigma\in G}\chi(\sigma)\theta^{\sigma}=p^n\theta_j^{\rho}$. If χ is trivial, then we have $\sum_{\sigma\in G}\chi(\sigma)\theta^{\sigma}=p^n$. □

Let N be a positive integer and $\mathfrak{F}_N$ the field of all modular functions of level N whose q-expansions at every cusp have coefficients in $\boldsymbol{Q}(e^{2\pi i/N})$ (cf. [**2**]).

Now we define automorphisms of $\mathfrak{F}_N$ (cf. [**3**], p. 211). Let d be an integer such that d is prime to N and σ_d the element of $G(\boldsymbol{Q}(e^{2\pi i/N})/\boldsymbol{Q})$ given by $(e^{2\pi i/N})^{\sigma_d}=e^{2\pi di/N}$. Let f be an element of $\mathfrak{F}_N$ whose q-expansion at ∞ is

$$f(z)=\sum_{n=n_0}^{\infty}a_nq^n\,.$$

We define

$$f^{\sigma_d}=\sum_{n=n_0}^{\infty}a_n^{\sigma_d}q^n\,.$$

Then it is well-known that f^{σ_d} is in $\mathfrak{F}_N$ (cf. [**3**], p. 210). Let $A=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ be

an integral matrix whose determinant d is prime to N. Then there exists a matrix $A'=\begin{pmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{pmatrix}$ in $SL_2(\boldsymbol{Z})$ with $A\equiv\begin{pmatrix}1 & 0\\ 0 & d\end{pmatrix}\begin{pmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{pmatrix} \pmod N$ (cf. [2], Lemma 1.38). Then we can define the following:

$$f^A(z)=f^{\sigma_d}\left(\frac{\alpha' z+\beta'}{\gamma' z+\delta'}\right) \quad \text{(cf. [3], p. 211).}$$

In the rest of this paper, let F denote an imaginary quadratic field, β an element of the integer ring O_F and α_1, α_2 basis of $F/\boldsymbol{Q}$. We denote by $B_{\alpha_1,\alpha_2}(\beta)=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ the regular representation of β with respect to α_1, α_2. Namely, $\beta\alpha_1=a\alpha_1+b\alpha_2$ and $\beta\alpha_2=c\alpha_1+d\alpha_2$ with $a, b, c, d\in\boldsymbol{Q}$. We denote by d_F the discriminant of F. For an integral ideal $\mathfrak{f}$ of F, we denote by $F(\bmod \mathfrak{f})$ the ray class field of F modulo $\mathfrak{f}$. Let $\mathfrak{l}$ be a prime ideal of F whose norm $N_{F/\boldsymbol{Q}}(\mathfrak{l})$ is prime to $\mathfrak{f}$. We denote by $\left(\frac{F(\bmod \mathfrak{f})/F}{\mathfrak{l}}\right)$ the Frobenius automorphism of $F(\bmod \mathfrak{f})/F$ corresponding to $\mathfrak{l}$.

Now, we can describe Shimura reciprocity law which plays an important role in this paper.

LEMMA 2 (cf. [2], p. 213, Theorem 3). *Let $f(z)$ be in $\mathfrak{F}_N$ and $\mathfrak{a}$ a fractional ideal of F with basis α_1, α_2. Let (β) be a prime ideal of F generated by an element β of O_F. We assume that (β) and its complex conjugate $(\bar\beta)$ are distinct and that $\beta\bar\beta$ is prime to d_FN. Let $L=F(\bmod (N))$ be the ray class field of F modulo N. If the imaginary part $\mathrm{Im}(\alpha_1/\alpha_2)$ of α_1/α_2 is positive, then $f(\alpha_1/\alpha_2)$ is in L and*

$$f\left(\frac{\alpha_1}{\alpha_2}\right)^{\left(\frac{L/F}{(\beta)}\right)}=f^{\beta\bar\beta B_{\alpha_1,\alpha_2}(\bar\beta)^{-1}}\left(\frac{\alpha_1}{\alpha_2}\right).$$

Let us remind that p is our fixed prime in F: $(p)=\mathfrak{p}\bar{\mathfrak{p}}$ and that m is the fixed positive integer. We may choose a base ω_1, ω_2 of $\bar{\mathfrak{p}}^m$ with $\mathrm{Im}(\omega_1/\omega_2)>0$ such that ω_1, ω_2/p^m is a basis of O_F. Then we should notice that $\mathfrak{p}$ does not divide ω_1 and that $\bar{\mathfrak{p}}$ does not divide ω_2/p^m.

