Subgroups of the modular group

By Kisao TAKEUCHI

(Communicated by Y. KAWADA)

§1. Introduction.

Let $\Gamma(1)$ be the elliptic modular group $SL_2(\boldsymbol{Z})$ and Γ be any subgroup of $\Gamma(1)$ of finite index. Denote by $\mathrm{Tr}(\Gamma)$ the set of all traces $\mathrm{tr}(\gamma)$ of elements γ of Γ. Then $\mathrm{Tr}(\Gamma)$ is a subset of the rational integer ring $\boldsymbol{Z}$. In particular, $\mathrm{Tr}(\Gamma(1))$ coincides with $\boldsymbol{Z}$. We are interested in the question if there exist any proper subgroups Γ of $\Gamma(1)$ satisfying the following condition,

$$\mathrm{Tr}(\Gamma)=\boldsymbol{Z}\,. \tag{1}$$

Put for any positive integer m,

$$\Gamma(m)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma(1)\,|\,a-1\equiv b\equiv c\equiv d-1\equiv 0 \pmod m\right\}.$$

Then $\Gamma(m)$ is a normal subgroup of $\Gamma(1)$ called the principal congruence subgroup of level m. Any subgroup Γ of $\Gamma(1)$ containing some $\Gamma(m)$ is called the congruence subgroup. The smallest positive integer of such m is called the level of Γ. In this paper we shall prove the following theorem.

THEOREM. *Let Γ be a congruence subgroup of $\Gamma(1)$ such that $\mathrm{Tr}(\Gamma)=\boldsymbol{Z}$. Then Γ coincides with $\Gamma(1)$.*

When we express the level m of Γ as the product of prime integers in the following way;

$$m=\prod_{i=1}^{r} p_i^{e_i}\,, \qquad (e_i\geqq 1) \tag{2}$$

we put

$$d(m)=\sum_{i=1}^{r} e_i\,. \tag{3}$$

We shall prove our theorem by induction on $d(m)$.

NOTATIONS: We denote by $\boldsymbol{Z}$ the ring of rational integers. Let m be a positive integer. Then we denote by $\bar{a}$ the reduction of $a \pmod m$ in $\boldsymbol{Z}/m\boldsymbol{Z}$. Denote by $\boldsymbol{F}_q$ the finite field consisting of q elements. Let S be a subset of a group G. We denote by $\langle S\rangle$ the subgroup of G generated by S.

§ 2. Several lemmas for congruence subgroups.

Let φ_m be the homomorphism of $\Gamma(1)$ to $SL_2(\boldsymbol{Z}/m\boldsymbol{Z})$ defined by

$$\varphi_m\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)=\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix},$$

for any element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $\Gamma(1)$.

LEMMA 1. *The quotient group $\Gamma(1)/\Gamma(m)$ of $\Gamma(1)$ by $\Gamma(m)$ is isomorphic to $SL_2(\boldsymbol{Z}/m\boldsymbol{Z})$ by the above defined φ_m. As to the index of $\Gamma(m)$ we have the following formula;*

$$[\Gamma(1):\Gamma(m)]=m^3\prod_{p\mid m}(1-1/p^2)\ ; \tag{3}$$

This lemma is well known (cf. [1]). We shall omit the proof.

From now on, we shall denote by $\bar{\gamma}$ (resp. $\bar{S}$) the image of an element γ (resp. a subset S) of $\Gamma(1)$ under φ_m.

LEMMA 2. *For a positive integer m, we have*

$$\mathrm{Tr}\,(\Gamma(m))=\{n\in\boldsymbol{Z}\mid n\equiv 2 \pmod{m^2}\}\ .$$

PROOF. Take any element γ of $\Gamma(m)$. Then we can express γ as follows;

$$\gamma=\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} 1+ma_1, & mb_1 \\ mc_1, & 1+md_1 \end{pmatrix}. \tag{4}$$

Taking the determinant of γ, we have

$$a_1+d_1=-m(a_1d_1-b_1c_1)\ . \tag{5}$$

Hence we see that

$$\mathrm{tr}\,(\gamma)=2-m^2(a_1d_1-b_1c_1)\ .$$

Conversely, given any integer n such that $n=2+m^2s$, we put

$$\gamma=\begin{pmatrix} 1+m^2s, & ms \\ m, & 1 \end{pmatrix}.$$

Then γ is contained in $\Gamma(m)$ and $\mathrm{tr}\,(\gamma)=n$. This completes the lemma.

LEMMA 3. (1) *For any prime integer $p\geqq 5$, $SL_2(\boldsymbol{F}_p)/\{\pm\bar{1}_2\}$ is a simple group. $\{\pm\bar{1}_2\}$ is the unique proper normal subgroup of $SL_2(\boldsymbol{F}_p)$.*

(2) *$SL_2(\boldsymbol{F}_3)/\{\pm\bar{1}_2\}$ is isomorphic to the alternating group A_4 of degree 4. The proper normal subgroup of $SL_2(\boldsymbol{F}_3)$ is either $\{\pm\bar{1}_2\}$ or*

$$\left\langle\begin{pmatrix} \bar{0} & \bar{1} \\ -\bar{1} & \bar{0} \end{pmatrix},\begin{pmatrix} \bar{1} & \bar{2} \\ -\bar{1} & -\bar{1} \end{pmatrix}\right\rangle.$$

(3) *$SL_2(\boldsymbol{F}_2)$ is isomorphic to the symmetric group S_3 of degree 3.* $\left\langle\begin{pmatrix}\bar{1} & \bar{1}\\ -\bar{1} & \bar{0}\end{pmatrix}\right\rangle$ *is the unique proper normal subgroup of $SL_2(\boldsymbol{F}_2)$.*

Since this is well known, we omit the proof (cf. [2]).

LEMMA 4. *Let p be any prime integer. Then $SL_2(\boldsymbol{F}_p)$ contains the elements of order p, $p-1$ and $p+1$.*

PROOF. This lemma is also well known (cf. [3]). Since $SL_2(\boldsymbol{F}_p)$ is of order $p(p^2-1)$ by (3), the Sylow p-subgroup of $SL_2(\boldsymbol{F}_p)$ is of order p. Hence there exists an element of order p.

