On putting $x = c$ in (8) we then have

$$d = \sum_{1 \leqslant j \leqslant n-1} (a_j c + b_j)^2,$$

as required.

Proof of Theorem 3. This follows from Theorem 2 on putting

$$x = x_n, \quad k = \boldsymbol{R}(x_1, \ldots, x_{n-1})$$

and using induction on n.

Added in proof. Dr A. Pfister has made some interesting applications of these theorems which will be published in the Journal of the London Mathematical Society.

References

[1] E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*, Abh. Math. Sem. Hamburg 5 (1927), pp. 100-115.

[2] J. W. S. Cassels, *Bounds for the least solutions of homogeneous quadratic equations*, Proc. Cambridge Phil. Soc. 51(1955), pp. 262-264.

[3] H. Davenport, *Note on a theorem of Cassels*, Proc. Cambridge Phil. Soc. 53(1957), pp. 539-540.

[4] — *A problematic identity*, Mathematika 10(1963), pp. 10-12.

[5] E. Landau, *Über die Darstellung definiter Funktionen durch Quadrate*, Math. Ann. 62 (1906), pp. 272-285.

[6] E. Witt, *Zerlegung reeller algebraischer Funktionen in Quadrate, Schiefkörper über reellem Funktionenkörper*, J. reine angew. Math. 171 (1934), pp. 4-11.

TRINITY COLLEGE, CAMBRIDGE

Reçu par la Rédaction le 18. 6. 1963

ACTA ARITHMETICA
IX (1964)

Symplectic modulary groups

by

M. Newman and J. R. Smart (Washington)

Dedicated to Professor L. J. Mordell on the occasion on his 75th birthday

1. Introduction. In this article we extend our investigation of modulary groups of matrices initiated in [2] for the $t \times t$ modular group to the $2t \times 2t$ symplectic modular group. The principal difficulty that had to be overcome was the proof of Theorem 1 below, which itself is a result of much interest, and suggests the following general question: Suppose that f is a mapping of the ring of $p \times p$ rational integral matrices into the ring of $q \times q$ rational integral matrices. Suppose further that n is a positive integer and that the congruence $f(A) \equiv 0 \pmod{n}$ has a solution A, where A is a $p \times p$ rational integral matrix. For what mappings f is it possible to deduce the existence of a matrix B such that $B \equiv A \pmod{n}$ and $f(B) = 0$? Examples of such mappings are $f(A) = 1 - \det(A)$, $f(A) = A - A'$ (Lemma 1 below) and $f(A) = AJA' - J$ (Theorem 1 below), where J is the $2t \times 2t$ matrix

$$\begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}.$$

Here I is the $t \times t$ identity matrix, and will stand in what follows for the identity matrix of arbitrary size.

In the discussion that follows *all* matrices will have rational integral entries. Γ will denote the $2t \times 2t$ symplectic modular group. Then Γ is the group of automorphs of J and consists of all $2t \times 2t$ matrices

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

such that $MJM' = J$. Such a matrix will be referred to as *symplectic*. It is easy to verify that M is symplectic if and only if

$$AD' - BC' = I, \quad AB' = BA', \quad CD' = DC'.$$

It is also true that if M is symplectic then so is M'.

If M is a matrix satisfying $MJM' \equiv J \pmod{n}$, then M will be said to be *symplectic modulo n*.

It is customary to consider not Γ, but Γ modulo its centrum $\{I, -I\}$. This is equivalent to identifying an element of Γ with its negative. For our purposes it is irrelevant whether or not this identification is made, and we accordingly retain the distinction.

The *principal congruence subgroup* of Γ of *level n*, denoted by $\Gamma(n)$, is defined as the totality of elements M of Γ such that

$$M \equiv \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix} \pmod{n}.$$

Then $\Gamma(n)$ is a normal subgroup of Γ, and one can define the *symplectic modulary group*

(1) $$\mathfrak{M}(a, b) = \Gamma(a)/\Gamma(b), \quad a \mid b.$$

Our principal result is to reduce the study of the groups (1) to the case when a and b are each powers of the same prime p; and under certain circumstances to determine them completely.

Many of the results that follow can be proved in just the same way as the corresponding results of [2]. When this is the case the proof is omitted and the reader is referred to [2] for full details.