LEMMA 3. *Let n be an integer with $0<m<n$ and β an element of O_F with $\beta\equiv1 \pmod{\mathfrak{p}^m}$ and $\beta\bar\beta\equiv1 \pmod{p^n}$. We can put $\bar\beta\omega_1=a\omega_1+b\omega_2$, $\bar\beta\omega_2=c\omega_1+d\omega_2$ with $a, b, c, d\in\boldsymbol{Z}$. Then we have $a\equiv b\equiv1 \pmod{p^m}$, $b\equiv0 \pmod{p^m}$ and $c\equiv0 \pmod{p^{2m}}$. Furthermore, if $\beta\not\equiv1 \pmod{\mathfrak{p}^{m+1}}$, then $d\not\equiv1 \pmod{p^{m+1}}$.*

PROOF. It follows from $\beta\equiv1 \pmod{\mathfrak{p}^m}$ and $\beta\bar\beta\equiv1 \pmod{p^n}$ that $\bar\beta$ is congruent to 1 modulo $\mathfrak{p}^m$. Hence we have $\beta\equiv1 \pmod{\bar{\mathfrak{p}}^m}$. This shows $\beta\equiv1 \pmod{p^m}$ and $\bar\beta\equiv1 \pmod{p^m}$. We put $\bar\beta=1+\gamma$. Then $\gamma\omega_1=(a-1)\omega_1+b\omega_2$ and $\gamma\omega_2=c\omega_1+(d-1)\omega_2$ are in $p^m\bar{\mathfrak{p}}^m$, which shows $a\equiv d\equiv1 \pmod{p^m}$ and $b\equiv c\equiv0$

$(\mathrm{mod}\ p^m)$. Since $\omega_2 \in (p^m)$ implies $\omega_2 \in \mathfrak{p}^m$, we have $c\omega_1 \in \mathfrak{p}^{2m}$. Hence $c \equiv 0$ $(\mathrm{mod}\ p^{2m})$ follows from $\omega_1 \notin \mathfrak{p}$. So we have $c\omega_1 \in \bar{\mathfrak{p}}^{3m}$. Now, we recall $\omega_2/p^m \notin \bar{\mathfrak{p}}$. This means $\omega_2 \notin \bar{\mathfrak{p}}^{m+1}$. Suppose that $\beta \not\equiv 1$ $(\mathrm{mod}\ \mathfrak{p}^{m+1})$. Then we have $\gamma\omega_2 \notin \bar{\mathfrak{p}}^{2m+1}$, which shows $d \not\equiv 1$ $(\mathrm{mod}\ p^{m+1})$. □

LEMMA 4. *Let β be an element of O_F with $\beta \equiv 1$ $(\mathrm{mod}\ \mathfrak{p}^{m+n})$ and $\beta\bar{\beta} \equiv 1$ $(\mathrm{mod}\ \mathfrak{p}^n)$. We put $\bar{\beta}\omega_1 = a\omega_1 + b\omega_2$, $\bar{\beta}\omega_2 = c\omega_1 + d\omega_2$ with $a, b, c, d \in \boldsymbol{Z}$. Then we have $a \equiv 1$ $(\mathrm{mod}\ p^n)$, $b \equiv 0$ $(\mathrm{mod}\ p^n)$, $c \equiv 0$ $(\mathrm{mod}\ p^{m+n})$, $d \equiv 1$ $(\mathrm{mod}\ p^{m+n})$.*

