TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 170, August 1972

m-SYMPLECTIC MATRICES

BY

EDWARD SPENCE

ABSTRACT. The symplectic modular group $\mathfrak{M}$ is the set of all $2n \times 2n$ matrices M with rational integral entries, which satisfy $MJM' = J$, $J = \left[\begin{smallmatrix} 0 & I \\ I & 0 \end{smallmatrix}\right]$, I being the identity $n \times n$ matrix. Let m be a positive integer. Then the $2n \times 2n$ matrix N is said to be *m-symplectic* if it has rational integral entries and if it satisfies $NJN' = mJ$. In this paper we consider canonical forms for m-symplectic matrices under left-multiplication by symplectic modular matrices (corresponding to Hermite's normal form) and under both left- and right-multiplication by symplectic modular matrices (corresponding to Smith's normal form). The number of canonical forms in each case is determined explicitly in terms of the prime divisors of m. Finally, corresponding results are stated, without proof, for 0-symplectic matrices; these are $2n \times 2n$ matrices M with rational integral entries and which satisfy $MJM' = M'JM = 0$.

1. **Introduction.** Canonical forms for $n \times n$ matrices with rational integral entries under the two equivalence relations of (i) premultiplying, and (ii) pre- and postmultiplying by unimodular matrices (i.e., matrices with rational integral entries and determinant unity) have been known for some time. These canonical forms are known as the Hermite and Smith normal form, respectively; an excellent account of the relevant elementary divisor theory is given in [1, pp. 32–43].

In this paper we define *m-symplectic matrices* and find canonical forms for them under premultiplication and both pre- and postmultiplication by *symplectic modular matrices*. Formulas for the number of canonical forms in each case have been found; in the second case the number is easy to find, while in the first, the solution is nontrivial and depends on the results of a previous paper [4].

It was only after these results were obtained that I discovered that H. Maass [2] and M. Sugawara [3] had already discussed these matrices (I am indebted to Professor Maass for bringing the existence of these papers to my attention). To them must go the credit for Theorem 2.1 below, which is expressed in a form slightly different from theirs.

2. **Canonical forms under left-multiplication.** Let Ω denote the set of all matrices with rational integral entries and let $J = \left[\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right]$ where I is the identity $n \times n$ matrix. The symplectic modular group $\mathfrak{M}$ is defined to be the set of matrices

Received by the editors May 7, 1971.

AMS 1970 *subject classifications*. Primary 15A21, 15A36, 10M20; Secondary 10A20.

Key words and phrases. Symplectic modular group, unimodular matrices, canonical forms, elementary divisor theory, multiplicative function.

$M = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$, where A, B, C and D are $n \times n$ matrices in Ω which satisfy

$$MJM' = J. \tag{2.1}$$

It is easily deduced from (2.1) that $M \in \mathfrak{M}$ if and only if

$$AB' = BA', \quad CD' = DC' \quad \text{and} \quad AD' - BC' = I. \tag{2.2}$$

Further, since $M \in \mathfrak{M}$ if and only if $M' \in \mathfrak{M}$, conditions (2.2) can be replaced by the equivalent ones:

$$A'C = C'A, \quad B'D = D'B \quad \text{and} \quad A'D - C'B = I. \tag{2.3}$$

Suppose now that A_1, B_1, C_1 and D_1 are $n \times n$ matrices in Ω and that m is a positive integer (the case $m = 0$ will be mentioned later). Call

$$M_1 = \begin{bmatrix} A_1 & B_1 \\ C_1 & D_1 \end{bmatrix}$$

m-symplectic if

$$M_1 J M_1' = mJ. \tag{2.4}$$

If the set of all such matrices M_1 is denoted by $\mathfrak{M}(m)$, then as in the derivation of (2.2) and (2.3), we have that $M = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right] \in \mathfrak{M}(m)$ if and only if either

$$AB' = BA', \quad CD' = DC' \quad \text{and} \quad AD' - BC' = mI, \tag{2.5}$$

or

$$A'C = C'A, \quad B'D = D'B \quad \text{and} \quad A'D - C'B = mI. \tag{2.6}$$

It is easy to verify that

$$N_1, N_2 \in \mathfrak{M}, \quad M \in \mathfrak{M}(m) \text{ imply } N_1 M N_2 \in \mathfrak{M}(m). \tag{2.7}$$

We now make the following definitions: Matrices M, $N \in \mathfrak{M}(m)$ are said to be *left-associated* if there exists $N_1 \in \mathfrak{M}$ such that $M = N_1 N$, and *equivalent* if there exist N_2, $N_3 \in \mathfrak{M}$ such that $M = N_2 N N_3$. Clearly the relations of being left-associated and of being equivalent are equivalence relations on $\mathfrak{M}(m)$. It is one of the objects of this paper to find a set of canonical forms for the relation of equivalence but to do this it is first necessary to consider the relation of being left-associated.