2. Matrices modulo n.

LEMMA 1. *Suppose that the matrix A satisfies $A \equiv A' \pmod{n}$. Then there is a symmetric matrix B such that $B \equiv A \pmod{n}$.*

Proof. Put $A = A' + nE$, where E is an integral matrix. Then $E' = -E$. Put $E = (e_{ij})$ and define

$$E^+ = \left(\tfrac{1}{2}(e_{ij} + |e_{ij}|)\right).$$

Then E^+ is an integral matrix, and is obtained from E by replacing all negative entries by 0. Furthermore (since E is skew-symmetric),

$$(E^+)' = \left(\tfrac{1}{2}(-e_{ij} + |e_{ij}|)\right),$$

and so $E = E^+ - (E^+)'$. Thus

$$A - A' = nE = n\left(E^+ - (E^+)'\right),$$

$$A - nE^+ = (A - nE^+)'.$$

Hence we may choose $B = A - nE^+$.

LEMMA 2. *Let $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ be symplectic modulo n. Then there is a symmetric matrix X such that*

$$\left(\det(A + XC), n\right) = 1.$$

The proof, with minor modifications, is identical with the proof of Lemma 6, pp. 377-378 of [1]. The essential observation is that $(\det M, n) = 1$ since $(\det M)^2 \equiv 1 \pmod{n}$.

LEMMA 3. *Suppose that P, Q are commuting symmetric matrices such that $M = \begin{bmatrix} P & 0 \\ 0 & Q \end{bmatrix}$ is symplectic modulo n. Then there is a symplectic matrix N such that $M \equiv N \pmod{n}$.*

Proof. M is symplectic modulo n if and only if $PQ \equiv I \pmod{n}$. Put $PQ = I - nE$, where E is symmetric and commutes with both P and Q. Then it is easily verified that the matrix

$$N = \begin{bmatrix} P + nEP & -nE \\ nE & Q \end{bmatrix}$$

is symplectic, and is certainly congruent to M modulo n.

We are now in a position to prove the main result of this section.

THEOREM 1. *Suppose that $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ is symplectic modulo n. Then there is a symplectic matrix N such that $M \equiv N \pmod{n}$.*

Proof. By Lemma 2, there is a symmetric matrix X such that $\left(\det(A + XC), n\right) = 1$. Put

$$M_1 = \begin{bmatrix} I & X \\ 0 & I \end{bmatrix} M = \begin{bmatrix} A + XC & B + XD \\ C & D \end{bmatrix} = \begin{bmatrix} A_1 & B_1 \\ C & D \end{bmatrix}.$$

Then M_1 is also symplectic modulo n, and $(\det A_1, n) = 1$. Define α by $\alpha \det A_1 \equiv 1 \pmod{n}$. Then $-\alpha C A_1^{adj}$ is symmetric modulo n. By Lemma 1, there is a symmetric matrix Y such that $Y \equiv -\alpha C A_1^{adj} \pmod{n}$. Put

$$M_2 = \begin{bmatrix} I & 0 \\ Y & I \end{bmatrix} M_1 = \begin{bmatrix} A_1 & B_1 \\ YA_1 + C & YB_1 + D \end{bmatrix} = \begin{bmatrix} A_1 & B_1 \\ C_1 & D_1 \end{bmatrix}.$$

Then M_2 is symplectic modulo n, and

$$C_1 = YA_1 + C \equiv -\alpha C A_1^{adj} A_1 + C \equiv 0 \pmod{n}.$$

Similarly, there is a symmetric matrix Z such that

$$M_3 = M_2 \begin{bmatrix} I & Z \\ 0 & I \end{bmatrix} = \begin{bmatrix} A_1 & A_1 Z + B_1 \\ C_1 & C_1 Z + D_1 \end{bmatrix} = \begin{bmatrix} A_1 & B_2 \\ C_1 & D_2 \end{bmatrix}$$

where $B_2 \equiv 0 \pmod{n}$. Thus M_3 is symplectic modulo n and

$$M_3 \equiv \begin{bmatrix} A_1 & 0 \\ 0 & D_2 \end{bmatrix} \pmod{n}.$$

Now (as in the Smith normal form) determine unimodular matrices U, V such that $P = UA_1V$ is diagonal. Put

$$M_4 = \begin{bmatrix} U & 0 \\ 0 & U'^{-1} \end{bmatrix} M_3 \begin{bmatrix} V & 0 \\ 0 & V'^{-1} \end{bmatrix} \equiv \begin{bmatrix} UA_1V & 0 \\ 0 & U'^{-1}D_2V'^{-1} \end{bmatrix} \pmod{n}.$$

