J. Math. Kyoto Univ. (JMKYAZ)
13-2 (1973) 381-390

Generators and relations of $\Gamma_0(N)$

By

Yasuhiro CHUMAN

(Communicated by Professor Nagata, July 3, 1972)

Let $\boldsymbol{Z}$ denote a ring of rational integers, and Γ denote the elliptic modular group $SL_2(Z)/\pm 1$. Let T (resp. S) denote the image in Γ of the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\left(\text{resp.} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right)$, and the matrix and its image in Γ will be identified in the following, thus

$$T=\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Then as is well known Γ is generated by T and S.

Let $\Gamma_0(N)$ denote the congruence subgroup of level N, i.e.

$$\Gamma_0(N)=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma \,|\, c \equiv 0 \bmod N\right\}.$$

If N is a prime p, it is easy to see that $\boldsymbol{R}=\{1, ST^i \,|\, i=0, 1,\dots, p-1\}$ is a system of representatives of the coset $\Gamma_0(N)\backslash\Gamma$. Furthermore $\boldsymbol{R}$ satisfies the following condition (F) introduced by Schreier [3] p.177.

(F) Let R be in $\boldsymbol{R}$ and R' be the element of Γ obtained by dropping the last term of R (e.g. if $R=ST^i$, then $R'=ST^{i-1}$), then R' is again in $\boldsymbol{R}$. Hence one can apply Reidemeister-Schreier method, and write down a system of generators and their fundamental relations of $\Gamma_0(p)$. It was actually carried out by Rademacher in [2].

In this note, we shall do a similar thing for general N.

1. Representatives of $\Gamma_0(N)\backslash\Gamma$. Our first task is to construct a system of coset representatives of $\Gamma_0(N)\backslash\Gamma$ satisfying the condition (F).

Lemma 1. *Let Γ_∞ denote the subgroup of Γ generated by T. Every double coset $\Gamma_0(N)\gamma\Gamma_\infty(\gamma\in\Gamma)$ contains an element of the form $ST^\alpha S$ $(\alpha\in\boldsymbol{Z})$.*

Proof. Let $\gamma=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Since $(a, c)=1$, we can find $x, y\in\boldsymbol{Z}$ such that $ax+cy=1$. Let t be the product of prime divisors of N co-prime to x, and put $x'=x-tc$, $y'=y-ta$. Then $ax'+cy'=1$ and $(x', N)=1$, hence there exist $z', w'\in\boldsymbol{Z}$ such that $g=\begin{bmatrix} x' & y' \\ Nz' & w' \end{bmatrix}\in\Gamma_0(N)$. Now $g\gamma=\begin{bmatrix} 1 & b' \\ c' & d' \end{bmatrix}$ by some $b', c', d'\in\boldsymbol{Z}$, and $g\gamma T^{-b'}=\begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix}=ST^\alpha S$ by some $\alpha\in\boldsymbol{Z}$ (Q. E. D.).

Lemma 2. *$ST^\alpha S$ and $ST^\beta S$ are in the same double coset if and only if the following two conditions* (1) *and* (2) *are satisfied*

(1) $$(\alpha, N)=(\beta, N).$$

Putting $(\alpha, N)=t$, $\alpha=\alpha' t$, $\beta=\beta' t$,

(2) $$\alpha'\equiv\beta' \bmod (t, N/t).$$

In paticular every $ST^\alpha S$ with α co-prime to N lies in the same double coset $\Gamma_0(N)TST\Gamma_0(N)=\Gamma_0(N)S\Gamma_\infty$.