Now put

$$\bar{\tau}_{p-1}=\begin{pmatrix}\omega & 0\\ 0 & 1/\omega\end{pmatrix},$$

where ω is a generator of the multiplicative group $\boldsymbol{F}_p^{\times}$. Then $\bar{\tau}_{p-1}$ is an element of $SL_2(\boldsymbol{F}_p)$ of order $p-1$.

Next let η be a generator of the multiplicative group $(\boldsymbol{F}_{p^2})^{\times}$. Then $\rho=\eta^{p-1}$ is of order $p+1$ and we see that

$$\rho\cdot\rho^p=1\,,\qquad \rho^p\neq\rho\,.$$

Since $\rho+\rho^p$ is contained in $\boldsymbol{F}_p$, we can find an element $\bar{\tau}_{p+1}$ of $SL_2(\boldsymbol{F}_p)$ such that

$$\mathrm{tr}\,(\bar{\tau}_{p+1})=\rho+\rho^p\,.$$

Then $\bar{\tau}_{p+1}$ is conjugate to the matrix $\begin{pmatrix}\rho & 0\\ 0 & \rho^p\end{pmatrix}$. Therefore $\bar{\tau}_{p+1}$ is of order $p+1$. This completes our lemma.

LEMMA 5. *Let p be any prime integer. For two positive integers e_1 and e_2, the commutator group $[\Gamma(p^{e_1}),\Gamma(p^{e_2})]$ of $\Gamma(p^{e_1})$ and $\Gamma(p^{e_2})$ is contained in $\Gamma(p^{e_1+e_2})$.*

PROOF. Take any element γ_i of $\Gamma(p^{e_i})$ $(1\leqq i\leqq 2)$. Then we can express γ_i as follows;

$$\gamma_i=1_2+p^{e_i}\cdot\Delta_i \tag{6}$$

where $\Delta_i=\begin{pmatrix}a_i & b_i\\ c_i & d_i\end{pmatrix}$ is an integral matrix. Now we have

$$\gamma_i^{-1}=1_2+p^{e_i}\cdot\Delta_i^* \tag{7}$$

where

$$\Delta_i^*=\begin{pmatrix}d_i & -b_i\\ -c_i & a_i\end{pmatrix}.$$

By (6) and (7) we have

$$\gamma_1\gamma_2 \equiv 1_2 + p^{e_1}\cdot A_1 + p^{e_2}\cdot A_2 \pmod{p^{e_1+e_2}},$$

$$\gamma_1^{-1}\gamma_2^{-1} \equiv 1_2 + p^{e_1}\cdot A_1^* + p^{e_2}\cdot A_2^* \pmod{p^{e_1+e_2}}.$$

Therefore, we see that

$$\gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1} \equiv 1_2 + p^{e_1}(A_1 + A_1^* + p^{e_1}\cdot A_1A_1^*) + p^{e_2}(A_2 + A_2^* + p^{e_2}\cdot A_2A_2^*) \pmod{p^{e_1+e_2}}.$$

In view of (5) we see that

$$A_i + A_i^* + p^{e_i}A_iA_i^* = 0 \qquad (1 \leqq i \leqq 2).$$

Hence $\gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}$ is contained in $\Gamma(p^{e_1+e_2})$. This completes Lemma 5.

COROLLARY 6. *If $e \geqq 1$, then the centralizer $C(\Gamma(p^e)/\Gamma(p^{e+1}))$ of $\Gamma(p^e)/\Gamma(p^{e+1})$ in $\Gamma(1)/\Gamma(p^{e+1})$ contains $\Gamma(p)/\Gamma(p^{e+1})$.*

PROOF. This is obvious from Lemma 5.

LEMMA 7. *Let p be a prime integer and e be a positive integer. Then $\Gamma(p^e)/\Gamma(p^{e+1})$ is an elementary abelian p-group of type (p, p, p).*

PROOF. By the formula (3) we see that the group $\Gamma(p^e)/\Gamma(p^{e+1})$ is of order p^3. By Corollary 6, $\Gamma(p^e)/\Gamma(p^{e+1})$ is abelian. Now take any element γ of $\Gamma(p^e)$. Then we can express γ as follows;

$$\gamma = 1_2 + p^e\cdot A,$$

where A is an integral matrix. We have the following expansion;

$$\gamma^p = 1_2 + \sum_{k=1}^{p}\binom{p}{k}p^{ek}\cdot A^k.$$

Since $\binom{p}{k}\cdot p^{ek}$ $(1 \leqq k \leqq p)$ is divisible by p^{e+1}, we see that γ^p is contained in $\Gamma(p^{e+1})$. This completes Lemma 7.

LEMMA 8. *Let p be a prime integer such that $p \geqq 3$. Let N be a normal subgroup of $\Gamma(1)$ such that $\Gamma(p^e) \supset N \supseteq \Gamma(p^{e+1})$ for some positive integer e. Then N coincides with either $\Gamma(p^e)$ or $\Gamma(p^{e+1})$.*

PROOF. Assume that $\Gamma(p^e) \supsetneq N \supsetneq \Gamma(p^{e+1})$. Then $\bar{N} = \varphi_{p^{e+1}}(N)$ is a normal subgroup of $\overline{\Gamma(1)} = \Gamma(1)/\Gamma(p^{e+1})$ contained in $\Gamma(p^e)/\Gamma(p^{e+1})$. By Lemma 7 $\bar{N}$ is an elementary abelian p-group of order p or p^2. $\Gamma(1)$ operates on $\bar{N}$ by the conjugation. Hence we have a homomorphism ρ of $\Gamma(1)$ to the automorphism group $\mathrm{Aut}(\bar{N})$ of $\bar{N}$. Since $\bar{N}$ can be considered as a vector space over $\boldsymbol{F}_p$ of dimension 1 or 2, $\mathrm{Aut}(\bar{N})$ is isomorphic to $GL_1(\boldsymbol{F}_p)$ or $GL_1(\boldsymbol{F}_p)$ according to the order of $\bar{N}$. ρ is not trivial because the center of $\overline{\Gamma(1)}$ is $\{\pm\bar{1}_2\}$ for any odd prime p. By Corollary 6, the kernel $\mathrm{Ker}(\rho)$ of ρ contains $\Gamma(p)$. Obviously $\mathrm{Ker}(\rho)$ contains

-1_2. Hence $\mathrm{Ker}(\rho)$ contains $\Gamma(p)\cdot\{\pm 1_2\}$.

