PACIFIC JOURNAL OF MATHEMATICS
Vol. 70, No. 2, 1977

NORMAL CONGRUENCE SUBGROUPS OF THE HECKE GROUPS $G(2^{(1/2)})$ AND $G(3^{(1/2)})$

L. ALAYNE PARSON

Normal congruence subgroups of the classical modular group have been completely classified by M. Newman and D. McQuillan. In this note we begin the classification of normal congruence subgroups of the Hecke groups $G(2^{(1/2)})$ and $G(3^{(1/2)})$.

-Our main result is that if G is a normal congruence subgroup of $G(m^{(1/2)})$, $m = 2, 3$, containing the principal congruence subgroup $\bar{\Gamma}_m(nm^{(1/2)})$ where $(n, 6) = 1$ and if G contains only even elements, then G is $\Gamma_m(dm^{(1/2)})$, $\bar{\Gamma}_m(dm^{(1/2)})$ where $d \mid n$ or $\Gamma_m(d)$, $\bar{\Gamma}_m(d)$ where $d \mid n$ and $d > 1$. To obtain this result we use facts about the level of a congruence subgroup which are of independent interest.

2. Definitions. The set of 2×2 matrices with integer entries and determinant one is the classical modular group which is denoted by $\Gamma(1)$. The principal congruence subgroups of level n are

$$\bar{\Gamma}(n) = \left\{ \begin{pmatrix} ab \\ cd \end{pmatrix} : a \equiv d \equiv +1 \pmod n, b \equiv c \equiv 0 \pmod n \right\}$$

and

$$\Gamma(n) = \left\{ \begin{pmatrix} ab \\ cd \end{pmatrix} : a \equiv d \equiv \pm 1 \pmod n, b \equiv c \equiv 0 \pmod n \right\}.$$

The modular group and its subgroups have been studied extensively. In particular, M. Newman **[5]** and D. McQuillan **[4]** have shown that if $\bar{\Gamma}(n) \subset G \subset \Gamma(1)$, $(n, 6) = 1$, then $G = \bar{\Gamma}(d)$ or $\Gamma(d)$ where $d \mid n$. The only additional result that we need is

$$\bar{\Gamma}(n)\bar{\Gamma}(k) = \Gamma(1), \qquad (n, k) = 1, \tag{2.1}$$

which was proved by M. Newman and J. R. Smart in **[6]**.

In **[1]** E. Hecke introduced an infinite class of discrete groups $\hat{G}(\lambda_q)$ of linear fractional transformations preserving the upper half plane. $\hat{G}(\lambda_q)$ is the group generated by $Sz = z + \lambda_q$ and $Tz = -1|z$ where $\lambda_q = 2\cos(\pi|q)$, q an integer, $q \geqq 3$. We are interested in the corresponding matrix groups. When $q = 3$, we have the modular group. When $q=4$ or 6, the resulting groups are $G(2^{(1/2)})$ and $G(3^{(1/2)})$. These two groups are of particular interest since they are the only Hecke groups, aside from the modular group, whose elements are completely known. They are also the only Hecke groups which are commensurable with the modular group.

It is well known ([2], [9]) that $G(m^{(1/2)})$, $m=2,3$, consists of the set of all matrices of the following two types:

$$\text{(i)} \qquad \begin{pmatrix} a & bm^{(1/2)} \\ cm^{(1/2)} & d \end{pmatrix}, a, b, c, d \in \mathbf{Z},\ ad - mbc = 1,$$

and

$$\text{(ii)} \qquad \begin{pmatrix} am^{(1/2)} & b \\ c & dm^{(1/2)} \end{pmatrix}, a, b, c, d \in \mathbf{Z},\ mad - bc = 1.$$

Those of type (i) are called even whereas those of type (ii) are called odd. The principal congruence subgroups of $G(m^{(1/2)})$ are defined by

$$\bar{\Gamma}_m(\mu) = \{M \in G(m^{(1/2)}) \colon M \equiv I \pmod{\mu}\},$$
$$\Gamma_m(\mu) = \{M \in G(m^{(1/2)}) \colon M \equiv \pm I \pmod{\mu}\},$$

where $\mu = N + Rm^{(1/2)}$ is a non-zero element of $\mathbf{Z}[m^{(1/2)}]$ and the congruence is elementwise in $\mathbf{Z}[m^{(1/2)}]$. In [7] it is shown that the proper principal congruence subgroups reduce to three basic types: $\mu = N$, $\mu = Nm^{(1/2)}$, $N \geqq 1$, and $\mu = N + Rm^{(1/2)}$, $(N, Rm) = 1$. In this last case, the principal congruence subgroups always contain odd elements whereas when $\mu = N$ or $Nm^{(1/2)}$, they contain only even elements. In particular,

