INCLUSION THEOREMS FOR CONGRUENCE SUBGROUPS

BY

M. NEWMAN AND I. REINER(1)

1. **Introduction.** We shall use the following notation throughout: $A^{(r)}$ denotes an $r\times r$ matrix A; $I^{(r)}$ denotes the r-rowed identity matrix; 0 will be used for a zero matrix of appropriate size. Congruence of matrices will be interpreted as elementwise congruence. We write $a|b$ to indicate that a divides b. Lower case italic letters will always denote integers.

Let G_t be the proper unimodular group consisting of all $t\times t$ matrices with integral elements and determinant $+1$. For a fixed partition: $t=r+s$ of t into two positive integers r and s, and for a fixed positive integer n, define the subgroup

$$G_{r,s}(n) = \left\{\begin{bmatrix} A^{(r)} & B \\ C & D^{(s)}\end{bmatrix} \in G_t: \quad C \equiv 0 \pmod{n}\right\}. \tag{1}$$

We shall prove:

THEOREM 1. *Let m, n be positive integers, and let H be a group such that*

$$G_{r,s}(mn) \subset H \subset G_{r,s}(n). \tag{2}$$

Then there exists a divisor d of m such that

$$H = G_{r,s}(dn). \tag{3}$$

Special cases of this have been proved in [1] and [3].

In the case where $t=2r$, define

$$G_r(m, n) = \left\{\begin{bmatrix} A^{(r)} & B \\ C & D^{(r)}\end{bmatrix} \in G_{2r}: \begin{matrix} B \equiv 0 \pmod{m}, \\ C \equiv 0 \pmod{n} \end{matrix}\right\}. \tag{4}$$

Then we shall show:

THEOREM 2. *Let H be a group satisfying*

$$G_r(m, n) \subset H \subset G_{2r}. \tag{5}$$

If $(m, n)=1$, then there exist integers m_1, n_1 with $m_1|m$, $n_1|n$, and

$$H = G_r(m_1, n_1). \tag{6}$$

Presented to the Society, October 26, 1957; received by the editors October 14, 1957.

(1) The work of the first author was supported (in part) by the Office of Naval Research, and that of the second author was supported (in part) by a contract with the National Science Foundation.

A special case of this (with $r=1$) was proved in [2], where it was also shown that the hypothesis $(m, n)=1$ could not be dropped.

To generalize further, let $\mathfrak{n}=(n_1, \cdots, n_{t-1})$, and define

$$G_t(\mathfrak{n}) = G_{1,t-1}(n_1) \cap G_{2,t-2}(n_2) \cap \cdots \cap G_{t-1,1}(n_{t-1}). \tag{7}$$

Thus an element $M \in G_t$ lies in $G_t(\mathfrak{n})$ if and only if for every partition $t=r+s$ $(1 \leqq r \leqq t-1)$ we have

$$M = \begin{bmatrix} A^{(r)} & B \\ C & D^{(s)} \end{bmatrix}, \qquad C \equiv 0 \pmod{n_r}.$$

We shall prove:

THEOREM 3. *Let $(m_i n_i, m_j n_j)=1$ for $1 \leqq i, j \leqq t-1$, $i \neq j$. Let H be a group such that*

$$G_t(\mathfrak{mn}) \subset H \subset G_t(\mathfrak{n}), \tag{8}$$

where $\mathfrak{mn}$ denotes $(m_1n_1, \cdots, m_{t-1}n_{t-1})$. Then there exists a vector

$$\mathfrak{d} = (d_1, \cdots, d_{t-1}),$$

with $d_1 | m_1, \cdots, d_{t-1} | m_{t-1}$, such that

$$H = G_t(\mathfrak{dn}). \tag{9}$$

Finally, we shall prove analogues of Theorems 1 and 2 for the symplectic modular group Γ_t of order t, which consists of all integral matrices

$$\begin{bmatrix} A^{(t)} & B \\ C & D^{(t)} \end{bmatrix}$$

satisfying

$$AB' = B'A, \qquad CD' = D'C, \qquad AD' - DC' = I.$$

2. We begin the proof of Theorem 1 with two lemmas.

LEMMA 1. *Let $t=r+s$, and let n be a fixed positive integer. For each*

$$M = \begin{bmatrix} A^{(r)} & B \\ C & D^{(s)} \end{bmatrix} \in G_t$$

there exists an integral $r \times s$ matrix X such that $(|A+XC|, n)=1$.