PROOF. It follows from $\beta \equiv 1$ $(\mathrm{mod}\ \mathfrak{p}^n)$ and $\beta\bar{\beta} \equiv 1$ $(\mathrm{mod}\ \mathfrak{p}^n)$ that $p^n\bar{\mathfrak{p}}^m$ divides $\bar{\beta} - 1$. We put $\bar{\beta} = 1 - \gamma$. Then $\gamma\omega_1 = (a-1)\omega_1 + b\omega_2 \in p^n\bar{\mathfrak{p}}^{2m}$ and $\gamma\omega_2 = c\omega_1 + (d-1)\omega_2$ $\in p^{m+n}\bar{\mathfrak{p}}^m$ which show $a \equiv 1$ $(\mathrm{mod}\ p^n)$, $b \equiv 0$ $(\mathrm{mod}\ p^n)$, $c \equiv 0$ $(\mathrm{mod}\ p^{m+n})$, $d \equiv 1$ $(\mathrm{mod}\ p^{m+n})$. □

DEFINITION. A modular function f of $\mathfrak{F}_N$ is said to be a unit of $\mathfrak{F}_N$, if f has no poles or zeros on the upper half plane.

LEMMA 5 (cf. [1], p. 37, Theorem 2.2). *Let N be a positive integer, τ an element of F with $\mathrm{Im}(\tau) > 0$ and f a unit of $\mathfrak{F}_{pN}$ whose q-expansions at every cusp have coefficients in $\boldsymbol{Z}[\zeta_N]$. If the lowest non-zero coefficients of q-expansions of f at every cusp are p-units, then $f(\tau)$ is a p-unit in $F(\mathrm{mod}\ p^N)$.*

Now, let β be an element of O_F with $\beta \equiv 1$ $(\mathrm{mod}\ \mathfrak{p}^m)$ and $\beta\bar{\beta} \equiv 1$ $(\mathrm{mod}\ p^n)$. We put $D = \begin{pmatrix} 1 & 0 \\ 0 & \beta\bar{\beta} \end{pmatrix}$. Then there exists a matrix $A(\beta)$ in Γ with $B_{\omega_1,\omega_2}(\beta) \equiv DA(\beta)$ $(\mathrm{mod}\ p^{m+n})$ by Lemma 3. Furthermore, if $\beta \not\equiv 1$ $(\mathrm{mod}\ \mathfrak{p}^{m+1})$, then $A(\beta)$ belongs to S by Lemma 3. If $\beta \equiv 1$ $(\mathrm{mod}\ \mathfrak{p}^{m+n})$, then $A(\beta)$ belongs to Γ_n' by Lemma 4.

After these preparations, we can now conclude our proof of Theorem 1. We recall $K = F(\mathrm{mod}\ \mathfrak{p}^{m+n})$ and $k = F(\mathrm{mod}\ \mathfrak{p}^m)$. Let β be an element of O_F. We put $L = F(\mathrm{mod}\ p^{m+n})$ and $\tau = \omega_1/\omega_2$. Then $f_n(\tau)$ is in L by Lemma 2. We suppose $\beta \equiv 1$ $(\mathrm{mod}\ \mathfrak{p}^{m+n})$ and $\beta\bar{\beta} \equiv 1$ $(\mathrm{mod}\ p^n)$. Then

$$f_n(\tau)^{\left(\frac{L/F}{(\beta)}\right)} = f_n^{DA(\beta)}(\tau) = f_n^{A(\beta)}(\tau) = f_n(\tau)$$

by Lemma 2. Hence we have $f(\tau) \in Kk_n$. Now, we suppose $\beta \equiv 1$ $(\mathrm{mod}\ \mathfrak{p}^m)$, $\beta \not\equiv 1$ $(\mathrm{mod}\ \mathfrak{p}^{m+1})$ and $\beta\bar{\beta} \equiv 1$ $(\mathrm{mod}\ p^n)$. Then

$$f_n(\tau)^{\left(\frac{L/F}{(\beta)}\right)} = f_n^{A(\beta)}(\tau)$$

follows from Lemma 2. Hence it follows from the assumption $(\mathrm{iii})_n$ that $f_n(\tau)^{\left(\frac{L/F}{(\beta)}\right)}/f_n(\tau)$ is a primitive p^n-th root of 1. Hence Theorem 1 follows from Lemma 1.

§ 2. Proof of Theorem 2.