$$\text{(2.2)} \quad \bar{\Gamma}_m(N) = \left\{ \begin{pmatrix} a & bm^{(1/2)} \\ cm^{(1/2)} & d \end{pmatrix} : \begin{matrix} a \equiv d \equiv 1 \pmod{N} \\ b \equiv c \equiv 0 \pmod{N} \end{matrix} \right\} \quad \text{if} \quad N \geqq 2$$

and

$$\text{(2.3)} \quad \bar{\Gamma}_m(Nm^{(1/2)}) = \left\{ \begin{pmatrix} a & bm^{(1/2)} \\ cm^{(1/2)} & d \end{pmatrix} : \begin{matrix} a \equiv d \equiv 1 \pmod{Nm}, \\ b \equiv c \equiv 0 \pmod{N} \end{matrix} \right\} \quad \text{if} \quad N \geqq 1.$$

Here the congruences are in $\mathbf{Z}$, rather than $\mathbf{Z}[m^{1/2}]$.

The index formulas are [7]:

$$|G(m^{(1/2)}) \colon \Gamma_m(m^{(1/2)})| = 2;$$

for $N \geqq 1$,

$$|G(m^{(1/2)}): \bar{\Gamma}_m(Nm^{(1/2)})| = 2(m-1)N^3 \prod_{p|N, p\neq m} (1-1/p^2);$$

for $N \geqq 2$,

$$|G(m^{(1/2)}): \bar{\Gamma}_m(N)| = \begin{cases} 2N^3 \prod_{p|N} (1-1/p^2) & \text{if } (N,m)=1, \\ 2(1-1/m)N^3 \prod_{p|N, p\neq m} (1-1/p^2) & \text{if } (N,m)=m. \end{cases}$$

Here p is a prime. We also note that $\Gamma_m(m^{(1/2)})$ is the group of even elements in $G(m^{(1/2)})$. Finally, a subgroup Γ of $G(m^{(1/2)})$ is called a congruence subgroup if Γ contains a principal congruence subgroup.

3. The level of a congruence subgroup.

In [8] K. Wohlfahrt proved that two definitions of the level of a congruence subgroup of the modular group were equivalent. In this section we prove that the corresponding definitions for the Hecke groups are equivalent. This result is extremely useful in producing examples of noncongruence subgroups. However, we use it in the proof of Theorem 4.2 to conclude that if a normal congruence subgroup contains $S^n = \begin{pmatrix} 1 & nm^{(1/2)} \\ 0 & 1 \end{pmatrix}$, then $\bar{\Gamma}_m(nm^{(1/2)}) \subset G$.

DEFINITION 3.1. The level of a congruence subgroup Γ is the smallest positive integer N such that $\bar{\Gamma}_m(Nm^{(1/2)}) \subset \Gamma$. Such an integer does exist since if $\Gamma \supset \bar{\Gamma}_m(\mu)$ with $\mu = N + Rm^{1/2}$, then $\Gamma \supset \bar{\Gamma}_m(Lm^{1/2})$ where $L = |N^2 - R^2 m|/(N, Rm)$.

DEFINITION 3.2. Let Γ be an arbitrary subgroup of finite index in $G(m^{(1/2)})$. For each M in $G(m^{(1/2)})$ let $\lambda = \lambda(M)$ be the smallest positive integer such that $M^{-1}S^{\lambda}M \in \Gamma$. Then the general level of Γ is defined to be the least common multiple of all the integers $\lambda(M)$, $M \in G(m^{(1/2)})$. Such an integer does exist because Γ has only a finite number of conjugate subgroups in $G(m^{(1/2)})$.