Proof. It is sufficient to show that for every prime p there exists an integral matrix X_p such that $p \nmid |A+X_pC|$. For we may then find an integral matrix X satisfying $X \equiv X_p \pmod{p}$ for each $p | n$. Since $|A + XC| \equiv |A+X_pC| \pmod{p}$, it then follows that $(|A+XC|, n)=1$.

Now let p be a fixed prime, and let $\alpha_1, \cdots, \alpha_r$ denote the rows of A, and

$\gamma_1, \cdots, \gamma_s$ those of C. Since the rows of X_pC are linear combinations of those of C, we need only show that there exist linear combinations

$$\beta_i = \sum_{j=1}^{s} x_{ij}\gamma_j \qquad (1 \leqq i \leqq r,\ x_{ij} \text{ integers})$$

such that $p \nmid \det(\alpha_i+\beta_i)$. Thus, we seek integers x_{ij} for which the vectors $\alpha_i+\beta_i$ $(1 \leqq i \leqq r)$ are linearly independent modulo p.

Since M is unimodular, the set $\{\alpha_1, \cdots, \alpha_r, \gamma_1, \cdots, \gamma_s\}$ contains exactly r linearly independent vectors modulo p. Suppose that r' of the α's are linearly independent modulo p $(r' \leqq r)$; for simplicity of notation, suppose that these are $\alpha_1, \cdots, \alpha_{r'}$. Then each α_k $(r' < k \leqq r)$ is a linear combination modulo p of $\alpha_1, \cdots, \alpha_{r'}$. Further, there exist $r-r'$ vectors $\gamma_1^*, \cdots, \gamma_{r-r'}^*$ among $\gamma_1, \cdots, \gamma_s$ such that the set $\{\alpha_1, \cdots, \alpha_{r'}, \gamma_1^*, \cdots, \gamma_{r-r'}^*\}$ is linearly independent modulo p. Then we need only choose $\beta_1 = \cdots = \beta_{r'} = 0$, $\beta_{r'+1} = \gamma_1^*, \cdots, \beta_r = \gamma_{r-r'}^*$ to achieve the desired result.

LEMMA 2. *Let $M \in G_{r,s}(n)$, and let m be a fixed positive integer. Then there exists an integral $r \times s$ matrix X and an integral $s \times r$ matrix Y such that*

$$W(nY)S(X)\,M \in G_{r,s}\,(m\,n), \tag{10}$$

where

$$W(nY) = \begin{bmatrix} I^{(r)} & 0 \\ nY & I^{(s)} \end{bmatrix}, \qquad S(X) = \begin{bmatrix} I^{(r)} & X \\ 0 & I^{(s)} \end{bmatrix}.$$

The entries of X and Y are integers determined only modulo m. Therefore the set of products $W(nY)S(X)$, as the entries of X and Y range over all residues modulo m, contains a full set of left coset representatives of $G_{r,s}(n)$ modulo $G_{r,s}(mn)$. Consequently $G_{r,s}(mn)$ is of finite index in $G_{r,s}(n)$.

Proof. Set

$$M = \begin{bmatrix} A^{(r)} & B \\ nC & D^{(s)} \end{bmatrix} \in G_{r,s}(n).$$

By Lemma 1, we can determine X modulo m such that $(|A+nXC|, m) = 1$. Set $A_0 = A+nXC$. Then

$$S(X)M = \begin{bmatrix} A_0 & * \\ nC & * \end{bmatrix},$$

and

$$W(nY)S(X)M = \begin{bmatrix} * & * \\ n(YA_0+C) & * \end{bmatrix}.$$

In order for (10) to hold, we need only show that Y modulo m can be determined so that $YA_0+C\equiv 0 \pmod{m}$.

