48. Classification of Normal Congruence Subgroups of $G(\sqrt{q})$. I

By Toshikazu TAKAGI
College of Arts and Sciences, Showa University

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1988)

1. Normal congruence subgroups of the modular group $SL_2(\boldsymbol{Z})$ was completely classified by McQuillan [1]. As a continuation, Parson [2] attempted the classification of normal congruence subgroups of the group $G(\sqrt{q})$ $(q=2, 3)$ and obtained partial results. The present author classified all normal congruence subgroups of the group $G(\sqrt{q})$ for any prime q ([3]). In this note, the main results of [3] are reported.

2. In the following, we denote by $(a, b; c, d)$ a 2×2 matrix such that the first (resp. second) row is $(a\ b)$ (resp. $(c\ d)$). For a rational prime q, the group $G(\sqrt{q})\,(=\Gamma)$ is defined by $G(\sqrt{q})=W^{-1}N(\Gamma_0(q))W$, where $W=(1, 0; 0, \sqrt{q})$ and $N(\Gamma_0(q))$ is the normalizer of $\Gamma_0(q)$ in $SL_2(\boldsymbol{R})$. The group $\Gamma^e=W^{-1}\Gamma_0(q)W$ is a normal subgroup of Γ with index 2, and $\Gamma=\Gamma^e\cup S\Gamma^e$ where $S=(0, -1; 1, 0)$. We call elements of Γ^e (resp. $S\Gamma^e$) *even* (resp. *odd*). Also a subgroup G is called *even* or *odd* according as $G\subset\Gamma^e$ or $G\not\subset\Gamma^e$. Let R and $\mathfrak{n}$ denote the ring of integers of the quadratic field $\boldsymbol{Q}(\sqrt{q})$ and a non-zero ideal of R respectively. Since Γ is a subgroup of $SL_2(R)$, the principal congruence subgroup $\Gamma(\mathfrak{n})$ of Γ can be defined as usual. Set $\boldsymbol{L}=\boldsymbol{N}\cup\boldsymbol{N}q^{1/2}$. A subgroup G of Γ is called a *congruence subgroup* if G contains $\Gamma^e(L)$ $(=\Gamma(L)\cap\Gamma^e)$ for some $L\in\boldsymbol{L}$, and the *level* of G is defined to be the smallest element L with such a property. We shall classify in § 3–4 (resp. 5) even (resp. odd) normal congruence subgroups.

3. For each $L\in\boldsymbol{L}$, set $H_q(L)=\Gamma^e/\Gamma^e(L)$. For a subgroup N of $H_q(L)$, the *level* of N can be defined similarly as in case of a subgroup of Γ. Denote by σ the automorphism of Γ^e defined by $X\mapsto S^{-1}XS$. σ induces an automorphism of $H_q(L)$, which is also denoted by σ. Then in order to classify all even normal congruence subgroups, it is sufficient to classify all normal σ-subgroups of $H_q(L)$ which are of level L.

Here we treat the case where L is a power of a prime. Suppose now that $L=q^s$ with $q\neq 2$, where $s=m$ or $m-1/2$ $(m\in\boldsymbol{N})$. Since $H_q(q^{1/2})$ is a cyclic group of order $q-1$, there exists a unique subgroup of $H_q(q^{1/2})$ of index ν for each divisor ν of $q-1$ $(\nu\neq 1)$. It is denoted by $T^{(q)}_{(\nu)}$. Let B_{m-1} and C_{m-1} be two elements of $H_q(q^m)$ defined by $B_{m-1}=(1, \overline{q^{m-1}\sqrt{q}}; 0, 1)$ and $C_{m-1}=(1, 0; \overline{q^{m-1}\sqrt{q}})$ where $^{-}$ indicates residue class mod L. When $q=3$ or 5, we denote by $R^{(q)}_m$ (resp. $S^{(q)}_m$) the cyclic group of order q generated by $B_{m-1}C^{-1}_{m-1}$ (resp. $B_{m-1}C_{m-1}$).

Theorem 1. *When $L=q^s$ $(q\neq 2,\ s=m,\ m-1/2\ (m\in\boldsymbol{N}))$, all normal σ-*

subgroups N of level L of $H_q(L)$ are the following:

(1) $L=q^{1/2}$: $N=T^{(q)}_{(\nu)}$ $(\nu|(q-1), \nu\neq 1)$.

(2) $L=q^{m-1/2}$ $(m\geqq 2)$ *or* q^m $(q\neq 3, 5, m\geqq 1)$: $N=1, \pm I$.

(3) $L=q^m(q=3, 5, m\geqq 1)$: $N=1, \pm I, R^{(q)}_m, \pm R^{(q)}_m, S^{(q)}_m, \pm S^{(q)}_m$.

