# LATTICE SUBGROUPS OF FREE CONGRUENCE GROUPS

*by* A. W. MASON

(Received 16 February, 1968)

**1. Introduction.** Let $\Gamma(1)$ denote the homogeneous modular group of $2 \times 2$ matrices with integral entries and determinant 1. Let $\hat{\Gamma}(1)$ be the inhomogeneous modular group of $2 \times 2$ integral matrices of determinant 1 in which a matrix is identified with its negative. $\hat{\Gamma}(N)$, the principal congruence subgroup of level $N$, is the subgroup of $\hat{\Gamma}(1)$ consisting of all $T \in \hat{\Gamma}(1)$ for which $T \equiv \pm I \pmod{N}$, where $N$ is a positive integer and $I$ is the identity matrix. A subgroup $\mathscr{G}$ of $\hat{\Gamma}(1)$ is said to be a congruence group of level $N$ if $\mathscr{G}$ contains $\hat{\Gamma}(N)$ and $N$ is the least such integer. Similarly, we denote by $\Gamma(N)$ the principal congruence subgroup of level $N$ of $\Gamma(1)$, consisting of those $T \in \Gamma(1)$ for which $T \equiv I \pmod{N}$, and we say that a subgroup $\mathscr{G}$ of $\Gamma(1)$ is a congruence group of level $N$ if $\mathscr{G}$ contains $\Gamma(N)$ and $N$ is minimal with respect to this property. In a recent paper [9] Rankin considered lattice subgroups of a free congruence subgroup $\hat{F}_n$ of rank $n$ of $\hat{\Gamma}(1)$. By a lattice subgroup of $\hat{F}_n$ we mean a subgroup of $\hat{F}_n$ which contains the commutator group $\hat{F}_n'$. In particular, he showed that, if $\hat{F}_n$ is a congruence group of level $N$ and if $\mathscr{G}$ is a lattice congruence subgroup of $\hat{F}_n$ of level $qr$, where $r$ is the largest divisor of $qr$ prime to $N$, then $N$ divides $q$ and $r$ divides 12. He then posed the problem of finding an upper bound for the factor $q$. It is the purpose of this paper to find such an upper bound for $q$. We also consider bounds for the factor $r$.

We note that, if $\mathscr{G}$ is a lattice congruence subgroup of level $qr$ of a free congruence subgroup $\hat{F}_n$ of level $N$, then $\mathscr{G} \cap \hat{\Gamma}(N)$ is a lattice congruence subgroup of $\hat{\Gamma}(N)$ of level $qr$. This reduces the problem to the consideration of lattice subgroups of $\hat{\Gamma}(N)$ which are congruence groups of level $qr$. We may also assume that such a lattice subgroup is normal in $\hat{\Gamma}(1)$, since the intersection of its conjugates is also a lattice congruence subgroup of $\hat{\Gamma}(N)$ of the same level $qr$. We therefore confine our attention to lattice subgroups of $\Gamma(N)$ in $\Gamma(1)$ which are congruence groups of level $qr$ and which are normal in $\Gamma(1)$. We use McQuillan's classification of normal congruence subgroups of $\Gamma(1)$ [4] and follow his notation.

**2.** Let $G \cong \prod_{i=1}^{s} G_i$, the direct product of $s$ finite groups $G_i$, and let $L$ be a subgroup of $G$. We let $F_i = \{g_i \in G_i : (1, 1, \ldots, g_i, \ldots, 1) \in L\}$ and call $F_i$ the $i$th foot of $L$.

THEOREM 1. *If $L$ is a normal subgroup of $G$, then $F_i$ is normal in $G_i$. If, in addition, $G/L$ is abelian, then $G_i/F_i$ is abelian* $(1 \leqq i \leqq s)$.

The proof is clear and is omitted.

Now let $N = \prod_{i=1}^{t} p_i^{\alpha_i}$ and $q = \prod_{i=1}^{t} p_i^{\beta_i}$, where $p_i$ is prime and $\beta_i \geqq \alpha_i > 0$ $(1 \leqq i \leqq t)$.

THEOREM 2. $\Gamma(N)/\Gamma(qr) \cong \Gamma(1)/\Gamma(r) \times \prod_{i=1}^{t} \Gamma(p_i^{\alpha_i})/\Gamma(p_i^{\beta_i})$.

https://doi.org/10.1017/S0017089500000641 Published online by Cambridge University Press

*Proof.* It is well known [7] that $\Gamma(d)/\Gamma(dmn) \cong \Gamma(d)/\Gamma(dm) \times \Gamma(d)/\Gamma(dn)$, when $d$ is an arbitrary positive integer and $(m,n) = 1$. By repeated applications of the above we obtain

$$\Gamma(N)/\Gamma(qr) \cong \Gamma(N)/\Gamma(Nr) \times \prod_{i=1}^{r} \Gamma(N)/\Gamma(Np_i^{\beta_i-\alpha_i}).$$