Now $(|A_0|, m)=1$, so that we may find an integer a with $a|A_0|\equiv 1 \pmod{m}$. Letting A_0^{adj} denote the adjoint of A_0, we set

$$Y \equiv -aCA_0^{\mathrm{adj}} \pmod{m}. \tag{11}$$

Using $A_0^{\mathrm{adj}}A_0=|A_0|I$, we obtain

$$YA_0 \equiv -C \pmod{m},$$

as desired.

The remainder of the lemma follows at once from (10).

We now proceed with the proof of Theorem 1. Let H be a group such that

$$G_{r,s}(mn) \subset H \subset G_{r,s}(n).$$

Using the argument in [1], we find by induction on the total number of prime factors of m that the conclusion of Theorem 1 is valid unless for every d dividing m, $d\neq 1$, we have

$$H \cap G_{r,s}(dn) = G_{r,s}(mn).$$

Suppose now that $H\neq G_{r,s}(mn)$. The above then shows that there exists a matrix

$$M = \begin{bmatrix} A^{(r)} & B \\ nC & D^{(s)} \end{bmatrix} \in H$$

such that $C\not\equiv 0 \pmod{d}$ for any divisor d of m, $d\neq 1$. Choose X, Y as in Lemma 2, and use the fact that $S(X)\in H$. Then we see that $W(nY)\in H$, where Y is chosen by use of (11). Hence also $Y\not\equiv 0 \pmod{d}$ for any divisor d of m, $d\neq 1$.

Call an $s\times r$ matrix T *permissible* if $W(nT)\in H$. We have shown the existence of a permissible matrix Y such that $Y\not\equiv 0 \pmod{d}$ for any divisor d of m, $d\neq 1$. We shall use this to deduce that every matrix is permissible. Since already $S(X)\in H$ for all X, it will then follow from Lemma 2 that $H=G_{r,s}(n)$, and the theorem will be proved.

Now we have

$$W(nT_1)\cdot W(nT_2) = W(n(T_1+T_2)),$$

and

$$\begin{bmatrix} V^{-1} & 0 \\ 0 & U \end{bmatrix} W(nT) \begin{bmatrix} V & 0 \\ 0 & U^{-1} \end{bmatrix} = W(nUTV), \quad U\in G_s, \quad V\in G_r.$$

Therefore if T_1 and T_2 are permissible, so is T_1+T_2. If T is permissible, then so is $-T$; and if $U \in G_s$, $V \in G_r$, then UTV is also permissible.

Starting with the permissible Y above, set $Y_1 = UYV$, with $U \in G_s$, $V \in G_r$. Then Y_1 is also permissible, and with proper choice of U and V, we may take Y_1 in Smith normal form:

$$Y_1 = \begin{bmatrix} h_1 & & & \\ & h_2 & & \\ & & \ddots & \\ & & & h_\mu \end{bmatrix}, \qquad \mu = \min(r, s),$$

where $h_1 | h_2 | \cdots | h_\mu$. If $(h_1, m) > 1$, then there is a prime $p | m$ such that $Y_1 \equiv 0 \pmod{p}$. Then also $Y \equiv 0 \pmod{p}$, which is impossible. Hence $(h_1, m) = 1$. Let us choose a so that $ah_1 \equiv 1 \pmod{m}$. Then $Y_2 = aY_1$ is also permissible. Since a permissible matrix remains permissible when multiples of m are added to its entries, we therefore have the permissible matrix

$$Y_3 = \begin{bmatrix} 1 & & & \\ & k_2 & & \\ & & \ddots & \\ & & & k_\mu \end{bmatrix}.$$