Suppose now $L=2^s$, where $q=2$ and $s=m$ or $m-1/2$ $(m\in N)$. When $s=m-1/2$, $K_{m-1/2}$ denotes the group of order 2 generated by $-(1+2^{m-1})I$ $(m\geqq 3)$. When $s=m$, there exist many normal σ-subgroups. Set $d_0=5$ $(\mathrm{mod}\ 2^m)\in(Z/2^mZ)^\times$. Let B_k, C_k and D_k be elements of $H_2(2^m)$ defined by $B_k=(1, 2^k\sqrt{2}\,; 0, 1)$, $C_k=(1, 0\,; 2^k\sqrt{2}, 1)$, $D_k=(d_0^{-t}, 0\,; 0, d_0^t)$ $(t=2^k)$, where $k=0, 1, \cdots, m$. Set $B=B_0$, $C=C_0$, $D=D_0$. If $t=2^{m-3}$ $(m\geqq 3)$, then $d_0^t=d_0^{-t}=1+2^{m-1}$ $(\mathrm{mod}\ 2^m)$, hence $D_{m-3}=(1+2^{m-1})I$. If $t=2^{m-4}$ $(m\geqq 5)$, then $d_0^t=1+2^{m-2}+2^{m-1}$ $(\mathrm{mod}\ 2^m)$ and $d_0^{-t}=1+2^{m-2}$ $(\mathrm{mod}\ 2^m)$.

Now let us define some σ-invariant normal subgroups of $H_2(2^m)$ which are of level 2^m. (i) $m=1$: $E_1=\langle BC\rangle$. (ii) $m=2$: $E_2^+=\langle B_1C_1\rangle$, $E_2^-=\langle -B_1C_1\rangle$, $K_2=\langle -B_1, C_1\rangle$, $R_2=\langle BC^{-1}\rangle E_2^+$, $S_2=\langle BC\rangle E_2^+$. (iii) $m\geqq 3$: $E_m^+=\langle E\rangle$, $E_m^-=\langle -E\rangle(E=B_{m-1}C_{m-1})$, $F_m^+=\langle D_{m-3}\rangle$, $F_m^-=\langle -D_{m-3}\rangle$, $G_m^+=\langle G\rangle$, $G_m^-=\langle -G\rangle(G=B_{m-1}C_{m-1}D_{m-3})$, $H_m^+=\langle C_{m-1}D_{m-3}\rangle E_m^+$, $H_m^-=\langle -C_{m-1}D_{m-3}\rangle E_m^+$, $I_m=\langle -B_{m-1}, -C_{m-1}\rangle$, $J_m^{++}=E_m^+F_m^+$, $J_m^{+-}=E_m^+F_m^-$, $J_m^{-+}=E_m^-F_m^+$, $J_m^{--}=E_m^-F_m^-$, $K_m^+=I_mF_m^+$, $K_m^-=I_mF_m^-$, $L_m^+=\langle L\rangle H_m^+$, $L_m^-=\langle -L\rangle H_m^+(L=B_{m-2}C_{m-2}^{-1})$, $M_m^+=\langle M\rangle H_m^+$, $M_m^-=\langle -M\rangle H_m^+(M=B_{m-2}C_{m-2})$, $E_{m-1}^{m+}=M_m^+F_m^-$, $E_{m-1}^{m-}=M_m^-F_m^-$. (iv) $m=3$: $P_3=\langle BC^{-1}\rangle L_3^+$, $Q_3=\langle BC^{-1}D\rangle L_3^+$, $S_3^+=\langle BC\rangle E_2^{3+}$, $S_3^-=\langle -BC\rangle E_2^{3+}$. (v) $m\geqq 4$: $N_m^+=\langle N\rangle F_m^+$, $N_m^-=\langle -N\rangle F_m^+(N=B_{m-2}C_{m-2}D_{m-4})$, $O_m^+=\langle O\rangle F_m^+$, $O_m^-=\langle -O\rangle F_m^+(O=B_{m-2}C_{m-2}^{-1}\cdot D_{m-4})$, $G_{m-1}^{m+}=N_m^+I_m$, $G_{m-1}^{m-}=N_mI_m$.

P_3 and Q_3 are not abelian and contain L_3^+ with index 4. S_3^+ and S_3^- are not abelian and contain E_2^{3+} with index 2. The other groups are all abelian.

Theorem 2. *When $L=2^s$ $(q=2, s=m$ or $m-1/2$ $(m\in N))$, all normal σ-subgroups N of level L of $H_2(L)$ are the following*:

(1) $L=2^{1/2}$: *N does not exist.*

(2) $L=2^{3/2}$: $N=1$.

(3) $L=2^{m-1/2}$ $(m\geqq 3)$: $N=1, \pm I, K_{m-1/2}$.

(4) $L=2$: $N=1, E_1$.