The result follows since $(r, N) = 1$, and so

$$\Gamma(N)/\Gamma(Nr) \cong \Gamma(1)/\Gamma(r).$$

Also

$$\Gamma(N)/\Gamma(Np_i^{\beta_i-\alpha_i}) \cong \Gamma(p_i^{\alpha_i})/\Gamma(p_i^{\beta_i}) \qquad (1 \leqq i \leqq t).$$

We write

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad U = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad W = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Let $\mathscr{G}^*$ be a lattice subgroup of $\Gamma(N)$ and let it be a congruence group of level $qr$. As previously stated, we may take $\mathscr{G}^*$ to be normal in $\Gamma(1)$. Let

$$\mathscr{G} \cong \mathscr{G}^*/\Gamma(qr).$$

Denote the foot of $\mathscr{G}$ in $\Gamma(1)/\Gamma(r)$ and $\Gamma(p_i^{\alpha_i})/\Gamma(p_i^{\beta_i})$ by $F$ and $F_i$ respectively $(1 \leqq i \leqq t)$. We let

$$F \cong F^*/\Gamma(r) \qquad \text{and} \qquad F_i \cong F_i^*/\Gamma(p_i^{\beta_i}).$$

We now apply Theorem 1 (with $L = \mathscr{G}$) and conclude that $F^*$ is a normal congruence subgroup of $\Gamma(1)$ of level $r$, such that $\Gamma(1)/F^*$ is abelian, and that $F_i^*$ is a normal congruence subgroup of $\Gamma(1)$ of level $p_i^{\beta_i}$, such that $\Gamma(p_i^{\alpha_i})/F_i^*$ is abelian.

THEOREM 3. *The factor $r$ divides* 12.

*Proof.* Clearly $F^* \supseteq \Gamma'(1)$, where $\Gamma'(1)$ is the commutator subgroup of $\Gamma(1)$. The result follows since van Lint has shown [3] that $\Gamma'(1)$ is a congruence group of level 12.

THEOREM 4. *If $p_i$ is an odd prime and $F_i^*$ is a lattice subgroup of $\Gamma(p_i^{\alpha_i})$ and a normal congruence subgroup of $\Gamma(1)$ of level $p_i^{\beta_i}$, then $p_i^{\beta_i}$ divides $p_i^{2\alpha_i}$.*

*Proof.* For $p_i$ odd, Section 3 of McQuillan's paper shows that $F_i^*$ is either $\Gamma(p_i^{\beta_i})$ or $\bar{\Gamma}(p_i^{\beta_i})$, when $\bar{\Gamma}(l) = \{A \in \Gamma(1) : A \equiv \pm I \,(\mathrm{mod}\, l)\}$.

Now if $F_i^* = \bar{\Gamma}(p_i^{\beta_i})$, then $-I \in F_i^*$. As $F_i^* \subseteq \Gamma(p_i^{\alpha_i})$, this implies that $-I \equiv I \,(\mathrm{mod}\, p_i^{\alpha_i})$, which leads to a contradiction as $p_i$ is odd and $\alpha_i > 0$.

Hence $F_i^* = \Gamma(p_i^{\beta_i})$, and we have that $\Gamma(p_i^{\alpha_i})/\Gamma(p_i^{\beta_i})$ is abelian. Thus we must have

$$U^{p_i^{\alpha_i}} W^{p_i^{\alpha_i}} \equiv W^{p_i^{\alpha_i}} U^{p_i^{\alpha_i}} \qquad (\text{mod } p_i^{\beta_i}),$$

which is true if and only if $p_i^{\beta_i}$ divides $p_i^{2\alpha_i}$.

We now consider lattice subgroups of $\Gamma(2^n)$ which are normal congruence subgroups of $\Gamma(1)$ of level $2^m$. Let $\mathscr{G}^*$ be such a subgroup and set

$$\mathscr{G} \cong \mathscr{G}^*/\Gamma(2^m).$$

The non-trivial possibilities for $\mathscr{G}$ are, in McQuillan's notation,

$$\mathscr{G} = Z(2^m); \quad E_m, \pm E_m \ (m \geqq 2); \quad C_m, H_m, \Lambda_m \ (m \geqq 3); \quad D_m, F_m, \pm D_m \ (m \geqq 4).$$

The group $\Lambda_m$ is not listed by McQuillan but is the normal subgroup corresponding to $\bar{\Gamma}(2^m)$, i.e. $\Lambda_m \cong \bar{\Gamma}(2^m)/\Gamma(2^m)$.

We consider the cases $n = 1$ and $n > 1$ separately. We denote the group $\Gamma(2^u)/\Gamma(2^m)$ by $K_m^u$.

THEOREM 5. *If $\mathscr{G}^*$ is a lattice subgroup of $\Gamma(2)$ and is a normal congruence subgroup of $\Gamma(1)$ of level $2^m$, then $2^m$ divides 16.*

*Proof.* The non-trivial possibilities for $\mathscr{G}$ are as listed above. We note that two matrices $A, B \in \mathscr{G}$ are considered as equal if and only if $A \equiv B \ (\text{mod } 2^m)$.