Then M_4 is symplectic modulo n and $M_4 \equiv \begin{bmatrix} P & 0 \\ 0 & Q \end{bmatrix} \pmod{n}$, where P is diagonal. Since $PQ' \equiv I \pmod{n}$, Q is congruent modulo n to a diagonal matrix. We have shown therefore that symplectic matrices R, S exist such that

$$M \equiv R \begin{bmatrix} P & 0 \\ 0 & Q \end{bmatrix} S \pmod{n},$$

where both P and Q are diagonal matrices. To complete the proof of the theorem it is only necessary to show that a symplectic matrix N_1 exists such that

$$N_1 \equiv \begin{bmatrix} P & 0 \\ 0 & Q \end{bmatrix} \pmod{n};$$

for then the matrix $N = RN_1S$ is also symplectic, and

$$N \equiv R \begin{bmatrix} P & 0 \\ 0 & Q \end{bmatrix} S \equiv M \pmod{n}.$$

But the existence of N_1 is guaranteed by Lemma 3, and so the proof of the theorem is complete.

3. Symplectic modulary groups. In this section m, n denote positive integers and

$$d = (m, n), \qquad \delta = [m, n].$$

LEMMA 4. *Suppose that $M \in \Gamma(d)$. Then Y can be determined so that $Y \in \Gamma(m)$, and*

$$Y \equiv M \pmod{n}. \tag{2}$$

Proof. Since $M \in \Gamma(d)$, we can write $M = I + dN$. Set $Y = I + mZ$. Then $Y \equiv I \pmod{m}$, and (2) becomes

$$mZ \equiv dN \pmod{n}, \qquad \frac{m}{d} Z \equiv N \left(\operatorname{mod} \frac{n}{d}\right).$$

Since $\left(\dfrac{m}{d}, \dfrac{n}{d}\right) = 1$, this has a solution Z_0. Thus there is a Y_0 such that

$$Y_0 \equiv I \pmod{m}, \qquad Y_0 \equiv M \pmod{n}.$$

Then Y_0 is symplectic modulo m and also modulo n; hence modulo δ. Thus Y can be determined so that $Y \equiv Y_0 \pmod{\delta}$ and Y is symplectic (Theorem 1). This Y satisfies the conditions of the lemma.

Lemma 4 now implies the following theorem.

THEOREM 2. *The normal subgroups $\Gamma(m)$, $\Gamma(n)$ of Γ satisfy*

$$\Gamma(m)\Gamma(n) = \Gamma(d), \tag{3}$$

$$\Gamma(m) \cap \Gamma(n) = \Gamma(\delta). \tag{4}$$

Proof. It is clear that $\Gamma(m)\Gamma(n) \subset \Gamma(d)$. Suppose that $M \in \Gamma(d)$. Determine Y as in Lemma 4. Then $Y \in \Gamma(m)$, $Y^{-1}M \in \Gamma(n)$ and $M = Y \cdot Y^{-1}M$. Hence $M \in \Gamma(m)\Gamma(n)$, $\Gamma(d) \subset \Gamma(m)\Gamma(n)$, and (3) is proved. Equation (4) is trivial.

In terms of the modulary groups $\mathfrak{M}(a, b) = \Gamma(a)/\Gamma(b)$, $a \mid b$, Theorem 2 implies by one of the isomorphism theorems

THEOREM 3. *We have the isomorphism*

$$\mathfrak{M}(d, m) \cong \mathfrak{M}(n, \delta). \tag{5}$$

It is now possible to follow the arguments in [2] without change to obtain the next three results:

THEOREM 4. *Let "$\times$" represent direct product. Then*

$$\mathfrak{M}(d, \delta) \cong \mathfrak{M}(d, m) \times \mathfrak{M}(d, n)$$

where $d = (m, n)$ and $\delta = [m, n]$.

THEOREM 5. *Suppose that m and n are arbitrary, $n = \prod_{p \mid n} p^{\beta_p}$. For each prime p dividing n write m as $m_p p^{\alpha_p}$, where $(m_p, p) = 1$ and $\alpha_p \geqslant 0$. Then $\mathfrak{M}(m, mn)$ is isomorphic to the direct product*

$$\prod_{p \mid n} \mathfrak{M}(p^{\alpha_p}, p^{\alpha_p + \beta_p}).$$

LEMMA 5. *If $n \mid m$ then $\mathfrak{M}(m, mn)$ is abelian.*

We now determine the structure of $\mathfrak{M}(m, mp^u)$ where p is a prime and $p^u \mid m$. Let E_{ij} be the matrix with 1 in position (i, j) and 0 elsewhere, and set