LEMMA 3.1. *Let L be a positive integer. Then $\Delta(S^N)\bar{\Gamma}_m(LNm) = \bar{\Gamma}_m(Nm^{(1/2)})$ where $\Delta(S^N)$ is the smallest normal subgroup of $G(m^{(1/2)})$ containing S^N.*

Proof. Since it is clear that $\Delta(S^N)\bar{\Gamma}_m(LNm) \subset \bar{\Gamma}_m(Nm^{(1/2)})$, it suffices to show that $\bar{\Gamma}_m(Nm^{(1/2)}) \subset \Delta(S^N)\bar{\Gamma}_m(LNm)$.
We first note that

$$(3.1) \qquad S^{Nx} = \begin{pmatrix} 1 & Nxm^{(1/2)} \\ 0 & 1 \end{pmatrix}, \qquad W^{Ny} = \begin{pmatrix} 1 & 0 \\ Nym^{(1/2)} & 1 \end{pmatrix},$$

and

$$V(z) = W^z S^{-N} W^{-z} = \begin{pmatrix} 1 + zNm & -Nm^{(1/2)} \\ z^2 Nm^{3/2} & 1 - zMn \end{pmatrix}$$

are all elements of $\Delta(S^N)$ for any integral value of x, y, and z. Now let $M = \begin{pmatrix} 1 + Nma & * \\ Ncm^{(1/2)} & * \end{pmatrix}$ be an element of $\bar{\Gamma}_m(Nm^{(1/2)})$. Since $(1 + Nma, N^2cm) = 1$, an integer x may be determined so that $(1 + Nma + N^2cxm, L) = 1$. For this x set

$$M_1 = S^{Nx}M = \begin{pmatrix} 1 + Nma + N^2cxm & * \\ Ncm^{(1/2)} & * \end{pmatrix} = \begin{pmatrix} 1 + Nma_1 & * \\ Ncm^{(1/2)} & * \end{pmatrix}.$$

Now consider

$$M_2 = V(z)M_1 = \begin{pmatrix} (1 + Nma_1)(1 + zNm) - N^2mc & * \\ * & * \end{pmatrix}.$$

Since $(1 + Nma_1, L) = 1$, we may choose z so that

$$z(1 + Nma_1) \equiv Nc - a_1 \pmod{L}$$

which is equivalent to

$$(1 + Nma_1)(1 + zNm) - N^2mc \equiv 1 \pmod{LNm}.$$

For this z

$$\begin{aligned} M_2 &\equiv \begin{pmatrix} 1 & Nb_2m^{(1/2)} \\ Nc_2m^{(1/2)} & 1 + b_2c_2N^2m \end{pmatrix} \pmod{LNm} \\ &= W^{c_2N} S^{b_2N} \pmod{LNm}. \end{aligned}$$

Therefore, $M \equiv S^{-Nx} V(z)^{-1} W^{c_2N} S^{b_2N} \pmod{LNm}$; and $M \in \Delta(S^N)\bar{\Gamma}_m(LNm)$ by (3.1). Since M was arbitrary, the proof of the lemma is complete.

THEOREM 3.1. *If Γ is a congruence subgroup of general level N, then* $\bar{\Gamma}_m(Nm^{(1/2)}) \subset \Gamma$. *In addition, if L is the level of Γ given by Definition* 3.1, $L = N$.

Proof. Since $\bar{\Gamma}_m(Lm^{(1/2)})$ and $\Delta(S^N)$ are contained in Γ, $\Delta(S^N)\bar{\Gamma}_m(LNm) = \bar{\Gamma}_m(Nm^{(1/2)}) \subset \Gamma$. It then follows that $L \leqq N$. However, it is clear from Definitions 3.1 and 3.2 that $L \geqq N$.

4. Classification Theorems for normal congruence subgroups.

We are now in a position to prove the main results of this note.

THEOREM 4.1. *Let n be an integer,* $(n, 6) = 1$. *Suppose G is a normal congruence subgroup of* $G(m^{(1/2)})$ *with* $\bar{\Gamma}_m(n) \subset G \subset \Gamma_m(m^{(1/2)})$. *Then* $G = \Gamma_m(m^{(1/2)})$, $\Gamma_m(d)$, *or* $\bar{\Gamma}_m(d)$ *where* $d \mid n$, $d > 1$.

Proof. Let φ be the isomorphism from $\Gamma_m(m^{(1/2)})$ onto the modular subgroup $\Gamma_0(m) = \left\{\begin{pmatrix} ab \\ cd \end{pmatrix} \in \Gamma(1) : c \equiv 0 \pmod{m}\right\}$ defined by

$$\varphi\left(\begin{pmatrix} a & bm^{(1/2)} \\ cm^{(1/2)} & d \end{pmatrix}\right) = \begin{pmatrix} a & b \\ cm & d \end{pmatrix}.$$

Then

$$\Gamma_m(m^{(1/2)})/\bar{\Gamma}_m(n) \cong \Gamma_0(m)/(\bar{\Gamma}(n) \cap \Gamma_0(m)).$$