Now it is readily seen that all the possible groups $\mathscr{G}$ have elements whose (1, 2) and (2, 1) entries are either zero or $2^{m-1}$. Now, considering $U^2$ and $W^2$ as members of $K_m^1$, we have, since $K_m^1/\mathscr{G}$ is abelian,

$$[U^2, W^2] = U^2 W^2 U^{-2} W^{-2} \in \mathscr{G}.$$

As $[U^2, W^2] = \begin{bmatrix} 21 & -8 \\ 8 & -3 \end{bmatrix}$, this implies that $8 \equiv 0$ or $2^{m-1} \ (\text{mod } 2^m)$. These two congruences combine into $16 \equiv 0 \ (\text{mod } 2^m)$, which gives the required result.

Now

$$D_4 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 5 & 8 \\ 8 & -3 \end{bmatrix}, \begin{bmatrix} 9 & 0 \\ 0 & 9 \end{bmatrix}, \begin{bmatrix} -3 & 8 \\ 8 & 5 \end{bmatrix} \right\},$$

when the matrices are considered modulo 16. Let

$$D_4 \cong D_4^*/\Gamma(16).$$

$\Gamma(2)$ is generated by $\pm U^2, W^2$, and hence the commutator subgroup $\Gamma'(2)$ is generated by $[U^{2\lambda}, W^{2\mu}]$, with $\lambda, \mu$ integral. Since

$$[U^{2\lambda}, W^{2\mu}] \equiv \begin{bmatrix} 1+4\lambda\mu & -8\mu\lambda^2 \\ 8\mu^2\lambda & 1-4\lambda\mu \end{bmatrix} \qquad (\text{mod } 16),$$

https://doi.org/10.1017/S0017089500000641 Published online by Cambridge University Press

it can be readily verified that $[U^{2\lambda}, W^{2\mu}] \in D_4^*$, for all $\lambda, \mu$. Hence $D_4^*$ is a lattice subgroup of $\Gamma(2)$ of level 16, which shows that the upper bound for $2^m$ is in fact attained. We note finally that $\pm D_4^*$ is also a lattice subgroup of $\Gamma(2)$ of level 16, where

$$\pm D_4 \cong \pm D_4^*/\Gamma(16).$$

We now assume that $n > 1$ and consider the non-trivial possibilities for the group $\mathscr{G}$, listed previously.

LEMMA 1. $\mathscr{G} \neq \Lambda_m, \pm E_m, \pm D_m, Z(2^m)$.

*Proof.* The result follows because each of the above groups corresponds to a subgroup of $\Gamma(1)$ containing $-I$.

Now $\mathscr{G} \subseteq K_m^n$ and $-I \notin \Gamma(2^n)$, when $n > 1$. We shall assume from now on without loss of generality that $m > n$.

LEMMA 2. *If $m > n$, $\mathscr{G} \neq H_m$ and $\mathscr{G} \neq F_m$.*

*Proof.* If $\mathscr{G} = H_m$, we have, since $\mathscr{G} \subseteq K_m^n$,

$$\begin{bmatrix} -1+2^{m-1} & 0 \\ 0 & -1+2^{m-1} \end{bmatrix} \equiv I \qquad (\text{mod}\, 2^n),$$

which is untrue as $n > 1$. Thus $\mathscr{G} \neq H_m$.

If $\mathscr{G} = F_m$, we have, since $\mathscr{G} \subseteq K_m^n$,

$$\begin{bmatrix} -1-2^{m-2} & 0 \\ 0 & -1+2^{m-2} \end{bmatrix} \equiv I \qquad (\text{mod}\, 2^n).$$

This yields the congruence $2^{m-2} \equiv 2 \ (\text{mod}\, 2^n)$.

Now we are assuming that $m-2 \geqq n-1$. If $m-2 > n-1$, then the congruence reduces to $2 \equiv 0 \ (\text{mod}\, 2^n)$, which is not so. If $m-2 = n-1$, then we have $2^{n-1} \equiv 2 \ (\text{mod}\, 2^n)$, which is only true if $n = 2$. But the existence of the group $F_m$ ensures that $m \geqq 4$. Hence $n+1 \geqq 4$ and so $n \geqq 3$, which gives the required contradiction.

Thus we may conclude that $\mathscr{G} \neq F_m$.

We shall now use Lemmas 1 and 2 to obtain the following theorem.

THEOREM 6. *If $\mathscr{G}^*$ is a lattice subgroup of $\Gamma(2^n)$ and is a normal congruence subgroup of $\Gamma(1)$ of level $2^m$, then $2^m$ divides $2^{2n+1}$.*

*Proof.* Lemmas 1 and 2 show that the remaining possibilities for $\mathscr{G}$ are

$$\mathscr{G} = D_m, E_m, C_m.$$

Suppose now that $\mathscr{G} = D_m$; we make the further assumption, again without loss of generality, that $m > n+1$. Now $D_m \subseteq K_m^{m-2} \subseteq K_m^n$, if $m > n+1$. But we know that $K_m^n/D_m$ is

https://doi.org/10.1017/S0017089500000641 Published online by Cambridge University Press

abelian. Hence $K_m^{m-2}/D_m$ is abelian and

$$(K_m^n/D_m)/(K_m^{m-2}/D_m) \cong K_m^n/K_m^{m-2} \cong \Gamma(2^n)/\Gamma(2^{m-2}).$$

Thus $\Gamma(2^n)/\Gamma(2^{m-2})$ is abelian and so

$$U^{2^n}W^{2^n} \equiv W^{2^n}U^{2^n} \pmod{2^{m-2}},$$

which is true if and only if $2^m$ divides $2^{2n+2}$.