(5) $L=2^2$: $N=1, \pm I, E_2^+, E_2^-, \pm E_2^+, K_2, R_2, S_2$.

(6) $L=2^m$ $(m\geqq 3)$: $N=1, \pm I, E_m^+, E_m^-, \pm E_m^+, F_m^+, F_m^-, \pm F_m^+, G_m^+, G_m^-, \pm G_m^+, H_m^+, H_m^-, \pm H_m^+, I_m, J_m^{++}, J_m^{+-}, J_m^{-+}, J_m^{--}, \pm J_m^{++}, K_m^+, K_m^-, L_m^+, L_m^-, \pm L_m^+, M_m^+, M_m^-, \pm M_m^+, E_{m-1}^{m+}, E_{m-1}^{m-}$ *and further, if $m=3$, then P_3, Q_3, S_3^+, S_3^-, or if $m\geqq 4$, then* $N_m^+, N_m^-, \pm N_m^+, O_m^+, O_m^-, \pm O_m^+, G_{m-1}^{m+}, G_{m-1}^{m-}$.

Suppose now $L=p^m$ $(m\in N)$, where p is a prime $\neq q$. Then $H_q(L)$ is isomorphic to $SL_2(Z/LZ)$ by the morphism $\phi: (a, b\sqrt{q}\,; c\sqrt{q}, d)\mapsto(a, b\,; cq, d)$ $(\mathrm{mod}\ L)$. All normal subgroups N of level L of $SL_2(Z/LZ)$ are known ([1]). Since it seems that there are some errors in the Proposition 1 in § 3 of [1], we give here all N explicitly. Let M denote the unique normal subgroup of $SL_2(Z/3Z)$ with index 3. When $L=2^m$, let $P=(0, -1\,; 1, -1)$, $B_{m-1}=(1, 2^{m-1}\,; 0, 1)$, $C_{m-1}=(1, 0\,; 2^{m-1}, 1)$, $D_k=(d_0^{-t}, 0\,; 0, d_0^t)$ $(t=2^k)$ be elements of $SL_2(Z/2^m Z)$. Now let us define some normal subgroups of level 2^m. (i) $m=1$: $Q_1=\langle P\rangle$. (ii) $m\geqq 2$: $E_m=\langle B_{m-1}C_{m-1}, C_{m-1}D_{m-3}\rangle$. (iii) $m=2$: $Q_2=\langle P\rangle E_2$. (iv) $m\geqq 3$: $F_m^+=\langle D_{m-3}\rangle$, $F_m^-=\langle -D_{m-3}\rangle$, $K_m=E_m F_m^-$. (v) $m\geqq 4$: $G_m^+=\langle X\rangle$, $G_m^-=\langle -X\rangle$ $(X=B_{m-1}C_{m-1}D_{m-4})$. We use the same notations for the corresponding subgroups of $H_q(L)$.

Theorem 3. *When $L=p^m$ $(m\in N)$ with p a prime $\neq q$, all normal σ-subgroups N of level L of $H_q(L)$ are the following*:

(1) $L=p^m$ $(p\neq 2, 3)$: $N=1, \pm I$.

(2) $L=3^m$ $(p=3)$: $N=1, \pm I, M$ $(m=1)$.

(3) $L=2$ $(p=2, m=1)$: $N=1, Q_1$.

(4) $L=2^2$ $(p=2, m=2)$: $N=1, \pm I, E_2, Q_2$.

(5) $L=2^m$ $(p=2, m\geqq 3)$: $N=1, \pm I, E_m, \pm E_m, F_m^+, F_m^-, \pm F_m^+, K_m$ *and further, if* $m\geqq 4$, *then* $G_m^+, G_m^-, \pm G_m^+$.

Remark. Our notations are different from those of [1]. The following table indicates the correspondence.

Table

our notations	M	Q_1	E_m	F_m^+	F_m^-	G_m^+	G_m^-
those of [1]	M	Q	E_m	C_m	H_m	D_m	F_m

In the Proposition 1 in §3 of [1], two groups Q_2 and K_m must be added, and the group $\pm E_2$ must be omitted, because $\pm E_2$ is of level 2 but not of level 2^2. Also in the Main theorem of [1], the group Q_2 must be added.

(to be continued.)

References

[1] D. L. McQuillan: Classification of normal congruence subgroups of the modular group. Amer. J. Math., **87**, 285–296 (1967).

[2] L. A. Parson: Normal congruence subgroups of the Hecke groups $G(2^{(1/2)})$ and $G(3^{(1/2)})$. Pacific J. Math., **70**, no. 2, 481–487 (1977).

[3] T. Takagi: Classification of normal congruence subgroups of $G(\sqrt{q})$ which is a conjugate of the normalizer of $\Gamma_0(q)$ (q: a prime). J. Coll. Arts and Sci., Showa Univ., vol. 18, pp. 63–99 (1987).