However, $\Gamma_0(m)/(\bar{\Gamma}(n) \cap \Gamma_0(m)) \cong \Gamma_0(m)\bar{\Gamma}(n)/\bar{\Gamma}(n) = \Gamma(1)/\bar{\Gamma}(n)$ since $\Gamma_0(m)\bar{\Gamma}(n) \supset \bar{\Gamma}(m)\bar{\Gamma}(n) = \Gamma(1)$ by (2.1). As noted earlier, for $(n, 6) = 1$ the only normal subgroups of $\Gamma(1)$ containing $\bar{\Gamma}(n)$ are $\bar{\Gamma}(d)$, $\Gamma(d)$, $d \mid n$, $d > 1$, and $\Gamma(1)$. These correspond to $\bar{\Gamma}_m(d)$, $\Gamma_m(d)$, $d \mid n$, $d > 1$, and $\Gamma_m(m^{(1/2)})$ and are then the only normal subgroups of $\Gamma_m(m^{(1/2)})$ containing $\bar{\Gamma}_m(n)$. Since they are all also normal in $G(m^{(1/2)})$, the proof of the theorem is complete.

The following theorem shows that the only normal congruence subgroups of level n, $(n, 6) = 1$, which contain only even elements are the principal congruence subgroups.

THEOREM 4.2. *Let G be a normal subgroup of* $G(m^{(1/2)})$ *with*

$$\bar{\Gamma}_m(nm^{(1/2)}) \subset G \subset \Gamma_m(m^{(1/2)}) \tag{4.1}$$

where $(n, 6) = 1$. *Then* $G = \Gamma_m(m^{(1/2)})$, $\bar{\Gamma}_m(m^{(1/2)})$, $\Gamma_m(d)$, $\bar{\Gamma}_m(d)$, $\Gamma_m(dm^{(1/2)})$, *or* $\bar{\Gamma}_m(dm^{(1/2)})$ *where* $d \mid n$, $d > 1$.

Proof. We first note that if n is odd, $\bar{\Gamma}_2(n2^{(1/2)}) = \bar{\Gamma}_2(n)$ and $\Gamma_2(n2^{(1/2)}) = \Gamma_2(n)$. This follows from (2.2) and (2.3). Thus, it suffices to take $m = 3$. Intersecting and producing in (4.1) with $\bar{\Gamma}_3(n)$ we have

$$\bar{\Gamma}_3(n3^{(1/2)}) \subset G \cap \bar{\Gamma}_3(n) \subset \bar{\Gamma}_3(n)$$
$$\bar{\Gamma}_3(n) \subset G\bar{\Gamma}_3(n) \subset \Gamma_3(3^{(1/2)}).$$

Since $|\bar{\Gamma}_3(n): \bar{\Gamma}_3(n3^{(1/2)})| = 2$, $G \cap \bar{\Gamma}_3(n) = \bar{\Gamma}_3(n)$ or $\bar{\Gamma}_3(n3^{(1/2)})$. If $G \cap \bar{\Gamma}_3(n) = \bar{\Gamma}_3(n)$, $\bar{\Gamma}_3(n) \subset G$; and $G = \Gamma_3(d)$, $\bar{\Gamma}_3(d)$, $d \mid n$, $d > 1$, or $\Gamma_3(3^{(1/2)})$ by Theorem 4.1. We now assume that $G \cap \bar{\Gamma}_3(n) = \bar{\Gamma}_3(n3^{(1/2)})$. Then

$$G\bar{\Gamma}_3(n)/G \cong \bar{\Gamma}_3(n)/\bar{\Gamma}_3(n3^{(1/2)});$$

and $|G\bar{\Gamma}_3(n)/G| = 2$.

Also by Theorem 4.1, $G\bar{\Gamma}_3(n) = \Gamma_3(3^{(1/2)})$, $\Gamma_3(d)$, or $\bar{\Gamma}_3(d)$, $d \mid n$, $d > 1$. If $G\bar{\Gamma}_3(n) = \Gamma_3(3^{(1/2)})$, $S^2 \in G$ since $S \in \Gamma_3(3^{(1/2)})$ and $|G\bar{\Gamma}_3(n)/G| = 2$. However, $S^n \in G$; and since $(2, n) = 1$, $S \in G$. Then $\bar{\Gamma}_3(3^{(1/2)}) \subset G$ by Theorem 3.1; and $G = \bar{\Gamma}_3(3^{(1/2)})$. Next, if $G\bar{\Gamma}_3(n) = \bar{\Gamma}_3(d)$, $S^{2d} \in G$; and since $(2d, n) = d$, $S^d \in G$. It then follows from Lemma 3.1 that $\bar{\Gamma}_3(d3^{(1/2)}) \subset G$; and $G = \bar{\Gamma}_3(d3^{(1/2)})$ since $|\bar{\Gamma}_3(d): \bar{\Gamma}_3(d3^{(1/2)})| = 2$. Finally, if $G\bar{\Gamma}_3(n) = \Gamma_3(d)$, a similar argument shows that $G = \Gamma_3(d3^{(1/2)})$.