Hence also

$$Y_4 = \begin{bmatrix} 0 & -k_2 & & & \\ 1 & 0 & & & \\ & & k_3 & & \\ & & & \ddots & \\ & & & & k_\mu \end{bmatrix}$$

and

$$Y_5 = Y_3 - Y_4 = \begin{bmatrix} 1 & k_2 & & & \\ -1 & k_2 & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0 \end{bmatrix}$$

are permissible. In Y_5 add the second row to the first row, and then subtract the matrix so obtained from Y_5, obtaining the permissible matrix which has 1 in the (1, 1) place, $-k_2$ in the (1, 2) place, and 0 elsewhere. In this matrix add k_2 times the first column to the second column, thereby obtaining the permissible matrix

$$Y_6 = \begin{bmatrix} 1 & & & & \\ & 0 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & 0 \end{bmatrix}.$$

Since also UY_6V is permissible for all $U \in G_s$, $V \in G_r$, we find that every matrix whose entries are all zeros except for a single 1, must be permissible. Therefore all matrices are permissible, and Theorem 1 is proved.

3. We now prove Theorem 2. Let H be a group satisfying

$$G_r(m, n) \subset H \subset G_{2r},$$

where $G_r(m, n)$ is defined by (4), and where $(m, n) = 1$. Choose integers a, b satisfying $am - bn = 1$, and set

$$K = \begin{bmatrix} amI^{(r)} & I \\ bnI & I^{(r)} \end{bmatrix} \in G_{2r}.$$

Then as in [2] we find that $K^{-1}G_r(m, n)K = G_{r,r}(mn)$, and the remainder of the proof of Theorem 2 follows from Theorem 1 just as in [2].

Theorem 2 is false for $(m, n) > 1$, as is shown in [2].

4. To prove Theorem 3, we begin with several lemmas.

LEMMA 3. *Let $n_1, \cdots, n_{t-1}$ be pairwise coprime, and let $M \in G_t$. Then there exists an upper triangular matrix $S \in G_t$ such that for each r $(1 \leqq r \leqq t-1)$ we have*

$$M = \begin{bmatrix} A^{(r)} & B \\ C & D^{(t-r)} \end{bmatrix}, \qquad S \equiv \begin{bmatrix} I^{(r)} & X_r \\ 0 & I^{(t-r)} \end{bmatrix} \pmod{n_r}, \tag{12}$$

and

$$(|A^{(r)} + X_rC|, n_r) = 1. \tag{13}$$

Proof. Let M be fixed. For each r, write M in the form (12). By Lemma 1, we may then choose X_r such that (13) holds. We then use the Chinese remainder theorem to determine an upper triangular matrix S satisfying

$$S \equiv \begin{bmatrix} I^{(r)} & X_r \\ 0 & I^{(t-r)} \end{bmatrix} \pmod{n_r}, \qquad 1 \leqq r \leqq t-1.$$

This completes the proof of the lemma.

LEMMA 4. *Let S be an integral $t \times t$ matrix such that $|S| \equiv 1 \pmod{n}$. Then there exists a matrix $T \in G_t$ such that $T \equiv S \pmod{n}$.*

Proof. (Although this lemma is known, references are hard to come by, and so we insert a proof.)

Set $T=S+nY$; we need only choose Y so that $|S+nY|=1$. Let $U, V \in G_t$ be chosen so that $USV=D$ is diagonal, and set $X=UYV$. Then

$$|S+nY| = |D+nX|,$$

so it suffices to show that we can find X such that $|D+nX|=1$, where D is diagonal and $|D|\equiv 1 \pmod{n}$.

Let $D=\operatorname{diag}(d_1, \cdots, d_t)$, and set $|D|=1+nd$. Choose X so that

$$D+nX = \begin{bmatrix} d_1+nx & 0 & 0 & \cdots 0 & ny \\ n & d_2 & 0 & \cdots 0 & 0 \\ 0 & n & d_3 & \cdots 0 & 0 \\ \cdot & \cdot & \cdot & \cdots\cdot & \cdot \\ 0 & 0 & 0 & \cdots n & d_t \end{bmatrix}.$$

Then

$$|D+nX| = 1+n(d+xd_2\cdots d_t \pm n^{t-1}y).$$

Since $(d_2\cdots d_t, n)=1$, we may choose integers x, y such that

$$d+xd_2\cdots d_t \pm n^{t-1}y = 0,$$

which completes the proof.