First consider the case $p\geqq 5$. By Lemma 3 (1), $\mathrm{Ker}(\rho)$ coincides with $\Gamma(p)\cdot\{\pm 1_2\}$ and ρ can be considered as an injective homomorphism of $\Gamma(1)/\Gamma(p)\cdot\{\pm 1_2\}$ to $GL_2(\boldsymbol{F}_p)$ or $GL_1(\boldsymbol{F}_p)$. Comparing the orders of these groups, the image $\mathrm{Im}(\rho)$ of ρ cannot be contained in $GL_1(\boldsymbol{F}_p)$. Hence $\bar{N}$ must be of order p^2 and $\mathrm{Im}(\rho)$ is a subgroup of $GL_2(\boldsymbol{F}_p)$. Since the matrix $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ is of order p in $\Gamma(1)/\Gamma(p)\cdot\{\pm 1_2\}$, $\rho\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right)$ is of order p in $GL_2(\boldsymbol{F}_p)$. Hence it is contained in $SL_2(\boldsymbol{F}_p)$. This shows that $\mathrm{Im}(\rho)\cap SL_2(\boldsymbol{F}_p)$ is a non-trivial normal subgroup of $\mathrm{Im}(\rho)$. Since $\mathrm{Im}(\rho)$ is isomorphic to the simple group $\Gamma(1)/\Gamma(p)\cdot\{\pm 1_2\}$, $\mathrm{Im}(\rho)\cap SL_2(\boldsymbol{F}_p)$ must coincides with $\mathrm{Im}(\rho)$. Hence $\mathrm{Im}(\rho)$ is contained in $SL_2(\boldsymbol{F}_p)$. Comparing the orders of these groups, we see that $\mathrm{Im}(\rho)$ is a subgroup of $SL_2(\boldsymbol{F}_p)$ of index 2. Hence $\mathrm{Im}(\rho)$ is a normal subgroup of $SL_2(\boldsymbol{F}_p)$ of index 2, which contradicts to Lemma 3 (1).

Now let us consider the case $p=3$. Since $\mathrm{Ker}(\rho)$ is a normal subgroup of $\Gamma(1)$ containing $\Gamma(3)\cdot\{\pm 1_2\}$, $\mathrm{Ker}(\rho)$ coincides with either $\Gamma(3)\cdot\{\pm 1_2\}$ or $\left\langle\Gamma(3),\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\begin{pmatrix}1 & 2\\ -1 & -1\end{pmatrix}\right\rangle$ by Lemma 3 (2).

Assume that $\mathrm{Ker}(\rho)=\Gamma(3)\cdot\{\pm 1_2\}$. Then $\bar{N}$ is of order 3^2 and $\mathrm{Im}(\rho)$ is a subgroup of $GL_2(\boldsymbol{F}_3)$ and is isomorphic to the alternating group A_4 of degree 4. Since $SL_2(\boldsymbol{F}_3)$ is a normal subgroup of $GL_2(\boldsymbol{F}_3)$ of index 2, $\mathrm{Im}(\rho)\cap SL_2(\boldsymbol{F}_3)$ is a normal subgroup of $\mathrm{Im}(\rho)$ of index at most 2. Since $\mathrm{Im}(\rho)$ is isomorphic to A_4, by Lemma 3 $\mathrm{Im}(\rho)\cap SL_2(\boldsymbol{F}_3)$ must coincide with $\mathrm{Im}(\rho)$. Hence $\mathrm{Im}(\rho)$ is contained in $SL_2(\boldsymbol{F}_3)$. Comparing the orders of these groups, we see that $\mathrm{Im}(\rho)$ is a normal subgroup of $SL_2(\boldsymbol{F}_3)$ of index 2 which contradicts to Lemma 3 (2).

Assume that $\mathrm{Ker}(\rho)=\left\langle\Gamma(3),\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix},\begin{pmatrix}1 & 2\\ -1 & -1\end{pmatrix}\right\rangle$. Then $\mathrm{Im}(\rho)$ is of order 3 and is generated by $\rho\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right)$. Hence $\bar{N}$ must be of order 3^2. Since $\mathrm{Aut}(\bar{N})$ is of order $2^4\cdot 3$, $\mathrm{Im}(\rho)$ is a 3-Sylow subgroup of $\mathrm{Aut}(\bar{N})$. Therefore, by taking a suitable basis $\{\bar{\gamma}_1,\bar{\gamma}_2\}$ of $\bar{N}$ over $\boldsymbol{F}_3$, we may assume that

$$\rho\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$

in $GL_2(\boldsymbol{F}_3)$. It follows that $\bar{\gamma}_2$ is fixed by $\rho\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right)$ and $\rho\left(\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\right)$. Hence $\bar{\gamma}_2$ is contained in the center $C(\Gamma(1)/\Gamma(3^{e+1}))$. Therefore we have $\bar{\gamma}_2=-\bar{1}_2$, which is a contradiction because $\Gamma(3^e)$ does not contain -1_2. This completes Lemma 8.