Proof. $\Gamma_0(N)ST^\alpha S\Gamma_\infty\ni ST^\beta S\Leftrightarrow \exists\, x\in\boldsymbol{Z},\ ST^\alpha ST^x ST^{-\beta}S\in\Gamma_0(N)\Leftrightarrow$ $\exists\, x\in\boldsymbol{Z},\ \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ -x & 1 \end{bmatrix}\begin{bmatrix} 1 & -\beta \\ 0 & 1 \end{bmatrix}\in S\Gamma_0(N)S\Leftrightarrow$

(3) $$\exists\, x\in\boldsymbol{Z},\ \alpha-\beta+\alpha\beta x\equiv 0 \bmod N.$$

The last condition (3) obviously implies $(\alpha, N)=(\beta, N)$. Putting $(\alpha, N)=t$, $\alpha=\alpha' t$, $\beta=\beta' t$; (3) $\Leftrightarrow \exists\, x\in\boldsymbol{Z},\ \alpha'-\beta'+t\alpha'\beta' x\equiv 0 \bmod N/t\Leftrightarrow \alpha'-\beta'\equiv 0 \bmod (t, N/t)$ as wanted.

The last statment follows from the equation

$$STS=\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}=T^{-1}ST^{-1}\in\Gamma_0(N)S\Gamma_\infty \quad \text{(Q. E. D.).}$$

For each proper divisor t of N, let $\{x(t, i) | 1 \leqq i \leqq \varphi(t, N/t)\}$ be a complete system of representatives of irreducible residue class $(\boldsymbol{Z}/(t, N/t)\boldsymbol{Z})^{\times} \bmod (t, N/t)$, chosen in such a way that any $x(t, i) < N$ and $(x(t, i), N) = 1$. Such a system of representatives certainly exists, because the natural map $(\boldsymbol{Z}/N\boldsymbol{Z})^{\times} \to (\boldsymbol{Z}/(t, N/t)\boldsymbol{Z})^{\times}$ is surjective.

We fix the representatives $x(t, i)$ once for all, and let M be a subset of $\boldsymbol{Z}$ defined by $\{tx(t, i) | 1 \leqq i \leqq (t, N/t)\}$ where t is extended over all proper divisors of N. Put $\boldsymbol{S} = \{1, S, ST^{x}S | x \in M\}$. Then by lemma 1, 2 $\boldsymbol{S}$ is a complete system of representatives of $\Gamma_0(N)\backslash\Gamma/\Gamma_\infty$, and its cardinality is equal to $\sum_{t/N} \varphi(t, N/t)$.

Proposition 1. *Put*

$$\boldsymbol{R} = \{I, ST^{k}, ST^{x}ST^{j(x)} | 0 \leqq k \leqq N-1, x \in M, 0 \leqq j(x) \leqq n(x)-1\},$$

where $n(x)$ denotes the smallest positive integer such that $n(x)x^2 \equiv 0 \bmod N$. Then $\boldsymbol{R}$ is a complete system of representatives of $\Gamma_0(N)\backslash\Gamma$. Furthermore $\boldsymbol{R}$ satisfies the Schreier condition (F).

Proof. As we remarked, Γ is a disjoint union of $\Gamma_0(N)g\Gamma_\infty$ with $g \in \boldsymbol{S}$. Let γ run through a complete system of representatives of $g^{-1}\Gamma_0(N)g \cap \Gamma_\infty\backslash\Gamma_\infty$, then $\Gamma_0(N)g\Gamma_\infty = \bigcup_{\gamma}\Gamma_0(N)g\gamma$ (disjoint). If $g = ST^{x}S$, $T^{n} \equiv 0 \bmod g^{-1}\Gamma_0(N)g \cap \Gamma_\infty$ if and only if $x^2 n \equiv 0 \bmod N$. Hence as a system of representatives of $g^{-1}\Gamma_0(N)g \cap \Gamma_\infty\backslash\Gamma_\infty$, we can take $\{I, T, \ldots, T^{n(x)-1}\}$. If $g = S$, it is easy to see that $\{T^{k} | 0 \leqq k \leqq N-1\}$ is a system of representatives. Now our last statment is obvious, because we have $ST^{k}(0 \leqq k \leqq N-1)$ in $\boldsymbol{R}$.