Let $\mathfrak{H}(m)$ denote the set of $2n \times 2n$ matrices of the form

$$\begin{bmatrix} Q_1 & m^{-1} S Q_2 \\ 0 & Q_2 \end{bmatrix}$$

where the $n \times n$ matrices Q_1, Q_2 and S satisfy the following conditions: Q_1, Q_2

and $S \in \Omega$, Q_1 is in Hermite's normal form and $\det Q_1 > 0$, $Q_1 Q_2' = mI$, $S = [s_{ij}]$ is symmetric, $0 \le s_{ij} < m$ $(1 \le i, j \le n)$ and $SQ_2 \equiv 0 \pmod m$. Then we have the following theorem:

Theorem 2.1. $\mathfrak{M}(m) = \mathfrak{M} \cdot \mathfrak{H}(m)$, *i.e. every m-symplectic matrix can be expressed uniquely as a product MH where* $M \in \mathfrak{M}$ *and* $H \in \mathfrak{H}(m)$.

The proof of this theorem may be found in [3] and in Satz 1 of [2].

In his paper [3], Sugawara observed that $\mathfrak{H}(m)$ is a finite set. However, more than this can be said, for it is possible to determine exactly the number of matrices in $\mathfrak{H}(m)$. It was shown in [4] that a necessary and sufficient condition for

$$AB' = mI, \tag{2.8}$$

with A and B $n \times n$ matrices in Ω, is that the Smith normal form of A be $\mathrm{diag}(d_1, d_2, \cdots, d_n)$ with $d_n \mid m$, i.e. there exist U and V in Γ (the group of all $n \times n$ matrices in Ω with determinant unity) such that $UAV = \mathrm{diag}(d_1, d_2, \cdots, d_n) = A^*$, say, where $d_{i-1} \mid d_i$ $(1 < i \le n)$ and $d_n \mid m$. It was also shown that the number of solutions A of (2.8) in Hermite's normal form and with positive determinant which have A^* as their Smith's normal form is $[\Gamma : A^{*-1}\Gamma A^* \cap \Gamma]$, the index of the subgroup $A^{*-1}\Gamma A^* \cap \Gamma$ in Γ. Call this number $N_n(d_1, d_2, \cdots, d_n)$ and let $h_n(m)$ denote the number of matrices in $\mathfrak{H}(m)$. Then in order to evaluate $h_n(m)$ it is clearly necessary, given A and B satisfying (2.8), to find how many distinct $\pmod m$ $n \times n$ symmetric $S \in \Omega$ there are such that $SB \equiv 0 \pmod m$. If, as above, $A^* = UAV = \mathrm{diag}(d_1, d_2, \cdots, d_n)$ is the Smith's normal form of A, then

$$\begin{aligned} SB \equiv 0 \pmod m &\Leftrightarrow B'S \equiv 0 \pmod m \\ &\Leftrightarrow V^{-1}B'U^{-1}USU' \equiv 0 \pmod m \\ &\Leftrightarrow B^*T \equiv 0 \pmod m \end{aligned}$$

where $T = USU' = [t_{ij}]$ is symmetric and $A^*B^* = mI$. Then $B^* = \mathrm{diag}(m/d_1, m/d_2, \cdots, m/d_n)$ and

$$\begin{aligned} B^*T \equiv 0 \pmod m &\Leftrightarrow t_{ij} \equiv 0 \pmod{\{d_i, d_j\}} \qquad (1 \le i, j \le n) \\ &\Leftrightarrow t_{ij} \equiv 0 \pmod{d_i} \qquad (1 \le i \le j \le n) \end{aligned}$$

since $d_i \mid d_j$ if $1 \le i \le j \le n$ and $t_{ij} = t_{ji}$. Thus the number of distinct $\pmod m$ symmetric T such that $B^*T \equiv 0 \pmod m$ is $(m/d_1)(m/d_2)^2 \cdots (m/d_n)^n$. Since, given U, T is uniquely determined by, and uniquely determines, S, it follows that the number of distinct $\pmod m$ symmetric S such that $SB \equiv 0 \pmod m$ is also $(m/d_1)(m/d_2)^2 \cdots (m/d_n)^n$. Combining the above results it is seen that the number of