LEMMA 9. *Let N be a normal subgroup of $\Gamma(1)$ such that $\Gamma(2^e)\supsetneqq N\supsetneqq\Gamma(2^{e+1})$ for some positive integer e. Then $\bar{N}=N/\Gamma(2^{e+1})$ is one of the following two*

subgroups;

$$\bar{N}=\begin{cases}\langle\overline{1+2^e\cdot 1_2}\rangle, & \text{if } \bar{N} \text{ is of order } 2,\\ \left\langle\begin{pmatrix}\overline{1+2^e} & \bar{0}\\ \bar{2}^e & \overline{1+2^e}\end{pmatrix},\begin{pmatrix}\overline{1+2^e} & \bar{2}^e\\ \bar{0} & \overline{1+2^e}\end{pmatrix}\right\rangle, & \text{if } \bar{N} \text{ is of order } 4.\end{cases}$$

PROOF. By Lemma 3 we distinguish the following three cases;

(1) $\mathrm{Ker}(\rho)=\Gamma'(1)$,

(2) $\mathrm{Ker}(\rho)=\left\langle\Gamma'(2),\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}\right\rangle$.

(3) $\mathrm{Ker}(\rho)=\Gamma'(2)$.

In the case of (1), $\bar{N}$ is contained in $\overline{\Gamma'(2^e)}\cap C(\overline{\Gamma'(1)})$. Since the center $C(\overline{\Gamma'(1)})$ of $\overline{\Gamma'(1)}=\Gamma'(1)/\Gamma'(2^{e+1})$ can be described explicitly as follows;

$$C(\overline{\Gamma'(1)})=\begin{cases}\{\pm\bar{1}_2\} & \text{if } e=1,\\ \{\pm\bar{1}_2,\ \pm\overline{1+2^e}\cdot\bar{1}_2\} & \text{if } e\geqq 2,\end{cases}$$

we see that for any $e\geqq 1$

$$\bar{N}=\langle\overline{1+2^e}\cdot\bar{1}_2\rangle\,.$$

Next consider the case (2). Take any element γ of N and put

$$\gamma=\begin{pmatrix}1+2^e a_1 & 2^e b_1\\ 2^e c_1 & 1+2^e d_1\end{pmatrix}.$$

Since $\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}$ is contained in $\mathrm{Ker}(\rho)$, we have

$$\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}^{-1}\begin{pmatrix}1+2^e a_1 & 2^e b_1\\ 2^e c_1 & 1+2^e d_1\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}\equiv\begin{pmatrix}1+2^e a_1 & 2^e b_1\\ 2^e c_1 & 1+2^e d_1\end{pmatrix}\pmod{2^{e+1}}.$$

Hence we see that

$$a_1\equiv b_1+d_1 \pmod 2,$$

$$c_1\equiv -b_1 \pmod 2.$$

By (5) we have

$$a_1+d_1\equiv 0 \pmod 2.$$

Hence we see that

$$b_1\equiv c_1\equiv 0 \pmod 2,\qquad a_1\equiv d_1 \pmod 2.$$

Therefore $\bar{N}$ is contained in $C(\overline{\Gamma'(1)})$, which contradicts to our assumption.

Finally consider the case (3). Since $\mathrm{Im}(\rho)$ is isomorphic to $SL_2(\boldsymbol{F}_2)$, $\bar{N}$ must

be of order 4 and ρ can be regarded as an isomorphism of $SL_2(\boldsymbol{F}_2)$ onto $SL_2(\boldsymbol{F}_2)$. Since it is easy to see that any automorphism of $SL_2(\boldsymbol{F}_2)$ is inner, by taking a suitable basis $\{\bar{\gamma}_1, \bar{\gamma}_2\}$ of $\bar{N}$ we may assume that

$$\rho(\gamma)\equiv\gamma \pmod 2$$

in $SL_2(\boldsymbol{F}_2)$ for any γ of $\Gamma(1)$.

Put

$$\gamma_i=\begin{pmatrix}1+2^e a_i & 2^e b_i\\ 2^e c_i & 1+2^e d_i\end{pmatrix} \qquad (1\leqq i\leqq 2)\ .$$

Then by the following relations;

$$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}^{-1}\cdot\gamma_1\cdot\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\equiv\gamma_2 \pmod{2^{e+1}}\ ,$$

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{-1}\cdot\gamma_2\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\equiv\gamma_1\gamma_2 \pmod{2^{e+1}}\ ,$$

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{-1}\cdot\gamma_2\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\equiv\gamma_2 \pmod{2^{e+1}}\ ,$$

we see easily that

$$\bar{\gamma}_1=\begin{pmatrix}\overline{1+2^e} & \bar{0}\\ \overline{2^e} & \overline{1+2^e}\end{pmatrix}, \qquad \bar{\gamma}_2=\begin{pmatrix}\overline{1+2^e} & \overline{2^e}\\ \bar{0} & \overline{1+2^e}\end{pmatrix}.$$

This completes Lemma 9.

LEMMA 10. *Let p be a prime integer. For an element γ of $\Gamma(1)$, γ^p is contained in $\Gamma(p)$ if and only if γ satisfies the following condition*;

$$\mathrm{tr}\,(\gamma)\equiv 2 \pmod p\ . \tag{8}$$

PROOF. Let S_p be the subgroup of $\Gamma(1)$ generated by $\Gamma(p)$ and $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. Then $\bar{S}_p=S_p/\Gamma(p)$ is a p-Sylow subgroup of $\overline{\Gamma(1)}$. Let γ be an element of $\Gamma(1)$ such that γ^p is contained in $\Gamma(p)$. Then by the Sylow's Theorem there exists an element γ_1 of $\Gamma(1)$ such that

$$\gamma_1^{-1}\cdot\gamma\cdot\gamma_1\equiv\begin{pmatrix}1 & s\\ 0 & 1\end{pmatrix} \pmod p\ . \tag{9}$$

Hence we see that γ satisfies the condition (8). Conversely, consider the element γ satisfying (8). Then we can find an element $\bar{\gamma}_1$ of $GL_2(\bar{\boldsymbol{F}}_p)$ where $\bar{\boldsymbol{F}}_p$ is the algebraic closure of $\boldsymbol{F}_p$, satisfying (9). Hence γ^p is contained in $\Gamma(p)$.