$$S_{ij} = \begin{cases} \begin{bmatrix} I & mE_{ii} \\ 0 & I \end{bmatrix}, & i = j, \\ \begin{bmatrix} I & m(E_{ij}+E_{ji}) \\ 0 & I \end{bmatrix}, & i < j, \end{cases}$$

$$W_{ij} = S'_{ij}, \tag{6}$$

$$R_{ij} = \begin{bmatrix} I + mE_{ij} & 0 \\ 0 & I - mE'_{ij} \end{bmatrix}.$$

There are $(t^2+t)/2$ matrices S_{ij}, $(t^2+t)/2$ matrices W_{ij}, and t^2 matrices R_{ij}. The matrices S_{ij}, W_{ij} are symplectic as are the matrices R_{ij}, $i \neq j$. The matrices R_{ii} are not symplectic but are symplectic modulo m^2 and so modulo mp^u, since $p^u \mid m$. This will suffice for our purposes, in view of Theorem 1.

We now prove

THEOREM 6. *Let p be a prime, $p^u \mid m$. Then $\mathfrak{M}(m, mp^u)$ is an abelian group of order $p^{u(2t^2+t)}$ and of type $(p^u, p^u, \ldots, p^u)$. The generators are given modulo mp^u by the matrices* (6).

Proof. By Lemma 5, $\mathfrak{M}(m, mp^u)$ is abelian. Suppose that

$$M = \begin{bmatrix} I+mA & mB \\ mC & I+mD \end{bmatrix} \epsilon \Gamma(m).$$

Then

$$D \equiv -A' \pmod{m}, \quad B \equiv B' \pmod{m}, \quad C \equiv C' \pmod{m}. \tag{7}$$

Since $p^u \mid m$, the congruences (7) also hold modulo p^u. By Lemma 1, symmetric matrices X, Y can be determined so that $X \equiv B \pmod{p^u}$, $Y \equiv C \pmod{p^u}$. Then

$$M \equiv \begin{bmatrix} I & mX \\ 0 & I \end{bmatrix} \begin{bmatrix} I & 0 \\ mY & I \end{bmatrix} \begin{bmatrix} I+mA & 0 \\ 0 & I-mA' \end{bmatrix} \pmod{mp^u}.$$

Now the matrices

$$\begin{bmatrix} I & mX \\ 0 & I \end{bmatrix}, \quad \begin{bmatrix} I & 0 \\ mY & I \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} I+mA & 0 \\ 0 & I-mA' \end{bmatrix}$$

can all be expressed modulo mp^u in an obvious way in terms of the matrices (6), so that these indeed generate $\Gamma(m)$ modulo $\Gamma(mp^u)$. Furthermore it is a simple computation to verify the independence of these generators modulo mp^u, each of which is of period p^u modulo $\Gamma(mp^u)$. The proof of the Theorem is concluded.

Making the choice $m = p^v$, we have

COROLLARY 1. *If $1 \leqslant u \leqslant v$ then $\mathfrak{M}(p^v, p^{u+v})$ is an abelian group of order $p^{u(2t^2+t)}$ and of type $(p^u, p^u, \ldots, p^u)$. The generators modulo $\Gamma(p^{u+v})$ may be chosen as the matrices* (6), *with $m = p^v$.*

Finally, Theorem 5 and Corollary 1 imply

THEOREM 7. *Suppose that $n \mid m$, $n = \prod_{p \mid n} p^{\beta_p}$. For each prime p dividing n write m as $m_p p^{\alpha_p}$, where $(m_p, p) = 1$. Then $1 \leqslant \beta_p \leqslant \alpha_p$ and $\mathfrak{M}(m, mn)$ is isomorphic to the direct product*

$$\prod_{p \mid n} \mathfrak{M}(p^{\alpha_p}, p^{\alpha_p+\beta_p}). \tag{8}$$

The direct factors in (8) *have the structure described in Theorem* 6.

References

[1] M. Newman and I. Reiner, *Inclusion theorems for congruence subgroups*, Trans. Amer. Math. Soc. 91(1959), pp. 369-379.

[2] M. Newman and J. R. Smart, *Modulary groups of $t \times t$ matrices*, Duke Math. J. 30(1963), pp. 253-257.

NATIONAL BUREAU OF STANDARDS, WASHINGTON, D. C.
and UNIVERSITY OF WISCONSIN, MADISON, WISCONSIN

Reçu par la Rédaction le 27. 6. 1963