$$\begin{bmatrix} A & m^{-1}SB \\ 0 & B \end{bmatrix} \in \mathfrak{H}(m),$$

where A has Smith's normal form $A^* = \operatorname{diag}(d_1, d_2, \cdots, d_n)$, is

$$N_n(d_1, d_2, \cdots, d_n) \prod_{j=1}^{n} (m/d_j)^j.$$

Thus

$$h_n(m) = m^{n(n+1)/2} \sum_{d_{i-1} \mid d_i \mid m} N_n(d_1, d_2, \cdots, d_n)/d_1 d_2^2 \cdots d_n^n. \tag{2.9}$$

To prove that $h_n(m)$ is multiplicative, i.e. that $h_n(m_1 m_2) = h_n(m_1)h_n(m_2)$ if $(m_1, m_2) = 1$, the following lemma is required:

Lemma 2.2. *If* $d_1 d_2 \cdots d_n = p_1^{\alpha(1)} p_2^{\alpha(2)} \cdots p_r^{\alpha(r)}$ ($p_1, p_2, \cdots, p_r$ *are distinct primes*) *and* $d_{i-1} \mid d_i$ $(1 < i \leq n)$, *then*

$$N_n(d_1, d_2, \cdots, d_n) = \prod_{i=1}^{r} N_n((d_1, p_i^{\alpha(i)}), \cdots, (d_n, p_i^{\alpha(i)})).$$

Proof. Let A be a solution of $AB = mI$ with $D = \operatorname{diag}(d_1, d_2, \cdots, d_n)$ Smith's normal form of A. Write $d = d_1 d_2 \cdots d_n$ so that $\det A = d$. Then as a result of Lemma 3 of [4], A can be expressed as a product $A = A_1 A_2 \cdots A_r$ where $\det A_i = p_i^{\alpha(i)}$ and $A_i B_i = mI$ ($B_i \in \Omega$, $1 \leq i \leq r$); in fact $B_i = A_{i+1} \cdots A_r B A_1 \cdots A_{i-1}$. Also, it is clear that D may be factorized as follows: $D = D_1 D_2 \cdots D_r$, where, for $1 \leq i \leq r$, $D_i = \operatorname{diag}((d_1, p_i^{\alpha(i)}), \cdots, (d_n, p_i^{\alpha(i)}))$ and $\det D_i = p_i^{\alpha(i)}$. In other words, there exist $U, V \in \Gamma$ such that

$$A_1 A_2 \cdots A_r = U D_1 D_2 \cdots D_r V. \tag{2.10}$$

From this we deduce that A_i has Smith's normal form D_i. For (2.10) implies that

$$\begin{aligned} p_1^{\alpha(1)}(A_2 \cdots A_r) &= \operatorname{adj} A_1 (U D_1 \cdots D_r V) \\ \Rightarrow p_1^{\alpha(1)}(A_2 \cdots A_r) \operatorname{adj}(D_2 \cdots D_r V) &= \operatorname{adj} A_1 \cdot U D_1 (d/p_1^{\alpha(1)}) \\ \Rightarrow \operatorname{adj} A_1 \cdot U D_1 &= p_1^{\alpha(1)} W, \qquad W \in \Omega, \end{aligned}$$

since $(p_1^{\alpha(1)}, d/p_1^{\alpha(1)}) = 1$. In fact, W is unimodular. This in turn implies that

$$U D_1 = A_1 W, \tag{2.11}$$

and consequently, A_1 has Smith's normal form D_1. Using (2.11) in (2.10) we obtain $A_2 \cdots A_r = W D_2 \cdots D_r V$, and repeated applications of the argument above prove that A_i has Smith's normal form D_i for $1 \leq i \leq r$.

Conversely, by Lemma 2 of [4], if $A_1, A_2, \cdots, A_r$ are such that $A_i B_i = mI$ for some $B_i \in \Omega$ ($1 \leq i \leq r$), and if A_i has Smith's normal form D_i, where $(\det D_i, \det D_j) = 1$ for $i \neq j$, then $A = A_1 A_2 \cdots A_r$ satisfies $AB = mI$ for some $B \in \Omega$, and A has Smith's normal form $D_1 D_2 \cdots D_r$.