However, if $m = 2n+2$, then the fact that $K_{2n+2}^n/D_{2n+2}$ is abelian implies that

$$[U^{2^n}, W^{2^n}] \in D_{2n+2}.$$

Now

$$[U^{2^n}, W^{2^n}] \equiv \begin{bmatrix} 1+2^{2n} & 0 \\ 0 & 1-2^{2n} \end{bmatrix} \pmod{2^{2n+2}}.$$

A simple inspection shows that $[U^{2^n}, W^{2^n}] \notin D_{2n+2}$. Hence we conclude that, if $\mathscr{G} = D_m$, then $2^m$ divides $2^{2n+1}$.

Suppose now that $\mathscr{G} = E_m$ or $C_m$. Now both $E_m$ and $C_m \subseteq K_m^{m-1} \subseteq K_m^n$, for $m > n$. Using an argument similar to that given in the first part of the theorem, we can show that the fact that $K_m^n/\mathscr{G}$ is abelian implies that $\Gamma(2^n)/\Gamma(2^{m-1})$ is abelian, for $\mathscr{G} = E_m$ or $C_m$. Thus

$$[U^{2^n}, W^{2^n}] \equiv I \pmod{2^{m-1}},$$

which is true if and only if $2^m$ divides $2^{2n+1}$.

The theorem is thus established and we now show that the upper bound of $2^{2n+1}$ is attained. Let

$$C_{2n+1} \cong C_{2n+1}^*/\Gamma(2^{2n+1}).$$

and suppose that $A, B \in \Gamma(2^n)$. Then

$$A = \begin{bmatrix} 1+a2^n & b2^n \\ c2^n & 1+d2^n \end{bmatrix}, \text{ where } (a+d) = 2^n(bc-ad),$$

and

$$B = \begin{bmatrix} 1+e2^n & f2^n \\ g2^n & 1+h2^n \end{bmatrix}, \text{ where } (e+h) = 2^n(fg-eh).$$

Thus

$$AB = \begin{bmatrix} 1+(a+e)2^n+(ae+bg)2^{2n} & (b+f)2^n+(af+bh)2^{2n} \\ (c+g)2^n+(ce+gd)2^{2n} & 1+(h+d)2^n+(cf+hd)2^{2n} \end{bmatrix},$$

and

$$A^{-1}B^{-1} = \begin{bmatrix} 1+(h+d)2^n+(hd+bg)2^{2n} & -\{(b+f)2^n+(fd+be)2^{2n}\} \\ -\{(c+g)2^n+(hc+ag)2^{2n}\} & 1+(a+e)2^n+(ae+fc)2^{2n} \end{bmatrix}.$$

https://doi.org/10.1017/S0017089500000641 Published online by Cambridge University Press

Now

$$[A,B]=ABA^{-1}B^{-1}\equiv\begin{bmatrix}1+(bg-fc)2^{2n} & 0\\ 0 & 1+(fc-bg)2^{2n}\end{bmatrix}\pmod{2^{2n+1}}.$$

Thus

$$[A,B]\equiv I\quad\text{or}\quad\begin{bmatrix}1+2^{2n} & 0\\ 0 & 1+2^{2n}\end{bmatrix}\pmod{2^{2n+1}}.$$

This implies that $[A,B]\in C^*_{2n+1}$, for all $A,B\in\Gamma(2^n)$. Thus $C^*_{2n+1}$ is a lattice subgroup of $\Gamma(2^n)$ and is a congruence group whose level is equal to the upper bound of $2^{2n+1}$.

We now tabulate the results, quoting the upper bounds for the factors $q$ and $r$ in each case and stating a lattice subgroup of $\Gamma(N)$ which is a congruence group whose level is equal to the upper bound for $qr$, denoted by $\max qr$.

We shall make use of the groups $\Gamma'(1)$, $M^*$ and $\Gamma^4$. The group $M^*$ is the group corresponding to $M$ quoted by McQuillan. $M^*$ is a normal congruence subgroup of $\Gamma(1)$ of level 3 containing $\Gamma'(1)$. The group $\Gamma^4$ is not listed by McQuillan. It is the subgroup of $\Gamma(1)$ generated by $\begin{bmatrix}0 & -1\\ 1 & -1\end{bmatrix}$ and $\begin{bmatrix}-1 & -1\\ 1 & 0\end{bmatrix}$ and can readily be shown to be a normal congruence subgroup of $\Gamma(1)$ of level 4, containing $\Gamma'(1)$. We put $N=2^nl$, where $n\geqq 0$ and $l$ is odd.