2. Generators and relations of $\Gamma_0(N)$. Now, we can apply Reidemeister-Schreier method. For any $X \in \Gamma$, let $\overline{X}$ denote the element R of $\boldsymbol{R}$ such that $X \in \Gamma_0(N)\overline{X}$. Then $\Gamma_0(N)$ is generated by

$$\text{(G)} \qquad \{RT\overline{RT}^{-1}, RS\overline{RS}^{-1} | R \in \boldsymbol{R}\}$$

with the set of defining relations

$$\text{(R)} \qquad \{RS^2R^{-1} = 1, R(ST)^3R^{-1} = 1 | R \in \boldsymbol{R}\}.$$

In the following, we shall explicitly write them out, and as Rademacher did in prime level case, simplify them until only a few (or none) of relations left.

(1) *Generators.* For each R in $\boldsymbol{R}$, we can easily check that $\overline{RT}$ and $\overline{RS}$ are given by the following:

$$\overline{IT}=I,\ \overline{ST^kT}=ST^k(k=0,\ 1,\ 2,\ \dots,\ N-2),\ \overline{ST^{N-1}T}=S,$$

$$\overline{ST^xST^{j(x)}T}=ST^xST^{j(x)+1}\ (j(x)=0,\ 1,\ 2,\ \dots,\ n(x)-2),$$

$$\overline{ST^xST^{n(x)-1}T}=ST^xS$$

and

$$\overline{IS}=S,\ \overline{SS}=T,\ \overline{ST^kS}=ST^{k*}\ ((k,\ N)=1,\ kk^*\equiv-1 \bmod N),$$

$$\overline{ST^kS}=ST^kS((k,\ N)\neq 1,\ k\in M),$$

$$\overline{ST^kS}=ST^{x(k)}ST^j\ ((k,\ N)\neq 1,\ k\notin M,\ x(jk+1)\equiv k \bmod N),$$

$$\overline{ST^xSS}=ST^x,\ \overline{ST^xST^jS}=ST^{k(j)}((jx-1,\ N)=1,\ k(jx-1)\equiv -x \bmod N),$$

$$\overline{ST^xST^jS}=ST^{x'}ST^{j'}\ ((jx-1,\ N)\neq 1,\ (jx-1)(j'x'-1)\equiv -xx' \bmod N).$$

Hence we can explicitly write (G) out as the following:

$$\{I,\ T,\ U,\ V(k),\ V(x,j)|1\leqq k\leqq N-1,\ 1\leqq j\leqq n(x)-1,\ x\in M\};$$

$$U=ST^NS,$$

$$V(k)=ST^kST^{-k^*}S \qquad ((k,\ N)=1)$$

$$V(k)=ST^kST^{-j(k)}ST^{-x(k)}S \qquad ((k,\ N)\neq 1,\ k\notin M)$$

$$=ST^kST^{n(k)}ST^{-k}S \qquad ((k,\ N)\neq 1,\ k\in M),$$

$$V(x,\ j)=ST^xST^jST^{-k(x,j)}S \qquad ((jx-1,\ N)=1,\ k(jx-1)\equiv -x \bmod N,\ k\notin M)$$

$$=ST^xST^jST^{-j'}ST^{-x'}S \quad ((jx-1)(j'x'-1)\equiv -xx' \bmod N).$$

Proposition 2. *Put*

$$G=\{T,\ U,\ V(k),\ V(x,\ j)|1\leqq k\leqq N-1,\ 1\leqq j\leqq n(x)-1,\ x\in M\}.$$

$\Gamma_0(N)$ is generated by the set $\boldsymbol{G}$.

(2) *Relations.* For $R=I$ and $R=S$, it is easy to see that new relations don't turn up from the first relation of (R).