Combining these two results proves the lemma.

Theorem 2.3. $h_n(m)$ *is multiplicative, i.e. if* $(m_1, m_2) = 1$ *then* $h_n(m_1 m_2) = h_n(m_1) h_n(m_2)$.

Proof. This follows almost immediately from Lemma 2.2. The proof is straightforward and is omitted. (See also [2] where an alternative proof is given.)

Theorem 2.4. *If p is a prime and s is a positive integer,*

$$h_n(p^s) = p^{sn(n+1)/2} \sum_{0 \le \alpha(1) \le \cdots \le \alpha(n) \le s} p^{e(\alpha)} \prod_{j=1}^{n} (1 - p^{-j}) \Big/ \prod_{i=1}^{k} \left\{ \prod_{j=1}^{r(i)} (1 - p^{-j}) \right\}$$

where $e(\alpha) = \sum_{j=1}^{n} (j - n - 1)\alpha(j)$ *and the dependence of the integers k and $r(i)$ on the n-tuple $(\alpha(1), \alpha(2), \cdots, \alpha(n))$ is given by*

$$(\alpha(1), \alpha(2), \cdots, \alpha(n)) \equiv \Big(\underbrace{a(1), \cdots, a(1)}_{r(1)\ \textit{factors}}, \underbrace{a(2), \cdots, a(2)}_{r(2)\ \textit{factors}}, \cdots, \underbrace{a(k), \cdots, a(k)}_{r(k)\ \textit{factors}} \Big),$$

$\alpha(1) = a(1) < a(2) < \cdots < a(k) = \alpha(n)$, $r(1) + r(2) + \cdots + r(k) = n$ *and* $r(i) \ge 1$ $(1 \le i \le k)$.

Proof. This is an immediate consequence of 2 above and Corollary 1 of [4] where it is shown that

$$p^{-c(\alpha)} N_n(p_1^{\alpha(1)}, p_2^{\alpha(2)}, \cdots, p_n^{\alpha(n)}) = \prod_{j=1}^{n} (1 - p^{-j}) \Big/ \prod_{i=1}^{k} \left\{ \prod_{j=1}^{r(i)} (1 - p^{-j}) \right\},$$

where $c(\alpha) = \sum_{j=1}^{n} (2j - n - 1)\alpha(j)$.

Thus the value of $h_n(m)$ can be calculated in a finite number of steps. For example, it is easy to show that

$$h_1(m) = \sum_{d \mid m} d$$

and

$$h_2(m) = \prod_{i=1}^{r} \{(p_i^{\alpha(i)+1} - 1)(p_i^{2\alpha(i)+3} + p_i^{2\alpha(i)+1} - p_i^{\alpha(i)+1} - 1)/(p_i - 1)(p_i^3 - 1)\}$$

when $m = p_1^{\alpha(1)} p_2^{\alpha(2)} \cdots p_r^{\alpha(r)}$. Unfortunately, for $n > 2$ the calculations involved are very complicated. However, a lower bound for $h_n(m)$ of a particularly simple form can be obtained. First we require a lemma.

Lemma 2.5. *If, for $k \ge 1$ and $n \ge 0$, polynomials $f_{nk}(x)$ are defined inductively by*

$$f_{nk}(x) = \sum_{r=0}^{n} \left\{ \prod_{j=1}^{n-r} \left(\frac{1 - x^{r+j}}{1 - x^j} \right) \right\} x^{r(r+1)/2} f_{r,k-1}(x),$$

and

$$f_{0k}(x) = f_{n0}(x) = 1,$$

then, for $0 \le x \le 1$ *and* $n \ge 1$,

$$f_{nk}(x) \ge (1 + x + \cdots + x^k)(1 + x^2 + \cdots + x^{2k}) \cdots (1 + x^n + \cdots + x^{nk}).$$