TABLE

| $(N, 12)$ | $q$ divides | $r$ divides | $\max qr$ | $\max qr$ attained by |
|---|---|---|---|---|
| 1 | $N^2$ | 12 | $12N^2$ | $\Gamma'(1)\cap\Gamma(N^2)$ |
| 2 | $4N^2$ | 3 | $12N^2$ | $D^*_4\cap\Gamma(l^2)\cap M^*$ |
| 3 | $N^2$ | 4 | $4N^2$ | $\Gamma(N^2)\cap\Gamma^4$ |
| 4 | $2N^2$ | 3 | $6N^2$ | $C^*_{2n+1}\cap\Gamma(l^2)\cap M^*$ |
| 6 | $4N^2$ | 1 | $4N^2$ | $D^*_4\cap\Gamma(l^2)$ |
| 12 | $2N^2$ | 1 | $2N^2$ | $C^*_{2n+1}\cap\Gamma(l^2)$ |

Further, for all integers $d$ such that $N$ divides $d$ and $d$ divides $\max qr$, a lattice subgroup of $\Gamma(N)$ which is a congruence group of level $d$ may be readily produced.

3. We now extend the results of the table to the inhomogeneous modular group $\hat{\Gamma}(1)$. We let $\mathscr{G}$ be a lattice subgroup of $\hat{\Gamma}(N)$ and let it be a congruence group of level $qr$, as before. We may take $\mathscr{G}$ to be normal in $\hat{\Gamma}(1)$. Let $\bar{\mathscr{G}}$ be the corresponding subgroup to $\mathscr{G}$ in $\Gamma(1)$. We have $\mathscr{G}\cong\bar{\mathscr{G}}/\Lambda$, where $\Lambda=\{I,-I\}$. It is easily verified that $\mathscr{G}$ is a congruence group of level $d$ in $\hat{\Gamma}(1)$ if and only if $\bar{\mathscr{G}}$ is a congruence group of level $d$ in $\Gamma(1)$.

We consider the cases $N=2$ and $N>2$ separately.

https://doi.org/10.1017/S0017089500000641 Published online by Cambridge University Press

THEOREM 7. *If $\hat{\mathscr{G}}$ is a lattice subgroup of $\hat{\Gamma}(2)$ and is a normal congruence subgroup of $\hat{\Gamma}(1)$ of level qr, then qr divides* 48.

*Proof.* We have $\hat{\Gamma}(2) \cong \Gamma(2)/\Lambda$ and $\hat{\mathscr{G}} \cong \bar{\mathscr{G}}/\Lambda$, when $\bar{\mathscr{G}}$ is the group corresponding to $\hat{\mathscr{G}}$ in $\Gamma(1)$. Then $\bar{\mathscr{G}}$ is a normal congruence subgroup of $\Gamma(1)$ and has level $qr$. We also have

$$\hat{\Gamma}(2)/\hat{\mathscr{G}} \cong \Gamma(2)/\bar{\mathscr{G}}.$$

Thus, since $\hat{\Gamma}(2)/\hat{\mathscr{G}}$ is abelian, $\bar{\mathscr{G}}$ is a lattice subgroup of $\Gamma(2)$. The result follows by applying the results of the table for the case $N = 2$.

Let $\hat{Z}^*(8)$, $\pm \hat{D}_4^*$ and $\hat{M}^*$ be the subgroups of $\hat{\Gamma}(1)$ corresponding to the subgroups $Z^*(8)$, $\pm D_4^*$ and $M^*$ of $\Gamma(1)$ respectively. $\hat{Z}^*(8)$ and $\pm \hat{D}_4^*$ are lattice congruence subgroups of $\hat{\Gamma}(2)$ of levels 8 and 16 respectively and $\hat{M}^*$ is a congruence group of level 3 containing $\hat{\Gamma}'(1)$, the commutator subgroup of $\hat{\Gamma}(1)$. The groups $\hat{H} \cap \hat{K}$, where $\hat{H} = \hat{\Gamma}(2)$, $\hat{\Gamma}(4)$, $\hat{Z}^*(8)$ or $\pm \hat{D}_4^*$, and $\hat{K} = \hat{\Gamma}(1)$ or $\hat{M}^*$, form a set of lattice congruence subgroups of $\hat{\Gamma}(2)$, whose levels are equal to the eight even divisors of 48, including 48 itself.

THEOREM 8. *If $N > 2$ and $\hat{\mathscr{G}}$ is a lattice subgroup of $\hat{\Gamma}(N)$ and is a normal congruence subgroup of $\hat{\Gamma}(1)$ of level qr, then there exists a lattice subgroup $\mathscr{G}$ of $\Gamma(N)$ in $\Gamma(1)$ such that $\mathscr{G}$ is a normal congruence subgroup of $\Gamma(1)$ of level qr and $\hat{\mathscr{G}} \cong \mathscr{G}$.*

*Proof.* Let $\bar{\mathscr{G}}$ be defined as before, so that $\hat{\mathscr{G}} \cong \bar{\mathscr{G}}/\Lambda$. We also have

$$\hat{\Gamma}(N) \cong \bar{\Gamma}(N)/\Lambda \cong \Gamma(N).$$

Now $\bar{\mathscr{G}} \subseteq \bar{\Gamma}(N)$ so that, for any $A \in \bar{\mathscr{G}}$, $A \equiv \pm I \pmod N$. We note that, as $N > 2$, we cannot have a member of $\bar{\mathscr{G}}$ congruent to both $I$ and $-I \pmod N$.