LEMMA 11. *Let p be a prime integer such that $p\geqq 5$ and e be a positive integer. Then γ^p is contained in $\Gamma(p^{e+1})$ if any only if γ is contained in $\Gamma(p^e)$.*

PROOF. We shall prove this lemma by induction on e. First consider the case $e=1$. Let us denote by t the trace of γ. If γ^p is contained in $\Gamma(p^2)$, then γ^p is contained in $\Gamma(p)$. Hence by Lemma 10, t can be expressed as follows;

$$t=2+pt_1 .$$

We have the following formula (cf. [4]),

$$\gamma^p=a\cdot\gamma+b1_2 \tag{10}$$

where

$$\begin{pmatrix} a \\ b \end{pmatrix}=\begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix}^p\begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{11}$$

Now we have the following relation;

$$\begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix}^p\equiv\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}^p+pt_1\sum_{k=0}^{p-1}\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}^k\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}^{p-k-1} \pmod{p^2} .$$

Since we have the following formula;

$$\begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}^n=\begin{pmatrix} 1+n & n \\ -n & 1-n \end{pmatrix}$$

for any integer n, we have

$$\begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix}^p\equiv\begin{pmatrix} 1+p & p \\ -p & 1-p \end{pmatrix}+pt_1\begin{pmatrix} -\sum_{k=0}^{p-1}(k+1)k, & -\sum_{k=0}^{p-1}(k+1)^2 \\ \sum_{k=0}^{p-1}k^2, & \sum_{k=0}^{p-1}(k+1)k \end{pmatrix} \pmod{p^2} .$$

Since $\sum_{k=0}^{p-1}(k+1)^2$, $\sum_{k=0}^{p-1}k^2$ and $\sum_{k=0}^{p-1}(k+1)k$ are all divisible by p for any prime integer $p\geqq 5$, we have

$$\begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix}^p\equiv\begin{pmatrix} 1+p & p \\ -p & 1-p \end{pmatrix} \pmod{p^2} . \tag{12}$$

By (10), (11) and (12) we have

$$p\cdot\gamma+(1-p)1_2=1_2 \pmod{p^2} .$$

Hence we see that

$$\gamma\equiv 1_2 \pmod{p} .$$

Next consider the case $e\geqq 2$. Assume that γ^p is contained in $\Gamma(p^{e+1})$. Then γ^p is contained in $\Gamma(p^e)$. Therefore, by the assumption of the induction γ is contained in $\Gamma(p^{e-1})$. If we express γ as follows;

$$\gamma \equiv 1_2 + p^{e-1} \cdot J ,$$

where J is an integral matrix, we have

$$\gamma^p \equiv 1_2 + p^e \cdot J + \sum_{k=2}^{p} \binom{p}{k} \cdot p^{k(e-1)} \cdot J^k \equiv 1_2 \pmod{p^{e+1}} .$$

Since $\binom{p}{k} p^{k(e-1)}$ $(2 \leqq k \leqq p)$ is divisible by p^{e+1}, we see that

$$p^e \cdot J \equiv 0 \pmod{p^{e+1}} .$$

Therefore,

$$p^{e-1} \cdot J \equiv 0 \pmod{p^e} .$$

This shows that γ is contained in $\Gamma(p^e)$. The converse part of our assertion is contained in Lemma 7.

LEMMA 12. *For any positive integer e, γ^3 is contained in $\Gamma(3^{e+1})$ if and only if either γ is contained in $\Gamma(3^e)$ or γ satisfies the following condition*;

$$\mathrm{tr}\,(\gamma) \equiv -1 \pmod{3^{e+1}} . \tag{13}$$

PROOF. If γ is contained in $\Gamma(3^e)$, then by Lemma 7, γ^3 is contained in $\Gamma(3^{e+1})$. Let γ be any element of $\Gamma(1)$ satisfying (13). By the following relation;

$$\gamma^3 = (t^2-1)\gamma - t \cdot 1_2 , \tag{14}$$

where $t = \mathrm{tr}\,(\gamma)$, we see easily that γ^3 is contained in $\Gamma(3^{e+1})$.

We shall prove the converse part of our lemma by induction on e. Consider the case $e=1$. Assume that γ^3 is contained in $\Gamma(3^2)$. Hence by (14), we have

$$(t+1) \cdot \{(t-1) \cdot \gamma - 1_2\} \equiv 0 \pmod{3^2} . \tag{15}$$

Since γ^3 is contained in $\Gamma(3)$, by Lemma 10, we have

$$t \equiv 2 \pmod{3} . \tag{16}$$

Hence $t+1$ is divisible by 3. If $t+1$ is divisible by 3^2, then γ satisfies (13). If $t+1$ is not divisible by 3^2, then by (15) we have

$$(t-1) \cdot \gamma - 1_2 \equiv 0 \pmod{3} .$$

In view of (16), we see that γ is contained in $\Gamma(3)$.

Consider now the case $e \geqq 2$. Assume that γ^3 is contained in $\Gamma(3^{e+1})$. Then γ^3 is contained in $\Gamma(3^e)$. Therefore, by the assumption of the induction, γ is contained in $\Gamma(3^{e-1})$ or $t = \mathrm{tr}\,(\gamma)$ satisfies the condition;

$$t \equiv -1 \pmod{3^e} . \tag{17}$$

If γ is contained in $\Gamma(3^{e-1})$, we can express γ as follows;

$$\gamma=1_2+3^{e-1}\cdot\Delta\,. \tag{18}$$

Therefore we have

$$\gamma^3=1_2+3^e\cdot\Delta+3^{2e-1}\cdot\Delta^2+3^{3(e-1)}\cdot\Delta^3\equiv 1_2 \pmod{3^{e+1}}\,.$$

Since 3^{2e-1} and $3^{3(e-1)}$ are divisible by 3^{e+1}, we have

$$3^e\cdot\Delta\equiv 0 \pmod{3^{e+1}}\,.$$

Hence

$$3^{e-1}\cdot\Delta\equiv 0 \pmod{3^e}\,.$$

This shows that γ is contained in $\Gamma(3^e)$.