For $R=ST^k(1\leqq k\leqq N-1)$,

$$\begin{aligned} RS^2R^{-1}&=ST^kS^2T^{-k}S \\ &=V(k)V(k_*) && ((k,\ N)=1) \\ &=V(k)V(x(k),\ j(k)) && ((k,\ N)\neq 1,\ k\notin M) \\ &=V(x,\ j)V(k(x,\ j)) && ((k,\ N)\neq 1,\ k=x\in M,\ (kj-1,\ N)=1) \\ &=V(x,\ j)V(x',\ j') && ((k,\ N)\neq 1,\ k=x\in M,\ (kj-1,\ N)\neq 1). \end{aligned}$$

For $R=ST^xST^j(0\leqq j\leqq n(x)-1)$,

$$\begin{aligned} RS^2R^{-1}&=ST^xST^jS^2T^{-j}ST^{-x}S \\ &=V(x,\ j)V(k(x,\ j)) && ((xj-1,\ N)=1) \\ &=V(x,\ j)V(x',\ j') && ((xj-1,\ N)\neq 1). \end{aligned}$$

Hence we obtain the following relations:

(R.1) $\quad V(k)V(k_*)=1 \qquad ((k,\ N)=1)$,

(R.2) $\quad V(k)V(x(k),\ j(k))=1 \qquad ((k,\ N)\neq 1,\ k\notin M)$,

(R.3) $\quad V(x,\ j)V(x',\ j')=1 \qquad ((xj-1,\ N)\neq 1)$.

On the second relation of (R), we obtain first relations $V(1)UT=1$ and $TV(1)U=1$ for $R=I$ and $R=S(R=ST)$ respectively, i.e.

(R.4) $\quad V(1)UT=1.$

For $R=ST^k$ $(2\leqq k\leqq N-1)$, if $(k,\ N)=1$ with $k_1=k_*+1$,

$$\begin{aligned} R(ST)^3R^{-1}&=ST^kSTSTST^{1-k}S \\ &=V(k)V(k_1)V(k_2) && ((k,\ N)=1,\ k_2=k_{1*}+1) \end{aligned}$$