Proof. A simple induction argument shows that, if $0 \le r \le n$,

$$\sum_{1 \le i(1) < \cdots < i(r) \le n} x^{i(1)+\cdots+i(r)} = x^{r(r+1)/2} \prod_{j=1}^{n-r} \left(\frac{1 - x^{r+j}}{1 - x^j} \right), \tag{2.12}$$

where an empty summation and product are taken to be 1. It is immediate that

$$f_{n1}(x) = \sum_{r=0}^{n} \sum_{1 \le i(1) < \cdots < i(r) \le n} x^{i(1)+\cdots+i(r)} = (1 + x)(1 + x^2) \cdots (1 + x^n)$$

and the result is true for all $n \ge 1$ and $k = 1$. Now let $s_k(x) = 1 + x + \cdots + x^k$ and suppose that there exists $k > 1$ such that $f_{r,k-1}(x) \ge s_{k-1}(x) s_{k-1}(x^2) \cdots s_{k-1}(x^r)$ for all $r \ge 1$. Then, by (2.12),

$$s_k(x) s_k(x^2) \cdots s_k(x^n) = (1 + x s_{k-1}(x))(1 + x^2 s_{k-1}(x^2)) \cdots (1 + x^n s_{k-1}(x^n))$$

$$= \sum_{r=0}^{n} \sum_{1 \le i(1) < \cdots < i(r) \le n} x^{i(1)+\cdots+i(r)} s_{k-1}(x^{i(1)}) s_{k-1}(x^{i(2)}) \cdots s_{k-1}(x^{i(r)})$$

$$\le \sum_{r=0}^{n} \sum_{1 \le i(1) < \cdots < i(r) \le n} x^{i(1)+\cdots+i(r)} s_{k-1}(x) s_{k-1}(x^2) \cdots s_{k-1}(x^r)$$

$$\le \sum_{r=0}^{n} \sum_{1 \le i(1) < \cdots < i(r) \le n} x^{i(1)+\cdots+i(r)} f_{r,k-1}(x) = f_{nk}(x),$$

and the lemma is proved.

I am grateful to S. D. Cohen for suggesting the above proof.

Theorem 2.6. $h_n(m) \ge \sigma_1(m)\sigma_2(m) \cdots \sigma_n(m)$ *where* $\sigma_k(m) = \sum_{d \mid m} d^k$.

Proof. Write $g_n(p^k) = p^{-kn(n+1)/2} h_n(p^k)$ for p a prime. Using Theorem 2.4 it is readily shown that

$$g_n(p^k) = \sum_{r=0}^{n} \left\{ \prod_{j=1}^{n-r} \frac{1 - p^{-r-j}}{1 - p^{-j}} \right\} p^{-r(r+1)/2} g_r(p^{k-1}) \qquad (k > 0).$$

Take $x = 1/p$ in Lemma 2.5 so that $f_{nk}(1/p) = g_n(p^k)$. Then

$$h_n(p^k) = p^{kn(n+1)/2} g_n(p^k) \geq p^{kn(n+1)/2} s_k(1/p) s_k(1/p^2) \cdots s_k(1/p^n)$$
$$= \sigma_1(p^k)\sigma_2(p^k) \cdots \sigma_n(p^k).$$

The proof of the theorem now follows since $h_n(m)$ and $\sigma_i(m)$ are both multiplicative.

3. **Canonical forms under equivalence.** Having established in §2 a 'Hermite's normal form' for m-symplectic matrices it will now be shown that there is also a 'Smith's normal form'. More precisely, we have

Theorem 3.1. *$\mathfrak{M}(m) = \mathfrak{M}\mathfrak{D}(m)\mathfrak{M}$, where $E \in \mathfrak{D}(m)$ if and only if $E =$ diag $(d_1, d_2, \cdots, d_{2n})$, the diagonal entries satisfying the conditions $d_i \mid d_{i+1}$ $(1 \leq i < n)$, $d_j^2 \mid m$ $(1 \leq j \leq n)$ and $d_k d_{n+k} = m$, $d_k > 0$ $(1 \leq k \leq n)$.*

Proof. By Theorem 2.1, given $M = [\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}] \in \mathfrak{M}(m)$, there exists $M_1 \in \mathfrak{M}$ such that

$$M_1 M = \begin{bmatrix} D_1 & S_1 D_1'^{-1} \\ 0 & mD_1'^{-1} \end{bmatrix}$$

where S_1 is symmetric. It is readily verified that D_1 is a nonsingular greatest right common divisor of A and C.