LEMMA 5. *Let* $\mathfrak{m}=(m_1, \cdots, m_{t-1})$, $\mathfrak{n}=(n_1, \cdots, n_{t-1})$, *where* $(m_i, n_i)=1$ *for* $1\leqq i\leqq t-1$, $(m_in_i, m_jn_j)=1$ *for* $1\leqq i, j\leqq t-1$, $i\neq j$, *and let* $M\in G_r(\mathfrak{n})$. *Then there is an upper triangular matrix* $S\in G_t$ *and a lower triangular matrix* $W\in G_t$ *such that* $WSM\in G_r(\mathfrak{m}\mathfrak{n})$. *The entries of* W *and* S *are determined only modulo* $m_1\cdots m_{t-1}$, *and hence* $G(\mathfrak{m}\mathfrak{n})$ *is of finite index in* $G(\mathfrak{n})$.

Proof. This lemma follows readily from Lemma 3 in the same way that Lemma 2 follows from Lemma 1.

We now proceed with the proof of Theorem 3. Let $\mathfrak{m}$, $\mathfrak{n}$ be chosen as in the above lemma, and let H be a group such that

$$G_t(\mathfrak{m}\mathfrak{n}) \subset H \subset G_t(\mathfrak{n}).$$

As in the proof of Theorem 1, by using induction on the total number of prime factors of $m_1m_2\cdots m_{t-1}$, we see that the theorem holds unless for every vector $\mathfrak{a}=(a_1, \cdots, a_{t-1})$ such that $a_1|m_1, \cdots, a_{t-1}|m_{t-1}$, except

$$\mathfrak{a} = (1, \cdots, 1),$$

we have

$$H\cap G_t(\mathfrak{a}\mathfrak{n}) = G_t(\mathfrak{n}\mathfrak{m}). \tag{14}$$

Suppose that $H\neq G_t(\mathfrak{m}\mathfrak{n})$; then H must contain an element M such that for each r $(1\leqq r\leqq t-1)$ we have

$$M = \begin{bmatrix} A^{(r)} & B \\ n_r C & D^{(t-r)} \end{bmatrix}$$

with $C \not\equiv 0 \pmod{a_r}$ for each divisor a_r of m_r, $a_r \neq 1$.

Now choose an upper triangular matrix S and a lower triangular matrix W as in Lemma 5, such that $WSM \in G_r(\mathfrak{mn}) \subset H$. Since also $S \in H$, this shows that $W \in H$. Further, for each r we have

$$W \equiv \begin{bmatrix} I^{(r)} & 0 \\ n_r Y_r & I^{(t-r)} \end{bmatrix} \pmod{m_r}, \tag{15}$$

where $Y_r \not\equiv 0 \pmod{a_r}$ for any a_r dividing m_r, $a_r \neq 1$.

Call a lower triangular matrix in G_t *permissible* if it is an element of H. The above-constructed W is permissible. If we can show that all lower triangular matrices in $G_t(\mathfrak{n})$ are permissible, then using Lemma 5 we will deduce that $H = G_t(\mathfrak{n})$, and Theorem 3 will be established.

Define the non-negative integer k by $m_1 = \cdots = m_{k-1} = 1$, $m_k > 1$. (If $m_1 > 1$, then choose $k = 1$.) We shall show that also $m_{k+1} = \cdots = m_{t-1} = 1$. For let $m_0 = m_{k+1} \cdots m_{t-1}$; then $(m_0, m_k) = 1$.

Now we remark that the matrix Y_r was determined only modulo m_r, and hence since $(m_r, n_r) = 1$, we could have chosen the permissible matrix W so that instead of (15) we have (for each r)

$$W \equiv \begin{bmatrix} I^{(r)} & 0 \\ n_r Y_r & I^{(t-r)} \end{bmatrix} \pmod{m_r n_r}. \tag{16}$$