We define a subset $\mathscr{G}$ of $\bar{\mathscr{G}}$ as follows.

$$\mathscr{G} = \{A \in \bar{\mathscr{G}} : A \equiv I \pmod N\}.$$

Clearly $\mathscr{G}$ is a subgroup of $\bar{\mathscr{G}}$ contained in $\Gamma(N)$, such that $\mathscr{G} \cong \bar{\mathscr{G}}/\Lambda$. Now $\hat{\Gamma}(qr) \subseteq \hat{\mathscr{G}}$ and $qr$ is minimal. This implies that $\bar{\Gamma}(qr)$ and hence $\Gamma(qr)$ is contained in $\bar{\mathscr{G}}$.

In fact $\Gamma(qr) \subseteq \mathscr{G}$; for, if not, there exists $X \in \bar{\mathscr{G}}$ such that

$$X \equiv I \pmod{qr} \qquad \text{and} \qquad X \equiv -I \pmod N.$$

This yields a contradiction, since $N$ divides $qr$ and $N > 2$. Moreover the level of $\mathscr{G}$ is exactly $qr$; for if there exists $d < qr$ such that $\Gamma(d) \subseteq \mathscr{G}$, then $\hat{\Gamma}(d) \subseteq \hat{\mathscr{G}}$, which contradicts the minimality of $qr$.

Finally $\mathscr{G}$ is of course normal in $\Gamma(1)$ and is a lattice subgroup of $\Gamma(N)$; for we have

$$\hat{\Gamma}(N)/\hat{\mathscr{G}} \cong \Gamma(N)/\mathscr{G}.$$

We note that, if $\mathscr{G}$ is a lattice subgroup of $\Gamma(N)$, where $N > 2$, and $\mathscr{G}$ is a normal congruence subgroup of $\Gamma(1)$ of level $qr$, then the subgroup $\hat{\mathscr{G}}$ of $\hat{\Gamma}(1)$ corresponding to $\mathscr{G}$, where $\mathscr{G} \cong \hat{\mathscr{G}}$, is a lattice subgroup of $\hat{\Gamma}(N)$ and is a normal congruence subgroup of $\hat{\Gamma}(1)$ of level $qr$. The fact that its level is exactly $qr$ follows from Theorem 8. For, clearly, $\hat{\Gamma}(qr) \subseteq \mathscr{G}$ and, if $\hat{\Gamma}(d) \subseteq \mathscr{G}$ with $d < qr$, then Theorem 8 shows that $\Gamma(d) \subseteq \mathscr{G}$, which contradicts the minimality of $qr$.

Theorems 7 and 8 show that the upper bounds for $qr$ in $\Gamma(1)$, shown in the table, also hold in $\hat{\Gamma}(1)$. Moreover the remarks following the two theorems show that the upper bounds are attained in $\hat{\Gamma}(1)$ in all cases. More generally, it is easily seen that, for all integers $d$ such that $d$ divides $\max qr$ and $N$ divides $d$, there exists a lattice subgroup of $\hat{\Gamma}(N)$ which is a congruence group of level $d$. In particular we note that in $\hat{\Gamma}(1)$ the factor $r$ divides 12 in all cases, a result obtained by Rankin by different methods.

**4.** In this section we introduce an infinite class of lattice subgroups of $\hat{\Gamma}(N)$ and use the results of the previous section to investigate which of these groups is a congruence group. These subgroups provide a natural extension to the subgroups $\Omega(p, S)$ of $\hat{\Gamma}(p)$ ($p$ a prime) introduced by Reiner [10], and for $p = 2$ by Fricke [1] and Pick [8], and contain an infinite set of subgroups of finite index in $\hat{\Gamma}(1)$ which are not congruence groups.

LEMMA 3. *For $N > 1$, $U^N$ may be taken as a free generator of $\hat{\Gamma}(N)$.*

*Proof.* For $N > 1$, it is well known that $\hat{\Gamma}(N)$ is a free group [5]. Further, $\hat{\Gamma}(N)$ has $n = \mu/N > 1$ incongruent cusps, where $\mu = [\hat{\Gamma}(1) : \hat{\Gamma}(N)]$. Now, by Section VI, 4 (p. 241) of [2], $\hat{\Gamma}(N)$ has a canonical fundamental region with $n$ incongruent parabolic vertices and $4g+n$ other " accidental " vertices, which are all congruent to each other mod $\hat{\Gamma}(N)$, where $g$ is the genus of $\hat{\Gamma}(N)$. The $n$ parabolic vertices determine $n$ parabolic generators $P_1, \ldots, P_n$, which form part of a set of $2g+n$ generators of $\hat{\Gamma}(N)$, and which satisfy one relation only (Theorem, p. 234 of [2]). We may take $P_1 = U^N$, and, as $n > 1$, we may use the relation to eliminate $P_2$, leaving a set of free generators of $\hat{\Gamma}(N)$, one of which is $U^N$.