As a first step in the proof of the theorem we show that by multiplication by suitable symplectic unimodular matrices we may assume that M is equivalent to a matrix of the form $[\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}]$ (the zero matrices being $n \times n$). First suppose that D_1' is a right divisor of $D_1^{-1}S_1$, so that $TD_1' = D_1^{-1}S_1$ for $T \in \Omega$ (in fact $T = D_1^{-1}S_1D_1'^{-1}$ is symmetric). Then $[\begin{smallmatrix} I & 0 \\ -T & I \end{smallmatrix}] \in \mathfrak{M}$ and

$$\begin{bmatrix} I & 0 \\ -T & I \end{bmatrix} M'M_1' = \begin{bmatrix} I & 0 \\ -T & I \end{bmatrix} \begin{bmatrix} D_1' & 0 \\ D_1^{-1}S_1 & mD_1^{-1} \end{bmatrix} = \begin{bmatrix} D_1' & 0 \\ 0 & mD_1^{-1} \end{bmatrix}$$

and, consequently,

$$M_1 M M_2 = \begin{bmatrix} D_1 & 0 \\ 0 & mD_1'^{-1} \end{bmatrix}, \quad \text{for } M_1, M_2 \in \mathfrak{M}.$$

If, however, D_1' is not a right divisor of $D_1^{-1}S_1$, there exists, as in the first stage of the theorem, $M_3 \in \mathfrak{M}$ such that

$$M_3 \begin{bmatrix} D_1' & 0 \\ D_1^{-1}S_1 & mD_1^{-1} \end{bmatrix} = \begin{bmatrix} D_2 & S_2 D_2'^{-1} \\ 0 & mD_2'^{-1} \end{bmatrix},$$

where S_2 is symmetric and D_2, being a greatest right common divisor of D_1' and $D_1^{-1}S_1$, is a *proper* right divisor of D_1'. Thus abs val det $D_2 <$ abs val det D_1 where

$$M_3M'M_1' = \begin{bmatrix} D_2 & S_2D_2'^{-1} \\ 0 & mD_2'^{-1} \end{bmatrix}.$$

If now D_2' is a right divisor of $D_2^{-1}S_2$, then, as above, there exist M_4, $M_5 \in \mathfrak{M}$ such that

$$M_4M'M_5 = \begin{bmatrix} D_2 & 0 \\ 0 & mD_2'^{-1} \end{bmatrix}.$$

On the other hand, if D_2' is not a right divisor of $D_2^{-1}S_2$ we repeat the argument given above with D_2' in place of D_1', and so on, to obtain a sequence of matrices $D_1, D_2, \cdots$ for which

(3.1) $\qquad$ abs val det $D_1 >$ abs val det $D_2 >$ abs val det $D_3 > \cdots$

and for which D_i' is not a right divisor of $D_i^{-1}S_i$ (S_i symmetric). Since the sequence (3.1) is a strictly decreasing sequence of positive integers, it must terminate. In other words, there exists D_k such that D_k' is a right divisor of $D_k^{-1}S_k$, and we obtain the existence of M_6, $M_7 \in \mathfrak{M}$ such that either

$$M_6MM_7 = \begin{bmatrix} D_k & 0 \\ 0 & mD_k'^{-1} \end{bmatrix}$$

or

$$M_6M'M_7 = \begin{bmatrix} D_k & 0 \\ 0 & mD_k'^{-1} \end{bmatrix}.$$

Thus, in either case, by transposition if necessary, we have shown that M is equivalent to a matrix of the form

$$\begin{bmatrix} P_1 & 0 \\ 0 & Q_1 \end{bmatrix}.$$

If $\hat{P}_1$ is the Smith's normal form of P_1, then there exist $U, V \in \Gamma$ such that $UP_1V = \hat{P}_1$, and since

$$\begin{bmatrix} U & 0 \\ 0 & U'^{-1} \end{bmatrix}, \begin{bmatrix} V & 0 \\ 0 & V'^{-1} \end{bmatrix} \in \mathfrak{M},$$

we have

$$\begin{bmatrix} U & 0 \\ 0 & U'^{-1} \end{bmatrix} \begin{bmatrix} P_1 & 0 \\ 0 & Q_1 \end{bmatrix} \begin{bmatrix} V & 0 \\ 0 & V'^{-1} \end{bmatrix} = \begin{bmatrix} \hat{P}_1 & 0 \\ 0 & m\hat{P}_1^{-1} \end{bmatrix}.$$

In other words M is equivalent to the matrix

$$\begin{bmatrix} \hat{P}_1 & 0 \\ 0 & m\hat{P}_1^{-1} \end{bmatrix}$$

where $\hat{P}_1 = \operatorname{diag}(p_1, p_2, \cdots, p_n)$, $p_{i-1} \mid p_i$ $(1 < i \leq n)$ and $p_n \mid m$.