Then $W \in H$, so also $W^{m_0} \in H$. Now for each r $(1 \leqq r \leqq t-1)$ we have

$$W^{m_0} \equiv \begin{bmatrix} I^{(r)} & 0 \\ n_r m_0 Y_r & I^{(t-r)} \end{bmatrix} \pmod{m_r n_r},$$

whence

$$W^{m_0} \in G_t(n_1, \cdots, n_k, m_{k+1}n_{k+1}, \cdots, m_{t-1}n_{t-1}).$$

Unless $(1, \cdots, 1, m_{k+1}, \cdots, m_{t-1}) = (1, \cdots, 1)$, we deduce from (15) that $W^{m_0} \in G_t(\mathfrak{mn})$, which is impossible because $W^{m_0} \notin G_{k-1,t-k+1}(m_k n_k)$. We thus have shown that $\mathfrak{m} = (1, \cdots, 1, m_k, 1, \cdots, 1)$.

We are now supposing that

$$G_t(\mathfrak{mn}) \subset H \subset G_t(\mathfrak{n}),$$

where $\mathfrak{m} = (1, \cdots, 1, m_k, 1, \cdots, 1)$, $m_k > 1$, that (14) holds, and that $H \neq G_t(\mathfrak{mn})$. We have shown the existence of a lower triangular matrix $W \in H$ such that (16) holds, with $Y_k \not\equiv 0 \pmod{a_k}$ for any a_k dividing m_k, $a_k \neq 1$. We are trying to prove that every lower triangular matrix in $G_t(\mathfrak{n})$ is permissible (that is, lies in H), and consequently that $H = G_t(\mathfrak{n})$.

Let $U \in G_k$, $V \in G_{t-k}$ be arbitrary. By Lemma 4, there exists a matrix $R \in G_t$ such that

$$R \equiv I \pmod{n_r}, \qquad 1 \leqq r \leqq t-1,\ r \neq k,$$

$$R \equiv \begin{bmatrix} U & 0 \\ 0 & V \end{bmatrix} \pmod{m_k n_k}.$$

Then $R \in G_t(\mathfrak{m}\mathfrak{n}) \subset H$, and hence also $W_1 = RWR^{-1} \in H$. But we have

$$W_1 \equiv \begin{bmatrix} I^{(k)} & 0 \\ n_k V Y_k U^{-1} & I^{(t-k)} \end{bmatrix} \pmod{m_k n_k},$$

and

$$W_1 \equiv \begin{bmatrix} I^{(r)} & 0 \\ n_r Y_r & I^{(t-r)} \end{bmatrix} \pmod{n_r}$$

for $1 \leqq r \leqq t-1$, $r \neq k$. The same reasoning as in the proof of Theorem 1 then shows that all lower triangular matrices in $G_t(\mathfrak{n})$ lie in H, whence $H = G_t(\mathfrak{n})$ and Theorem 3 is proved.

5. We conclude with an examination of the symplectic modular group Γ_t of order t (see [4]). Let

$$\Gamma_t(m, n) = \left\{ \begin{bmatrix} A^{(t)} & B \\ C & D^{(t)} \end{bmatrix} \in \Gamma_t : \begin{matrix} B \equiv 0 \pmod{m}, \\ C \equiv 0 \pmod{n} \end{matrix} \right\},$$

and set $\Gamma_t(n) = \Gamma_t(1, n)$. We shall prove analogues of Theorems 1 and 2. We begin with

LEMMA 6. *Let n be a fixed positive integer, and let*

$$M = \begin{bmatrix} A^{(t)} & B \\ C & D^{(t)} \end{bmatrix} \in \Gamma_t.$$

Then there exists a symmetric $t \times t$ matrix X such that $(|A + XC|, n) = 1$.

Proof. As in the proof of Lemma 1, it suffices to show for each prime p that there exists a symmetric matrix X_p for which $p \nmid |A + X_p C|$. For U, $V \in G_t$ we have

$$\begin{bmatrix} U & 0 \\ 0 & U'^{-1} \end{bmatrix} M \begin{bmatrix} V & 0 \\ 0 & V'^{-1} \end{bmatrix} = \begin{bmatrix} A_1^{(t)} & B_1 \\ C_1 & D_1^{(t)} \end{bmatrix} \in \Gamma_t,$$

with $A_1 = UAV$, $C_1 = U'^{-1}CV$. Set $Y_p = UX_pU'$; then

$$A_1 + Y_p C_1 = U(A + X_p C)V.$$

Hence we need only find a symmetric matrix Y_p such that $p \nmid |A_1 + Y_p C_1|$.