$$=V(k)V(k_1, 1) \qquad (k_1\in M,\ k-1\notin M)$$

$$=V(k)V(k-1) \qquad (k\in M,\ k-1\in M)$$

$$=V(k)V(k_1)V(x(k_1), j(x)) \ ((k_1, N)\neq 1,\ k_1\notin M,\ k-1\notin M)$$

$$=V(k)V(k_1)V(k-1) \qquad ((k_1, N)\neq 1,\ k_1\notin M,\ k-1\in M);$$

if $(k, N)\neq 1$ and $k(=x)\in M$,

$$R(ST)^3R^{-1}=ST^xSTSTST^{1-x}S$$

$$=V(x, 1)V(k(x)+1) \qquad ((x-1, N)=1,\ x\neq k(x))$$

$$=V(x)V(x+1) \qquad ((x-1, N)=1,\ x\neq k(x))$$

$$=V(x, 1)V(x-1) \qquad ((x-1, N)\neq 1,\ x'=k-1)$$

$$=V(x, 1)V(x', j'+1) \qquad ((x-1, N)\neq 1,\ x'\neq k-1);$$

if $(k, N)\neq 1$ and $k\notin M$,

$$R(ST)^3R^{-1}=V(k)V(x(k), j(k)+1)V(k(x, j+1)+1)$$

$$((x(j+1)-1, N)=1,\ k(x, j+1)\notin M)$$

$$=V(k)V(x(k))V(x(k)+1)$$

$$((x(j+1)-1, N)=1,\ k(x, j+1)\in M)$$

$$=V(k)V(x(k), j(k)+1)V(x', (j+1)')$$

$$((x(j+1)-1, N)\neq 1,\ k-1\notin M)$$

$$=V(k)V(x(k), j(k)+1)V(k-1)$$

$$((x(j+1)-1, N)\neq 1,\ k-1\in M).$$

For $R=ST^xST^j(0\leqq j\leqq n(x)-1)$,

$$R(ST)^3R^{-1}=ST^{x+1}STSTST^{-x}S \qquad (j=0)$$

$$=V(x+1)V(x) \qquad ((x+1, N)=1,\ n(x)=1)$$

$$=V(x+1)V((x+1)_*+1)V(x) \quad ((x+1, N)=1,\ n(x)\neq 1)$$

$$= V(x+1, 1)V(x) \qquad (x+1 \in M)$$

$$= V(k)V(x(k), j(k)+1)V(x) \qquad (k = x+1, (k, N) \neq 1, k \notin M),$$

$$R(ST)^3R^{-1} = ST^xSTSTSTST^{1-x}S \qquad (j=1)$$

$$= V(x, 1)V(k(x)+1) \qquad ((x-1, N)=1)$$

$$= V(x, 1)V(x', j'+1) \qquad ((x-1, N) \neq 1, x \neq x'+1)$$

$$= V(x, 1)V(x-1) \qquad ((x-1, N)=1, x = x'+1),$$

$$R(ST)^3R^{-1} = ST^xST^jSTSTST^{1-j}ST^{-x}S \quad (2 \leqq j \leqq n(x)-1)$$

$$= V(x, j)V(k(x, j)+1, 1) \qquad ((xj-1, N)=1, k(x, j)+1 \in M)$$

$$= V(x, j)V(k)V(k_*+1, j-1) \qquad ((xj-1, N)=1, k = k(x, j)+1, (k, N)=1)$$

$$= V(x, j)V(k)V(x(k), j(k)+1) \qquad ((xj-1, N)=1, k = k(x, j)+1, (k, N) \neq 1)$$

$$= V(x, j)V(x', j'+1)V(x, j-1)^{-1} \qquad ((xj-1, N) \neq 1, n(x') \neq j'+1)$$

$$= V(x, j)V(x')V(x+1) \qquad ((xj-1, N)=1, n(x')=j'+1).$$

Proposition 3. *The following nine rebations (R.5−13) together with the dbove four relations (R.1−4) make up a system of fundamental relations of $\Gamma_0(N)$ for the system of generators* $\boldsymbol{G}$.

(R.5) $\quad V(k)V(k_1)V(k_2)=1 \qquad ((k, N)=1, (k_1, N)=1, k_1 = k_*+1, k_2 = k_{1*}+1),$

(R.6) $\quad V(k)V(k-1)=1 \qquad ((k, N)=1, k-1 \in M, k_*+1 \in M),$

(R.7) $\quad V(k)V(k_*+1, 1)=1 \qquad ((k, N)=1, k-1 \notin M, k_*+1 \in M),$

(R.8) $V(k)V(k_*+1)V(x(k_*+1), j(k_*+1))=1 \quad ((k, N)=1, (k_*+1, N) \neq 1, k_*+1 \notin M, k-1 \notin M)$,

(R.9) $V(k)V(k_*+1)V(k-1)=1 \quad ((k, N)=1, (k_*+1, N)\neq 1, k_*+1 \notin M, k-1 \in M)$,

(R.10) $V(x, 1)V(x-1)=1 \quad ((x-1, N)\neq 1, x-1 \in M)$,

(R.11) $V(x, 1)V(x', j'+1)=1 \quad ((x-1, N)\neq 1, x-1 \notin M)$,

(R.12) $V(k)V(x(k), j(k))V(x(k)', (j(k)+1)')=1$

$((k, N)\neq 1, k \notin M, k-1 \notin M)$,

(R.13) $V(k)V(x(k), j(k))V(k-1)=1 \quad ((k, N)\neq 1, k \notin M, k-1 \in M)$.

3. Eliminations. In this section, we shall eliminate unnecessary generators and relations.

Firstly, note that the number of the generators in $\boldsymbol{G}$ is given by the following:

$$|\boldsymbol{G}|=|\boldsymbol{R}|-|M|.$$

Because the elements of $\boldsymbol{G}$ are T, U, $V(x)$ $(1\leqq k\leqq N-1)$ and $V(x, j)$ $(1\leqq j\leqq n(x)-1)$, and the number of $V(x, j)$ is $\sum_{x\in M}(n(x)-1)=|\boldsymbol{R}|-N-1-|M|$.

Secondly, note that $k^2\equiv -1 \bmod N$ has solutions if and only if the following condition is satisfied:

(3.1) $N=2^{\nu(2)}N'$, $0\leqq \nu(2)\leqq 1$, $(N', 2)=1$ and $p\equiv 1 \bmod 4$ for any prime divisor p of N'.