Let $\Omega=\boldsymbol{Z}\tau_1+\boldsymbol{Z}\tau_2$ be a lattice in $\boldsymbol{C}$ with $\mathrm{Im}(\tau_1/\tau_2)>0$. We let σ_Ω denote the usual Weierstrass σ-function:

$$\sigma_\Omega(z)=z\prod_{\omega\in\Omega-\{0\}}\left(1-\frac{z}{\omega}\right)e^{z/\omega+z^2/2\omega^2}.$$

We put

$$\eta_i=2\frac{\sigma_\Omega'(\tau_i/2)}{\sigma_\Omega(\tau_i/2)}\qquad\text{for } i=1,\ 2.$$

We define the Klein form

$$f(a_1,\ a_2\,;\,\tau_1,\ \tau_2)=e^{-(a_1\eta_1+a_2\eta_2)(a_1\tau_1+a_2\tau_2)/2}\sigma_\Omega(a_1\tau_1+a_2\tau_2)$$

for real numbers a_1, a_2. We recall that for b_1, $b_2\in\boldsymbol{Z}$

$$f(a_1+b_1,\ a_2+b_2\,;\,\tau_1,\ \tau_2)=-(-1)^{(b_1+1)(b_2+1)}e^{\pi i(a_1b_2-a_2b_1)}f(a_1,\ a_2\,;\,\tau_1,\ \tau_2)\quad(1)$$

(cf. [1], p. 28). Now let N be a positive integer, r and s integers with $(r/N,\ s/N)\notin\boldsymbol{Z}\times\boldsymbol{Z}$. Let $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL_2(\boldsymbol{Z})$ with $(r(a-1)+cs)/N\in\boldsymbol{Z}$ and ε an integer with $(br+(d-1)s-\varepsilon)/N\in\boldsymbol{Z}$. Then (1) implies:

$$f\left(\left(\frac{r}{N},\ \frac{s}{N}\right)A\,;\,\tau_1,\ \tau_2\right)=-(-1)^{((a-1)r/N+cs/N+1)(br/N+((d-1)s-\varepsilon)/N+1)}$$

$$\times e^{\pi i(br^2+(d-a)rs-cs^2-\varepsilon(ra+cs))/N^2}f\left(\frac{r}{N},\ \frac{s+\varepsilon}{N}\,;\,\tau_1,\ \tau_2\right)\qquad(2)$$

(cf. [1], p. 28). We put

$$\eta(z)=e^{\pi iz/12}\prod_{\nu=1}^{\infty}(1-e^{2\pi i\nu z})$$

and define the Siegel functions

$$g\left(\frac{r}{N},\ \frac{s}{N}\right)=g\left(\frac{r}{N},\ \frac{s}{N}\right)(z)=2\pi i\eta(z)^2f\left(\frac{r}{N},\ \frac{s}{N}\,;\,z,\ 1\right).$$

Then $g(r/N,\ s/N)$ has the following property (cf. [1], p. 31):

(A) $g(r/N,\ s/N)$ is a modular function.

(B) $g(r/N,\ s/N)$ has no poles or zeros on the upper half plane.

(C) $g(r/N,\ s/N)$ has the q-product expression

$$g\left(\frac{r}{N},\ \frac{s}{N}\right)=-q^{((r/N)^2-(r/N)+1/6)/2}e^{\pi i(s/N)(r/N-1)}(1-q^{r/N}e^{(s/N)2\pi i})$$

$$\times\prod_{\nu=1}^{\infty}(1-q^{\nu+r/N}e^{(s/N)2\pi i})(1-q^{\nu-r/N}e^{-(s/N)2\pi i}),$$

where q is $e^{2\pi iz}$.

In the rest of § 2, let n be an integer with $m<n\leqq[3m/2]$, $\mu=n-m$ and s an integer such that p does not divide s. We put

$$\delta_p=\begin{cases}12 & \text{if } p\neq 3,\\ 4 & \text{if } p=3\end{cases}$$

and

$$\tilde{g}\Big(\frac{r}{p^{2m}},\frac{s}{p^{2m}}\Big)=\Big(e^{-\pi i(s/p^{2m})(r/p^{2m}-1)}g\Big(\frac{r}{p^{2m}},\frac{s}{p^{2m}}\Big)\Big)^{\delta_p}.$$