LEMMA 4. *The rank of $\hat{\Gamma}(2)$ is 2 and, when $N > 2$, the rank of $\hat{\Gamma}(N)$ is $1+\mu(N)/12$, where*

$$\mu(N) = N^3 \prod_{p/N} \left(1 - \frac{1}{p^2}\right).$$

*Proof.* It is known that $\hat{\Gamma}(2)$ is freely generated by $U^2$ and $W^2$. Using this fact we may compute the rank of $\hat{\Gamma}(2N)$ ($N > 1$) by the well known Reidemeister–Schreier formula for the rank of a subgroup of finite index in a free group of finite rank. The rank of $\hat{\Gamma}(N)$ ($N > 2$) may then be calculated from the rank of $\hat{\Gamma}(2N)$ using the Reidemeister–Schreier formula in reverse.

Let $P = \hat{\Gamma}(N)/\hat{\Gamma}'(N)$ and let $P^S$ be the subgroup of $P$ generated by the $S$th powers of the elements of $P$ ($S \geqq 1$). Denote by $\Omega(N, S)$ the inverse image of $P^S$ under the canonical mapping of $\hat{\Gamma}(N)$ onto $P$. It is readily seen that $\Omega(N, S)$ consists of those elements of $\hat{\Gamma}(N)$ for which the exponent sums with respect to each of the free generators of $\hat{\Gamma}(N)$ is a multiple of $S$. Clearly $\Omega(N, S)$ is a lattice subgroup of $\hat{\Gamma}(N)$ and is normal in $\hat{\Gamma}(1)$. It also follows that $[\hat{\Gamma}(N) : \Omega(N, S)] = S^\sigma$, where $\sigma$ is the rank of $\hat{\Gamma}(N)$.

LEMMA 5. *If $S_1$ divides $S_2$, then $\Omega(N, S_1) \supseteq \Omega(N, S_2)$.*
The proof is obvious.

THEOREM 9. *$\Omega(N, S)$ is a congruence group if and only if $\Omega(N, S) \supseteq \hat{\Gamma}(NS)$.*

*Proof.* The level of $\Omega(N, S)$, as defined by Wohlfahrt in [**11**], is $NS$. This follows from the normality of $\Omega(N, S)$ in $\hat{\Gamma}(1)$ and from the fact that $U^N$ may be taken as a free generator of $\hat{\Gamma}(N)$. We obtain the required result by applying Theorem 2 of Wohlfahrt's paper.

We now use Theorem 9 to investigate which of the groups $\Omega(N, S)$ is a congruence group. The results obtained will include these of Reiner, for clearly, when $N$ is a prime $p$, the groups are the subgroups $\Omega(p, S)$ introduced by him. We treat the cases $N = 2$, $N = 3$ and $N \geqq 4$ separately.

THEOREM 10. *$\Omega(2, S)$ is a congruence subgroup if and only if $S = 1, 2, 4, 8$.*

*Proof.* If $\Omega(2, S)$ is a congruence group, then by Theorem 9 and the results shown in the table in Section 2 we may conclude that $S$ divides 24.

If $S$ is any divisor of 24 divisible by 3, then Lemma 5 implies that $\Omega(2, 3)$ is a congruence subgroup. However, $[\hat{\Gamma}(2) : \Omega(2, 3)] = 9$ and $[\hat{\Gamma}(2) : \hat{\Gamma}(6)] = 12$, which yields an immediate contradiction. Hence $\Omega(2, 3)$ is not a congruence subgroup.

There remain the cases $S = 1, 2, 4, 8$ to consider. We note that $\hat{\Gamma}(2)$ is freely generated by $U^2$ and $W^2$. The proof for the case $S = 8$ is to be found in Theorem 3 of a paper by Newman [**6**]. In fact Newman shows that $\hat{\Gamma}(16)$ is contained in that lattice subgroup of $\hat{\Gamma}(2)$ whose elements have exponent sums with respect to the generator $U^2$ that are multiples of 8. However, elementary modifications of his proof show that any element of $\hat{\Gamma}(16)$ also has its exponent sum with respect to the generator $W^2$ congruent to zero modulo 8. Since $\Omega(2, 8)$ is a congruence group, so also are $\Omega(2, 1)$, $\Omega(2, 2)$ and $\Omega(2, 4)$, by Lemma 5. Clearly $\Omega(2, 1) = \hat{\Gamma}(2)$ and it is also readily verified that $\Omega(2, 2) = \hat{\Gamma}(4)$, $\Omega(2, 4) = \hat{Z}^*(8)$ and $\Omega(2, 8) = \pm \hat{D}_4^*$. This completes the proof of the theorem.

THEOREM 11. *$\Omega(3, S)$ is a congruence subgroup if and only if $S = 1, 3$.*

*Proof.* If $\Omega(3, S)$ is a congruence subgroup, then by Theorem 9 and the results for $N = 3$ in the table, we conclude that $S$ divides 12. If $S$ is an even divisor of 12, then Lemma 5 implies that $\Omega(3, 2)$ is a congruence subgroup. But $[\hat{\Gamma}(3) : \Omega(3, 2)] = 8$ and $[\hat{\Gamma}(3) : \hat{\Gamma}(6)] = 6$, which yields an immediate contradiction.