Now let $K = [k_{jl}]$ be the $n \times n$ matrix defined by

$$k_{jl} = \begin{cases} 0 & \text{if } j \neq l, \\ 0 & \text{if } j = l = i, \\ 1 & \text{otherwise}. \end{cases}$$

Then $K^2 = K$, $(I - K)^2 = I - K$ and $\left[\begin{smallmatrix} K & I-K \\ K-I & K \end{smallmatrix}\right] \in \mathfrak{M}$. Also,

$$\begin{bmatrix} K & K - I \\ I - K & K \end{bmatrix} \begin{bmatrix} \hat{P}_1 & 0 \\ 0 & m\hat{P}_1^{-1} \end{bmatrix} \begin{bmatrix} K & I - K \\ K - I & K \end{bmatrix}$$

$$= \begin{bmatrix} K\hat{P}_1 + (I - K)m\hat{P}_1^{-1} & 0 \\ 0 & (I - K)\hat{P}_1 + mK\hat{P}_1^{-1} \end{bmatrix}$$

which is the diagonal matrix obtained from $\operatorname{diag}(p_1, \cdots, p_n, m/p_1, \cdots, m/p_n)$ by interchanging p_i and m/p_i. Because of this we may assume that $p_1^2 \leq m$.

Suppose now that $p_1 \nmid m/p_n$ (if this is not so, pass on to consider p_2 as will be described below) and interchange p_n and m/p_n as above. Then $\gcd(p_1, p_2, \cdots, p_{n-1}, m/p_n) = q_1 < p_1$ and there exist $U_1, V_1 \in \Gamma$ such that $U_1 \operatorname{diag}(p_1, p_2, \cdots, p_{n-1}, m/p_n)V_1 = \operatorname{diag}(q_1, q_2, \cdots, q_n)$, where $q_{i-1} \mid q_i$ $(1 < i \leq n)$. It is immediate that M is equivalent to the matrix

$\operatorname{diag}(q_1, \cdots, q_n, m/q_1, \cdots, m/q_n)$. If $q_1 \nmid m/q_n$ repeat the above argument, and so on, to obtain a sequence of positive divisors of p_1, $p_1 > q_1 > r_1 > \cdots$ which must terminate after a finite number of steps. Thus we will obtain an equivalent m-symplectic matrix

$$\begin{bmatrix} D & 0 \\ 0 & mD^{-1} \end{bmatrix}, \quad D = \operatorname{diag}(d_1, d_2, \cdots, d_n),$$

in which $d_{i-1} \mid d_i$ $(1 < i \leq n)$ and $d_1 \mid m/d_n$. Since $d_1 \mid d_n$ we also have $d_1^2 \mid m$.

We may now suppose that $d_2^2 \leq m$, for if not, replace it by m/d_2 which is divisible by d_1, and $(m/d_2)^2 \leq m$. Repeating the above argument with d_2 in place of p_1 we may also assume that $d_2 \mid m/d_n$, and hence that $d_2^2 \mid m$. Similarly for $d_3, \cdots, d_{n-1}$, so that it is valid to assume that $d_3^2 \mid m, \cdots, d_{n-1}^2 \mid m$. If $d_n^2 \mid m$ the theorem is proved; if not, $(d_n, m/d_n) = a_n < d_n$ and there exist integers x and y with $(x, y) = 1$ such that $d_n x + (m/d_n)y = a_n$. Let $A_3, A_4, B_3, B_4, C_3, C_4, D_3, D_4$ be the $n \times n$ diagonal matrices defined by

$$\begin{aligned} A_3 &= \operatorname{diag}(1, 1, \cdots, 1, x), & B_3 &= \operatorname{diag}(0, 0, \cdots, 0, y), \\ C_3 &= \operatorname{diag}(0, 0, \cdots, 0, -m/a_n d_n), & D_3 &= \operatorname{diag}(1, 1, \cdots, 1, d_n/a_n), \\ A_4 &= I, & B_4 &= \operatorname{diag}(0, 0, \cdots, 0, -my/a_n d_n), \\ C_4 &= \operatorname{diag}(0, 0, \cdots, 0, 1), & D_4 &= \operatorname{diag}(1, 1, \cdots, 1, x d_n/a_n). \end{aligned}$$