By proper choice of U, $V \in G_t$, we may assume that A_1 is diagonal. Let

$$A_1 \equiv \begin{bmatrix} E^{(k)} & 0 \\ 0 & 0 \end{bmatrix} \pmod{p},$$

where E is diagonal and nonsingular modulo p. (The case where $A \equiv 0 \pmod{p}$ is easily disposed of separately.) Setting

$$C_1 = \begin{bmatrix} C_{11}^{(k)} & C_{12} \\ C_{21} & C_{22}^{(t-k)} \end{bmatrix},$$

the symmetry of $A_1' C_1$ shows that $C_{12} \equiv 0 \pmod{p}$. Hence

$$\begin{bmatrix} A_1 \\ C_1 \end{bmatrix} \equiv \begin{bmatrix} E & 0 \\ 0 & 0 \\ C_{11} & 0 \\ C_{21} & C_{22} \end{bmatrix} \pmod{p},$$

whence $p \nmid |C_{22}|$. Then set

$$Y_p = \begin{bmatrix} 0 & 0 \\ 0 & I^{(t-k)} \end{bmatrix},$$

and obtain

$$A_1 + Y_p C_1 \equiv \begin{bmatrix} E & 0 \\ C_{21} & C_{22} \end{bmatrix} \pmod{p};$$

which shows that $p \nmid |A_1 + Y_p C_1|$. This completes the proof of the lemma.

LEMMA 7. *Let $M \in \Gamma_t(n)$, and let m be a fixed positive integer. Then there exist symmetric integral $t \times t$ matrices X, Y, whose entries are determined only modulo m, such that*

$$W(nY)S(X)M \in \Gamma_t(mn),$$

where

$$W(nY) = \begin{bmatrix} I^{(t)} & 0 \\ nY & I^{(t)} \end{bmatrix}, \qquad S(X) = \begin{bmatrix} I^{(t)} & X \\ 0 & I^{(t)} \end{bmatrix}.$$

Proof. The proof follows that of Lemma 2. The only additional fact needed is that the matrix Y determined by Equation (11) can be chosen to be symmetric, since the symmetry of $A_0' C$ implies that of CA_0^{adj}.

We now have

THEOREM 4. *Let m, n be positive integers, and let H be a group such that*

$$\Gamma_t(mn) \subset H \subset \Gamma_t(n).$$

Then there exists a divisor d of m such that $H=\Gamma_t(dn)$.

Proof. This theorem follows from Lemmas 6 and 7 in the same manner that Theorem 1 follows from Lemmas 1 and 2. We omit the details.

THEOREM 5. *Let* m, n *be positive coprime integers, and let* H *be a group satisfying*

$$\Gamma_t(m, n) \subset H \subset \Gamma_t.$$

Then there exist integers m_1, n_1 *with* $m_1 | m$, $n_1 | n$, *and* $H=\Gamma_t(m_1, n_1)$.

Proof. The proof of Theorem 2 carries over to this case with minor modifications. We omit the details.

REFERENCES

1. Morris Newman, *Structure theorems for modular subgroups*, Duke Math. J. vol. 22 (1955) pp. 25–32.

2. ———, *An inclusion theorem for modular groups*, Proc. Amer. Math. Soc. vol. 8 (1957) pp. 125–127.

3. Irving Reiner and J. D. Swift, *Congruence subgroups of matrix groups*, Pacific J. Math. vol. 6 (1956) pp. 529–540.

4. L. K. Hua and Irving Reiner, *On the generators of the symplectic modular group*, Trans. Amer. Math. Soc. vol. 65 (1949) pp. 415–426.

NATIONAL BUREAU OF STANDARDS,
WASHINGTON, D. C.
UNIVERSITY OF ILLINOIS,
URBANA, ILL.