The restriction on n in the preceding theorem is indeed necessary as is shown by the following theorem on the commutator subgroup of $G(m^{(1/2)})$.

THEOREM 4.3. *$G(2^{(1/2)})'$, the commutator subgroup of $G(2^{(1/2)})$, is of level 8 but is not a principal congruence subgroup. $G(3^{(1/2)})'$ is of level 6 but is not a principal congruence subgroup.*

Proof. In [3] M. Knopp determined all characters on $G(m^{(1/2)})$. When $m = 2$, the characters form an abelian group of order eight. It is easily verified that they are all one on $\bar{\Gamma}_2(8)$. Thus $G(2^{(1/2)})' \supset \bar{\Gamma}_2(8)$. Since not all characters are one on S^n for any $n < 8$, $\bar{\Gamma}_2(8)$ is the largest principal congruence subgroup contained in $G(2^{(1/2)})'$. When $m = 3$, the characters form an abelian group of order 12. In this case $\bar{\Gamma}_2(6)$ is the largest principal congruence subgroup on which all characters are identically one. To see that $G(m^{(1/2)})'$ is not a principal congruence subgroup we note that $STS^{-1}T^{-1} = \begin{pmatrix} m+1 & m^{(1/2)} \\ m^{(1/2)} & 1 \end{pmatrix}$

is an element of $G(m^{(1/2)})'$ but is certainly not an element of $\bar{\Gamma}_2(8)$ when $m = 2$ or $\bar{\Gamma}_3(6)$ when $m = 3$.

5. Conclusion. It is clear that there is still much to be done in order to complete the classification of normal congruence subgroups. If $(n, 6) > 1$, there are certainly non-principal normal congruence subgroups of level n containing only even elements. If G is a normal congruence subgroup containing odd elements, additional problems arise. Theorem 4.2 may be used to determine the group of even elements in G. However, G need not be a principal congruence subgroup. For example, let G be the normal closure in $G(m^{(1/2)})$ of $\{\Gamma_m(p), T\}$ where p is a prime chosen so that no element in $\mathbf{Z}[m^{(1/2)}]$ has norm $\pm p$. Then G is of level p; and the group of even elements in G is $\Gamma_m(p)$. G is not a principal congruence subgroup since the group of even elements in $\Gamma_m(N + Rm^{(1/2)})$, $(N, Rm) = 1$, is $\Gamma_m(|N^2 - R^2m|)$.

References

1. E. Hecke, *Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung*, Math. Ann., **112** (1936), 664–699.

2. J. I. Hutchinson, *On a class of automorphic functions*, Trans. Amer. Math. Soc., **3** (1902), 1–11.

3. M. I. Knopp, *Determination of certain roots of unity in the theory of automorphic forms of dimension zero*, Duke Math. J., **27** (1960), 497–506.

4. D. L. McQuillan, *Classification of normal congruence subgroups of the modular group*, Amer. J. Math., **87** (1965), 285–296.

5. M. Newman, *Normal congruence subgroups of the modular group*, Amer. J. Math., **85** (1963), 419–427.

6. M. F. Newman and J. R. Smart, *Modulary groups of $t \times t$ matrices*, Duke Math. J., **30** (1963), 253–257.

7. L. A. Parson, *Generalized Kloosterman sums and the Fourier coefficients of cusp forms*, Trans. Amer. Math. Soc., **217** (1976), 329–350.

8. K. Wohlfahrt, *An extension of F. Klein's level concept*, Illinois J. Math., **8** (1964), 529–535.

9. J. Young, *On the group belonging to the sign* $(0, 3; 2, 4, \infty)$ *and the functions belonging to it*, Trans. Amer. Math. Soc., **5** (1904), 81–104.

Received December 22, 1976 and in revised form April 28, 1977.

THE OHIO STATE UNIVERSITY
COLUMBUS, OH 43210