Hence if N does not satisfy (3.1), we can eliminate $1/2|\boldsymbol{R}|-|M|-1$ generators from $\boldsymbol{G}$ by relations (R.1–3). Because the number of distinct generators appearing in (R.1–3) is $\sum_{x\in M}(n(x)-1)+N-1-|M|=|\boldsymbol{R}|-2|M|-2N-2$. If N satisfies (3.1), there are two k's satisfying $k^2\equiv -1 \bmod N$ and for these two k's, (R.1) has the form $V(k)^2=1$. Hence in this case, the number of generators eliminated by (R.1–3) is $1/2|\boldsymbol{R}|-|M|-2$.

Furthermore, note that $k(k-1)\equiv -1 \bmod N$ has solutions if and only if the following condition is satisfied:

(3.2) $N=3^{\nu(3)}N'$, $0\leqq\nu(3)\leqq 1$, $(N', 3)=1$ and $p\equiv 1 \bmod 3$ for any prime divisor p of N'.

Hence if N does not satisfy (3.2), we can eliminate $1/3|\boldsymbol{R}|$ ($=1/3$ (the number of the second relations in (R))) generators from $\boldsymbol{G}$ by relations (R.4-13). If N satisfies (3.2), (R.5) is $V(k)^3=1$ for two k's satisfying $k(k-1)\equiv -1 \bmod N'$, hence in this case, the number eliminated by (R.4-13) is $1/3(|\boldsymbol{R}|-2)$.

Now, we obtain the following proposition.

Proposition 4. *Let N be $N>3$ and $N=2^{\nu(2)}3^{\nu(3)}N'$ with $(N', 6)=1$. We shall distinguish the following four cases*: (1) $\nu(2)=\nu(3)=0$, *and* $p\equiv 1 \bmod 12$ *for any prime divisor p of N'*; (2) $0\leqq\nu(2)\leqq 1$, $\nu(3)=0$, $p\equiv 1 \bmod 4$ *for any prime divisor p of N' and* $q\not\equiv 1 \bmod 3$ *for some prime divisor q of N'*; (3) $\nu(2)=0$, $0\leqq\nu(3)\leqq 1$, $p\equiv 1 \bmod 3$ *for any divisor p of N' and* $q\not\equiv 1 \bmod 4$ *for some prime divisor q of N'*; (4) *the case other than* (1), (2) *and* (3).

Put

$$m(N)=\begin{cases} 1/6(16+|\boldsymbol{R}|) & (\textit{case}\ (1)) \\ 1/6(12+|\boldsymbol{R}|) & (\textit{case}\ (2)) \\ 1/6(10+|\boldsymbol{R}|) & (\textit{case}\ (3)) \\ 1/6(6+|\boldsymbol{R}|) & (\textit{case}\ (4)), \end{cases}$$

then $\Gamma_0(N)$ is generated by a subset $\boldsymbol{G}_0$ of cardinality $m(N)$ of $\boldsymbol{G}$. In case (1) *and* (2), *there are two defining relations of the form*

$$V(k_1)^2=1 \text{ and } V(k_2)^2=1$$

with $k_i\equiv -1 \bmod N$ $(i=1, 2)$. *In case* (1) *and* (3), *there are two defining relations of the form*

$$V(k_1)^3=1 \text{ and } V(k_2)^3=1$$

with $(2k_i-1)^2\equiv -3 \mod N$ $(i=1, 2)$. *There are no other relations among the generators* $\boldsymbol{G}_0$. *In paticular* $\boldsymbol{G}_0$ *is a minimal system of generators of* $\Gamma_0(N)$.

UNIVERSITY OF OSAKA PREFECTURE

References

[1] H. Frasch, Die Erzeugenden der Hauptkongruenzgruppen für primzahlstufen, Math. Ann. (**108**) 1932, 229–252.

[2] H. Rademacher, Uber die Erzeugenden von Kongruenzuntergruppen der Modulgruppe, Ham. Abh. (**7**) 1929, 134–148.

[3] O. Schreier, Die Untergruppen der freien Gruppen, Ham. Abh. (**5**) 1927, 161–183.