Then

$$\begin{bmatrix} A_3 & B_3 \\ C_3 & D_3 \end{bmatrix}, \begin{bmatrix} A_4 & B_4 \\ C_4 & D_4 \end{bmatrix} \in \mathfrak{M},$$

and it is easily checked that

$$\begin{bmatrix} A_3 & B_3 \\ C_3 & D_3 \end{bmatrix} \begin{bmatrix} D & 0 \\ 0 & mD^{-1} \end{bmatrix} \begin{bmatrix} A_4 & B_4 \\ C_4 & D_4 \end{bmatrix} = \begin{bmatrix} \hat{D} & 0 \\ 0 & m\hat{D}^{-1} \end{bmatrix}$$

where $\hat{D} = \operatorname{diag}(d_1, d_2, \cdots, d_{n-1}, a_n)$. Since $d_i \mid a_n$ $(1 \leq i < n)$ and $m/a_n = (m/a_n d_n)(d_n/a_n)a_n$, $a_n^2 \mid m$ and the theorem is proved.

It is immediate that this canonical form is unique. For if $D^+ = \operatorname{diag}(d_1, d_2, \cdots, d_n, d_{2n}, d_{2n-1}, \cdots, d_{n+1})$ is one form and $C^+ = \operatorname{diag}(c_1, c_2, \cdots, c_n, c_{2n}, c_{2n-1}, \cdots, c_{n+1})$ is another, D^+ has Smith's normal form $\operatorname{diag}(d_1, d_2, \cdots, d_n, d_{n+1}, \cdots, d_{2n})$ and C^+ has Smith's normal form $\operatorname{diag}(c_1, c_2, \cdots, c_n, c_{n+1}, \cdots, c_{2n})$. Thus $c_i = d_i$ $(1 \leq i \leq 2n)$, Smith's normal form being unique.

To evaluate $|\mathfrak{D}(m)|$, the number of distinct canonical forms under equivalence, it is only necessary to find the number of diagonal matrices $D = \operatorname{diag}(d_1, d_2, \cdots, d_n)$ where $d_{i-1} \mid d_i$ $(1 < i \leq n)$ and $d_i^2 \mid m$ $(1 \leq i \leq n)$. If $g_n(m)$ is this number, then clearly

$$g_n(m) = \sum_{d^2 \mid m} g_{n-1}(m/d^2).$$

Since $g_1(m) = \sum_{d^2 \mid m} 1 = \prod_{i=1}^{r}(1 + [\alpha(i)/2])$, where $m = q_1^{\alpha(1)} q_2^{\alpha(2)} \cdots q_r^{\alpha(r)}$ is the prime decomposition of m, $g_n(m)$ can be calculated in a finite number of steps. In fact, it is easily shown that $g_n(m) = \prod_{i=1}^{r}\binom{\beta(i)}{n}$, where $\beta(i) = [\alpha(i)/2] + n$.

4. **0-symplectic matrices.** In this section we state the corresponding results for *0-symplectic matrices* which are matrices M of size $2n \times 2n$ with integral entries and which satisfy $M'JM = MJM' = 0$. Corresponding to Theorems 3.1 and 2.1 we have

Theorem 4.1. *If $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ of rank r is 0-symplectic, then M is equivalent to a matrix of the form*

$$\begin{bmatrix} A_r & 0 \\ 0 & 0 \end{bmatrix},$$

where $A_r = \operatorname{diag}(a_1, a_2, \cdots, a_r, 0, \cdots, 0)$ is of size $n \times n$ and is in Smith's normal form. This form is unique.

Theorem 4.2. *If M, of size $2n \times 2n$, is 0-symplectic, there exists $M_1 \in \mathfrak{M}$ such that*

$$M_1 M = \begin{bmatrix} Q_1 & Q_2 \\ 0 & 0 \end{bmatrix},$$

where Q_1 is $n \times n$ and in Hermite's normal form.

The contents of the above paper formed part of a Ph. D. thesis presented in 1968 to the University of Glasgow; the author gratefully acknowledges the debt he owes to his supervisor Professor R. A. Rankin for his advice and encouragement.

REFERENCES

1. C. C. MacDuffee, *The theory of matrices*, Chelsea, New York, 1946.

2. H. Maass, *Die Primzahlen in der Theorie der Siegelschen Modulfunktionen*, Math. Ann. 124 (1951), 87–122. MR 13, 823.

3. M. Sugawara, *On the transformation theory of Siegel's modular group of the n-th degree*, Proc. Imp. Acad. Japan 13 (1937), 335–338.

4. E. Spence, *Matrix divisors of mI*, Acta Arith. 20 (1972).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GLASGOW, GLASGOW, W. 2., SCOTLAND