Trivially $\Omega(3, 1) = \hat{\Gamma}(3)$ and, since $\hat{\Gamma}(3)$ is freely generated by $(U^{-1}W)^{-v}U^3(U^{-1}W)^v$ $(v = 1, 2, 3)$, it is easily verified that $\hat{\Gamma}(9) = \Omega(3, 3)$. This completes the proof of the theorem.

THEOREM 12. *If $N \geqq 4$, $\Omega(N, S)$ is a congruence subgroup if and only if $S = 1$.*

*Proof.* If $\Omega(N, S)$ is a congruence subgroup, then, by Theorem 9 and the results of the table in Section 2, $S$ divides $12N$. Clearly $\Omega(N, 1) = \hat{\Gamma}(N)$ which is a congruence subgroup and, if $S > 1$, then Lemma 5 implies that $\Omega(N, p)$ is a congruence subgroup, where $p$ is any prime dividing $S$. Now, since $S$ divides $12N$, this implies that $\Omega(N, p)$ is a congruence subgroup, where $p$ is any prime dividing $N$, or, when $(N, 2) = 1$, that $\Omega(N, 2)$ is a congruence subgroup, or, when $(N, 3) = 1$, that $\Omega(N, 3)$ is a congruence subgroup. We shall obtain a contradiction in the most general case for $(N, 6) = 1$. The remaining cases for $N \geqq 4$ are proved similarly.

When $(N, 6) = 1$,

$$[\hat{\Gamma}(N):\hat{\Gamma}(Np)] = p^3, \quad [\hat{\Gamma}(N):\hat{\Gamma}(2N)] = 6, \quad [\hat{\Gamma}(N):\hat{\Gamma}(3N)] = 24.$$

Also

$$[\hat{\Gamma}(N):\Omega(N,p)] = p^\sigma, \quad [\hat{\Gamma}(N):\Omega(N,2)] = 2^\sigma, \quad [\hat{\Gamma}(N):\Omega(N,3)] = 3^\sigma.$$

Contradictions follow in all cases since the formula established in Lemma 4 shows that $\sigma > 3$. The proof of the theorem is complete.

We conclude by observing that we may easily extend Lemma 3 in the following way. If $\mathscr{G}$ is any free normal subgroup of finite index $\mu$ in $\hat{\Gamma}(1)$, whose level, as defined by Wohlfahrt in [11], is $N$, then we may take $U^N$ to be a free generator of $\mathscr{G}$, provided $\mu/N > 1$. As the commutator subgroup $\mathscr{G}' \subseteq \mathscr{G}$, the level of $\mathscr{G}'$ is a multiple of $N$. If $\mu/N > 1$ and $U^{Nl} \in \mathscr{G}'$, for some integer $l$, this implies a non-trivial relation between the free generators of $\mathscr{G}$, which is an obvious contradiction. Hence, when $\mu/N > 1$, the level of $\mathscr{G}'$ is infinite. In fact $\mu/N > 1$ for all free normal subgroups $\mathscr{G}$ of finite index in $\hat{\Gamma}(1)$, except for $\mathscr{G} = \hat{\Gamma}'(1)$, when $\mu = N = 6$. This discussion shows that Proposition 1 of [9] only holds for $\mathscr{G} = \hat{\Gamma}'(1)$, where the level of $\mathscr{G}' = \hat{\Gamma}''(1)$ is 6.

## REFERENCES

**1.** R. Fricke, Über die Substitutionsgruppen, welche zu den aus Legendre'schen Integralmodul $k^2(\omega)$ gezogenen Wuhrzeln gehören, *Math. Ann.* **28** (1887), 99–118.

**2.** Joseph Lehner, *Discontinuous groups and automorphic functions*, Mathematical Surveys, No. VIII, American Mathematical Society (Providence, R.I., 1964).

**3.** J. H. van Lint, On the multiplier system of the Riemann–Dedekind function $\eta$, *Nederl. Akad. Wetensch. Proc. Ser. A* **61** (=*Indag. Math.* **20**) (1958), 522–527.

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

**5.** M. Newman, Free subgroups and normal subgroups of the modular group, *Illinois J. Math.* **8** (1964), 262–265.

**6.** M. Newman, On a problem of G. Sansone, *Ann. Mat. pura appl.* **65** (1964), 27–34.

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

**8.** G. Pick, Über gewisse ganzzahlige lineare Substitutionen, welche sich nicht durch algebraische Congruenzen erklären lassen, *Math. Ann.* **28** (1887), 119–124.

**9.** R. A. Rankin, Lattice subgroups of free congruence groups, *Inventiones Math.* **2** (1967), 215–221.

**10.** I. Reiner, Normal subgroups of the unimodular group, *Illinois J. Math.* **2** (1958), 142–144.

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

UNIVERSITY OF GLASGOW