If t satisfies (17), then by (14) we have

$$(t+1)/3^e\cdot\{(t-1)\cdot\gamma-1_2\}=0 \pmod 3. \tag{19}$$

Assume that $(t+1)/3^e$ is not divisible by 3. Then we have

$$(t-1)\cdot\gamma-1_2\equiv 0 \pmod 3\,.$$

By (17) we see that γ is contained in $\Gamma(3)$. Hence by Lemma 2,

$$t\equiv 2 \pmod{3^2}\,.$$

This contradicts to (17). Therefore, $t+1$ must be divisible by 3^{e+1}. This completes Lemma 12.

For any positive integer e, we denote by N_e the subgroup of $\Gamma(1)$ generated by $\Gamma(2^{e+1})$ and an element δ_e of $\Gamma(1)$ defined by

$$\delta_e\equiv(1+2^e)1_2 \pmod{2^{e+1}}\,.$$

Then N_e is a subgroup of $\Gamma(2^e)$ such that $\bar{N}_e=N_e/\Gamma(2^{e+1})$ is of order 2 (cf. Lemma 9). We shall prove the following lemma.

LEMMA 13. (1) *γ^2 is contained in N_1 if and only if either γ is contained in $\Gamma(2)$ or $t=\mathrm{tr}(\gamma)$ satisfies the condition*;

$$\mathrm{tr}(\gamma)\equiv 0 \pmod{2^2}\,. \tag{20}$$

(2) *For any positive integer e, γ^2 is contained in N_{e+1} if and only if γ is contained in $\langle N_e, -1_2\rangle$.*

PROOF. (1) For any element γ of $\Gamma(1)$ we have the relation;

$$\gamma^2-t\cdot\gamma+1_2=0\,, \tag{21}$$

where $t=\mathrm{tr}(\gamma)$. Assume that γ^2 is contained in N_1. Since N_1 coincides with

$\langle \Gamma(2^2), -1_2 \rangle$, we see that

$$t \cdot \gamma \equiv 0 \text{ or } 2 \cdot 1_2 \pmod{2^2} . \tag{22}$$

Hence we see that t is divisible by 2. If $t/2$ is divisible by 2, then t satisfies (20). If $t/2$ is not divisible by 2, then by (22) γ is contained in $\Gamma(2)$. The converse part of our lemma is easily proved by (21) and Lemma 7.

(2) Assume that γ^2 is contained in N_{e+1}. This means that

$$\gamma^2 \equiv \varepsilon_{e+1} 1_2 \pmod{2^{e+2}} ,$$

where $\varepsilon_{e+1} = 1$ or $1+2^{e+1}$. By (21) we have

$$t \cdot \gamma \equiv 2 \cdot \varepsilon_e \cdot 1_2 \pmod{2^{e+2}} .$$

Hence t is divisible by 2 and we have

$$t/2 \cdot \gamma \equiv \varepsilon_e \cdot 1_2 \pmod{2^{e+1}} . \tag{23}$$

Taking the determinant of both sides of (23), we have

$$(t/2)^2 \equiv 1 \pmod{2^{e+1}} .$$

Hence

$$t/2 \equiv \pm \varepsilon_e \pmod{2^{e+1}} .$$

By (23) we see that γ is contained in $\langle N_e, -1_2 \rangle$. The converse part is easily seen by Lemma 7 and by the following relation;

$$(1+2^e)^2 \equiv 1+2^{e+1} \pmod{2^{e+2}} ,$$

for any integer $e \geqq 2$.

§ 3. Proof in the case $m=p$.

In this section we shall prove our theorem in the case $d(m)=1$ i.e. m is a prime integer p. Let Γ be a subgroup of $\Gamma(1)$ containing $\Gamma(p)$ with the condition (1).

First consider the case $p \geqq 3$. By Lemma 4 there exists an element γ of $\Gamma(1)$ such that $\bar{\gamma}$ is of order $p-1$ in $SL_2(\boldsymbol{F}_p)$. Since Γ satisfies the condition (1), we can find an element γ_{p-1} of Γ such that $\mathrm{tr}(\bar{\gamma}_{p-1}) = \mathrm{tr}(\bar{\gamma})$ in $\boldsymbol{F}_p$. Then $\bar{\gamma}_{p-1}$ is of order $p-1$. Similarly, we can find an element γ_{p+1} of Γ such that $\bar{\gamma}_{p+1}$ is of order $p+1$ in $SL_2(\boldsymbol{F}_p)$. Now take an element γ_p of Γ such that $\mathrm{tr}(\gamma_p)-2$ is divisible by p but not by p^2. Then by Lemma 2 and Lemma 10, we see that γ_p is of order p in $SL_2(\boldsymbol{F}_p)$.

Let q be any prime integer and q^r be the highest power of q dividing

$(p-1)p(p+1)$. If q is an odd prime integer, q^r divides one of $p-1$, p or $p+1$ because $(p-1)/2$, p and $(p+1)/2$ are mutually relatively prime. If $q=2$, then 2^{r-1} divides $p-1$ or $p+1$ by the same reasons as above. Therefore we see that the order of $\Gamma/\Gamma'(p)$ is a multiple of $p(p^2-1)/2$. This means that Γ is of index at most 2. Hence Γ is a normal subgroup of $\Gamma(1)$. By the following proposition, we see that Γ coincides with $\Gamma(1)$.

PROPOSITION 1. *Let Γ be a normal subgroup of $\Gamma(1)$ with the condition (1). Then Γ coincides with $\Gamma(1)$.*

PROOF. By the condition (1) Γ contains an element γ_2 (resp. γ_3) such that $\mathrm{tr}(\gamma_2)=0$ (resp. $\mathrm{tr}(\gamma_3)=-1$). γ_2 is conjugate to $\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ (resp. γ_3 is conjugate to $\begin{pmatrix}0&1\\-1&1\end{pmatrix}^{\pm1}$). Hence $\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ and $\begin{pmatrix}0&1\\-1&1\end{pmatrix}$ are contained in Γ. Since these two elements generate $\Gamma(1)$, Γ coincides with $\Gamma(1)$. This completes Proposition 1.