Let

$$X_s=\Big\{\tilde{g}\Big(\frac{p^{\mu}+p^{m+\mu}j}{p^{2m}},\frac{p^{m+\mu}v+(1-p^mj)s}{p^{2m}}\Big);\ v,\ j\in\boldsymbol{Z},\ 0\leqq v,\ j<p^{m-\mu}\Big\}.$$

Then we can easily show by (2) that for any element $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ of Γ, there exists a unique element ξ of X_s and non-zero complex number c' such that

$$\tilde{g}\Big(\frac{ap^{\mu}+cs}{p^{2m}},\frac{bp^{\mu}+ds}{p^{2m}}\Big)=c'\xi\qquad\text{(cf. [1], p. 19 and p. 75)}.$$

For simplicity, we put $\alpha_j=p^{\mu}+p^{m+\mu}j$ and $\beta_{j,v,s}=p^{m+\mu}v+s(1-p^mj)$. Then we obtain by easy calculation the following:

LEMMA 6.

$$\sum_{0\leqq j,v<p^{m-\mu}}\alpha_j^2\equiv p^{2m}\pmod{p^{3m}};$$

$$\sum_{0\leqq j,v<p^{m-\mu}}\alpha_j\beta_{j,v,s}\equiv p^{2m-\mu}s\pmod{p^{2m}};$$

$$\sum_{0\leqq j,v<p^{m-\mu}}\beta_{j,v,s}^2\equiv p^{2m-2\mu}s^2\pmod{p^{2m}}.$$

LEMMA 7. *Let σ be an element of Γ and μ as above. We put*

$$\rho=\sigma^{p^m}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\quad\text{and}\quad h=\prod_{\xi\in X_s}\xi.$$

Then

$$\frac{h^{\rho}}{h}=\zeta_{4m}^{(\delta_p/2)(d-a)sp^{2m-\mu}}.$$

PROOF. We can easily show $a\equiv d\equiv 1\pmod{p^{2m}}$, $b\equiv 0\pmod{p^{2m}}$ and $c\equiv 0\pmod{p^{3m}}$. It follows from (2) and Lemma 6 that

$$\frac{h^{\rho}}{h}=\zeta_{4m}^{(\delta_p/2)\sum_{j,v}(b\alpha_j^2+(d-a)\alpha_j\beta_{j,v,s}-c\beta_{j,v,s}^2)}$$

$$=\zeta_{4m}^{(\delta_p/2)(d-a)sp^{2m-\mu}}.$$

□

LEMMA 8. *Let h be as in Lemma 7 and $\rho=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ an element of Γ'_n. Then*

$$\frac{h^\rho}{h}=\zeta_{4m}^{(\delta_p/2)(bp^{2m}-cs^2p^{2m-2\mu})}.$$

PROOF. For the integer b, we choose an integer b' with $bp^\mu\equiv p^{m+2\mu}b'$ (mod p^{2m}) and $0\leqq b'<p^{m-2\mu}$. We put

$$\varepsilon_v=\begin{cases} p^{m+2\mu}b' & \text{if } 0\leqq v<p^{m-\mu}-p^\mu b' \\ p^{m+2\mu}b'-p^{2m} & \text{if } p^{m-\mu}-p^\mu b'\leqq v<p^{m-\mu}.\end{cases}$$

For simplicity we put $\gamma_{j,v,s}=a\alpha_j+c\beta_{j,v,s}$. Then we have by (2) and Lemma 6

$$\frac{h^\rho}{h}=\zeta_{4m}^{(\delta_p/2)(bp^{2m}-cs^2p^{2m-2\mu}-\Sigma_{j,v}\varepsilon_v\gamma_{j,v,s})}.$$

By easy calculation, we have

$$\begin{aligned}\sum_{j,v}\varepsilon_v\gamma_{j,v,s} &\equiv \sum_v\varepsilon_v\sum_j(ap^\mu+p^{m+\mu}j+cs)\\ &\equiv \sum_v\varepsilon_v\Big(p^m+\frac{p^{2m}(p^{m-\mu}-1)}{2}\Big)\\ &\equiv \sum_v\varepsilon_v\Big(p^m-\frac{p^{2m}}{2}\Big)=0 \pmod{p^{4m}}.\end{aligned}$$