Next consider the case $p=2$. In the same way as in the case $p\geqq3$, we can find an element γ_2 (resp. γ_3) of Γ such that $\bar{\gamma}_2$ (resp. $\bar{\gamma}_3$) is of order 2 (resp. 3) in $SL_2(\boldsymbol{F}_2)$. Hence $\bar{\Gamma}$ coincides with $SL_2(\boldsymbol{F}_2)$. This shows that Γ coincides with $\Gamma(2)$ in the case $p=2$.

§ 4. Proof in the case $m=p^e$.

In this section we shall prove our theorem in the case $m=p^e$ for a prime integer p. Let Γ be a subgroup of $\Gamma(1)$ with the condition (1). Assume that Γ contains $\Gamma(p^e)$ for a positive integer e. We use the induction on e. In the case $e=1$ we have already finished in § 3. Now assume that the assertion is valid for any integer smaller than e. $\langle\Gamma,\Gamma(p^{e-1})\rangle$ contains $\Gamma(p^{e-1})$ and satisfies the condition (1). Hence by the assumption of the induction we see that $\langle\Gamma,\Gamma(p^{e-1})\rangle$ coincides with $\Gamma(1)$.

Since $\Gamma\cap\Gamma(p^{e-1})$ lies between $\Gamma(p^e)$ and $\Gamma(p^{e-1})$, by Lemma 7 $\Gamma\cap\Gamma(p^{e-1})$ is a normal subgroup of $\Gamma(p^{e-1})$. On the other hand, $\Gamma\cap\Gamma(p^{e-1})$ is a normal subgroup of Γ. Therefore $\Gamma\cap\Gamma(p^{e-1})$ is a normal subgroup of $\langle\Gamma,\Gamma(p^{e-1})\rangle=\Gamma(1)$.

Now consider the case $p\geqq5$. By Lemma 8, $\Gamma\cap\Gamma(p^{e-1})$ coincides with $\Gamma(p^{e-1})$ or $\Gamma(p^e)$. If $\Gamma\cap\Gamma(p^{e-1})=\Gamma(p^{e-1})$, then Γ contains $\Gamma(p^{e-1})$. By the assumption of the induction, we see that Γ coincides with $\Gamma(1)$. Assume that $\Gamma\cap\Gamma(p^{e-1})=\Gamma(p^e)$. Now we consider the subgroup $\Gamma\cap\Gamma(p^{e-2})$ if $e\geqq3$ (resp. $\Gamma\cap S_p$ if $e=2$ where $S_p=\left\langle\Gamma(p),\begin{pmatrix}1&1\\0&1\end{pmatrix}\right\rangle$). Then $\Gamma\cap\Gamma(p^{e-2})/\Gamma(p^e)$ (resp. $\Gamma\cap S_p/\Gamma(p^2)$) is an elementary abelian p-group of order p^3 (resp. p). Hence by Lemma 11, $\Gamma\cap\Gamma(p^{e-2})$ coincides with $\Gamma(p^{e-1})$ if $e\geqq3$. In this case Γ contains $\Gamma(p^{e-1})$. Hence $\Gamma\cap\Gamma(p^{e-1})=\Gamma(p^{e-1})$,

which contradicts to our assumption. If $e=2$, then by Lemma 11, $\Gamma\cap S_p$ is contained in $\Gamma(p)$. Hence $\Gamma(p^2)=\Gamma\cap\Gamma(p)=(\Gamma\cap S_p)\cap\Gamma(p)=\Gamma\cap S_p$, which is a contradiction.

Next consider the case $p=3$. By Lemma 8 we see that $\Gamma\cap\Gamma(3^{e-1})$ coincides with $\Gamma(3^{e-1})$ or $\Gamma(3^e)$. If $\Gamma\cap\Gamma(3^{e-1})=\Gamma(3^{e-1})$, then Γ contains $\Gamma(3^{e-1})$. Hence by the assumption of the induction, we see that Γ coincides with $\Gamma(1)$.

Assume that $\Gamma\cap\Gamma(3^{e-1})=\Gamma(3^e)$. Take an element γ of Γ satisfying the following conditions;

$$\mathrm{tr}\,(\gamma)\equiv -1 \pmod{3^{e-1}}\,, \tag{24}$$

$$\mathrm{tr}\,(\gamma)\not\equiv -1 \pmod{3^e}\,. \tag{25}$$

This is possible because Γ satisfies the condition (1). Then by Lemma 10 and Lemma 12, γ^3 is contained in $\Gamma(3^{e-1})\cap\Gamma=\Gamma(3^e)$. Hence by Lemma 12, in view of (25), we see that γ is contained in $\Gamma(3^{e-1})$. By Lemma 2, we have

$$\mathrm{tr}\,(\gamma)\equiv 2 \pmod{3^{2(e-1)}}\,. \tag{26}$$

If $e\geqq 3$, then this contradicts to (24). If $e=2$, we may take γ such that $\mathrm{tr}\,(\gamma)=5$. This contradicts to (26).

Finally consider the case $p=2$. If $\Gamma\cap\Gamma(2^{e-1})$ is of index at most 2 in $\Gamma(2^{e-1})$, then Γ is of index at most 2 in $\Gamma(1)$. Hence Γ is a normal subgroup of $\Gamma(1)$. By Proposition 1, we see that Γ coincides with $\Gamma(1)$. Now we may assume that $\Gamma\cap\Gamma(2^{e-1})/\Gamma(2^e)$ is of order at most 2. By Lemma 9, $\Gamma\cap\Gamma(2^{e-1})$ is contained in $N_{e-1}=\langle\Gamma(2^e),\,\delta_{e-1}\rangle$.

Assume that $e=2$. We take an element γ of Γ such that

$$\mathrm{tr}\,(\gamma)=6\,. \tag{27}$$

Then by Lemma 10, γ^2 is contained in $\Gamma\cap\Gamma(2)$. Hence it is contained in N_1. In view of (27), by Lemma 13, we see that γ is contained in $\Gamma\cap\Gamma(2)$ and hence in N_1. Therefore, by Lemma 2, we see that

$$\mathrm{tr}\,(\gamma)\equiv\pm 2 \pmod{2^4}\,.$$

This contradicts to (27).

Assume that $e\geqq 3$. Take any element γ of $\Gamma\cap\Gamma(2^{e-2})$. Then γ^2 is contained in $\Gamma\cap\Gamma(2^{e-1})$. Hence it is contained in N_{e-1}. By Lemma 13, γ is contained $\langle N_{e-2},-1_2\rangle$. If $-\gamma$ is contained in N_{e-2}, then it is contained in $\Gamma(2^{e-2})$. Hence -1_2 is contained in $\Gamma(2^{e-2})$. This is a contradiction if $e\geqq 4$. Therefore, if $e\geqq 4$, then γ is contained in N_{e-2}. If $e=3$, then -1_2 is contained in N_1. Hence γ is contained in N_1. Therefore, we see that $\Gamma\cap\Gamma(2^{e-2})$ is contained in N_{e-2} for any

$e \geqq 3$. On the other hand, we have $\Gamma(2^{e-2}) = \langle \Gamma \cap \Gamma(2^{e-2}), \Gamma(2^{e-1}) \rangle$ because $\langle \Gamma, \Gamma(2^{e-1}) \rangle$ coincides with $\Gamma(1)$. Hence $\Gamma(2^{e-2})$ is contained in N_{e-2}, which is a contradiction.

§ 5. Proof in the general case.

Let Γ be a subgroup of $\Gamma(1)$ with the condition (1). Assume that Γ contains $\Gamma(m)$, where m is expressed as follows;

$$m = \prod_{i=1}^{r} p_i^{e_i} \qquad (e_i \geqq 1) .$$

Since we have already finished the proof of our theorem in the case $r=1$ in § 4, we may assume that $r \geqq 2$. Now put

$$m_i = m/p_i \qquad (1 \leqq i \leqq r) . \tag{28}$$

By the assumption of the induction, we may assume that

$$\Gamma(1) = \langle \Gamma, \Gamma(m_i) \rangle \qquad (1 \leqq i \leqq r) . \tag{29}$$

Now we shall prove the following proposition.

PROPOSITION 2. *Let the notations be as above. If $r \geqq 2$; then under the assumption* (29), *$\Gamma \cap \Gamma(m_i)$ $(1 \leqq i \leqq r)$ is a normal subgroup of $\Gamma(1)$.*

PROOF. Since Γ normalizes $\Gamma \cap \Gamma(m_i)$, by (29), it is enough to show that $\Gamma(m_j)$ $(j \neq i)$ normalizes $\Gamma \cap \Gamma(m_i)$. Since both of $\Gamma(m_i)$ and $\Gamma(m_j)$ are normal subgroups of $\Gamma(1)$, the commutator subgroup $[\Gamma(m_i), \Gamma(m_j)]$ of $\Gamma(m_i)$ and $\Gamma(m_j)$ is contained in $\Gamma(m_i) \cap \Gamma(m_j)$. Hence it is contained in $\Gamma(m)$. Therefore, $\gamma_j^{-1}(\Gamma \cap \Gamma(m_i))\gamma_j$ is contained in $\Gamma \cap \Gamma(m_i)$ for any element γ_j of $\Gamma(m_j)$. This completes Proposition 2.

Consider the case $e_i = 1$ for at least two indices i. Since $\Gamma(m_i)/\Gamma(m)$ is isomorphic to $SL_2(\boldsymbol{F}_{p_i})$, by Proposition 2 $\Gamma \cap \Gamma(m_i)/\Gamma(m)$ is isomorphic to a normal subgroup $\bar{M}_i$ of $SL_2(\boldsymbol{F}_{p_i})$. By Lemma 3, as to the index of $\bar{M}_i$, there are the following cases;

$$[SL_2(\boldsymbol{F}_{p_i}) : \bar{M}_i] = \begin{cases} 1,\ 2,\ 6 & \text{if } p_i = 2 , \\ 1,\ 3,\ 12,\ 24 & \text{if } p_i = 3 , \\ 1,\ p_i(p_i^2-1)/2,\ p_i(p_i^2-1) & \text{if } p_i \geqq 5 . \end{cases} \tag{30}$$

Since we have the following equality;

$$[\Gamma(1) : \Gamma] = [\Gamma(m_i) : \Gamma \cap \Gamma(m_i)] = [SL_2(\boldsymbol{F}_{p_i}) : \bar{M}_i]$$

for at least two indices i, we see easily that $[\Gamma(1) : \Gamma] = 1$.

Consider the case $e_i = 1$ for only one index i. Then we have $e_j \geqq 2$ for any $j \neq i$. Hence $\Gamma(m_j)/\Gamma(m)$ is of order p_j^3. In view of (30), $[\Gamma(1) : \Gamma] = [SL_2(\boldsymbol{F}_{p_i}) : \bar{M}_i]$

divides p_j^3 if and only if either $[\Gamma(1);\Gamma]=1$ or $p_i=p_j$. However, the latter case is impossible.

Finally consider the case $e_i \geqq 2$ for all index i. In this case $[\Gamma(1):\Gamma]$ must divide p_i^3 for all i. Hence it is equal to 1. This completes the proof of our theorem.

References

[1] Shimura, G., Introduction to the arithmetic theory of automorphic functions, Iwanami and Princeton Univ., 1971.
[2] Huppert, B., Endliche Gruppen I, Springer, 1967.
[3] Gierster, J., Die Untergruppen der Galois'schen Gruppe der Modulargleichungen für den Fall eines primzahligen Transformationsgrades, Math. Ann. **18** (1881), 319-365.
[4] Takeuchi, K., On a Fuchsian group commensurable with the unimodular group, J. Fac. Sci. Univ. Tokyo, Sec. I, **15** (1968), 107-109.

(Received October 24, 1972)

Department of Mathematics
Faculty of Science and Engineering
Saitama University
Urawa, Saitama
338 Japan