□

In the rest of this section, we put $t=-1+p^{m-\mu}$ and

$$f_n=\Big(\prod_{\xi\in X_1}\xi^{-t^2}\Big)\Big(\prod_{\xi\in X_t}\xi\Big).$$

Let

$$\boldsymbol{S}=\Big\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma;\ d\not\equiv 1 \pmod{p^{m+1}}\Big\}.$$

For an element σ of $\boldsymbol{S}$, we put $\sigma^{p^m}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$. Then we can easily show $d\not\equiv 1$ (mod p^{2m+1}) and $a\not\equiv d$ (mod p^{2m+1}). Hence we have the following Lemma 9 by Lemma 7, 8:

LEMMA 9. *Let σ be an element of $\boldsymbol{S}$. We put $\rho=\sigma^{p^m}$. Then f_n is a modular function with respect to Γ'_n and f_n^ρ/f_n is a primitive p^μ-th root of* 1.

LEMMA 10. *The above modular function f_n has the following property*:

(a) *f_n has no poles or zeros on the upper half plane.*

(b) *The q-expansions of f_n at every cusp have coefficients in $\boldsymbol{Z}[\zeta_{m+n}]$ and the leading coefficients of q-expansions of f_n at every cusp are p-units.*

(c) *The q-expansion of f_n at ∞ has coefficients in $\boldsymbol{Z}[\zeta_n]$.*

PROOF. The property (a) is an immediate consequence of (B) and (b) follows from (C) (cf. [1], p. 37). Let σ_s be an automorphism of $\mathfrak{F}_{p^{4m}}$ as in §1. The property (c) follows from

$$f_n = \prod_{0\leq j,\nu<p^{m-\mu}} \left(\tilde{g}\left(\frac{\alpha_j}{p^{2m}}, \frac{\beta_{j,0,t}}{p^{2m}}\right)^{-t^2} \tilde{g}\left(\frac{\alpha_j}{p^{2m}}, \frac{\beta_{j,0,t}}{p^{2m}}\right)\right)^{\sigma_1 + p^{m+\mu}\nu}. \qquad \square$$

Our Theorem 2 follows now from Lemma 9 and 10.

§3. Proof of Theorem 3.

Let N be a positive integer. We denote by V_N the set of elements $(r/p^N, s/p^N)$ with $0\leqq r<p^N/2$ and $0\leqq s<p^N$ such that r or s is prime to p. Let f be a modular function with $(\mathrm{i})_n$, $(\mathrm{ii})_n$ and $(\mathrm{iii})_n$. It follows from $(\mathrm{iii})_n$ that f^{p^n} is a modular function with respect to Γ. By [1], p. 83, there exist non-zero complex number c and integers $m(r, s)$ with

$$f^{p^n} = c \prod_{(r/p^{2m}, s/p^{2m})\in V_{2m}} g\left(\frac{r}{p^{2m}}, \frac{s}{p^{2m}}\right)^{m(r,s)}.$$

Hence, it follows from [1], p. 82, Theorem 1.1 that there exist non-zero complex number c' and integers $m(r, s)'$ with

$$f = c' \prod_{(r/p^{2m}, s/p^{2m})\in V_{2m}} g\left(\frac{r}{p^{2m}}, \frac{s}{p^{2m}}\right)^{m(r,s)'}.$$

Let σ be any element of S. We put $\rho=\sigma^{p^m}$. In a similar way as in the proof of Lemma 7 and 9 (consider Γ orbit of $g(r/p^{2m}, s/p^{2m})$), we can show that f^ρ/f is a $p^{[m/2]}$-th root of 1. This means $n\leqq[3m/2]$.

References

[1] D. Kubert and S. Lang, Modular units, Grundlehren Math. Wiss., **244**, Springer, 1981.
[2] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami Shoten and Princeton University Press, 1971.
[3] H. M. Stark, L-functions at $s=1$. IV, Adv. in Math., **35** (1980), 197-235.
[4] M. J. Taylor, Relative Galois module structure of rings of integers and elliptic functions II, Ann. of Math., **121** (1985), 519-535.

Keiichi KOMATSU
Department of Mathematics
Tokyo University of
Agriculture and Technology
Fuchu, Tokyo
Japan