THE INDEX OF A SUBGROUP OF THE SYMPLECTIC MODULAR GROUP

Edward Spence

1. INTRODUCTION

Let Ω_n be the semigroup of all n-by-n matrices with rational integral entries, and let $\mathcal{M}_n$ denote the symplectic modular group of degree n; that is, let $\mathcal{M}_n$ be the group of all matrices $M \in \Omega_{2n}$ that satisfy the equation

$$M'JM = J, \tag{1}$$

where $J = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$, I being the identity n-by-n matrix. If $M \in \mathcal{M}_n$ is partitioned as $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ with $A, B, C, D \in \Omega_n$, it is easy to see that (1) is equivalent to the conditions

$$AB' = BA', \quad CD' = DC', \quad \text{and} \quad AD' - BC' = I. \tag{2}$$

A matrix $N \in \Omega_{2n}$ is called m-*symplectic* (m a positive integer) if it satisfies the condition

$$N'JN = mJ. \tag{3}$$

Denote the set of m-symplectic matrices by $\mathcal{M}_n(m)$, and call two matrices $M, N \in \mathcal{M}_n(m)$ *left-associated* if there exists an $M_1 \in \mathcal{M}_n$ such that $M = M_1 N$, and *equivalent* if there exist $M_2, M_3 \in \mathcal{M}_n$ such that $M = M_2 N M_3$. Clearly, the relations of being left-associated and of being equivalent are equivalence relations on $\mathcal{M}_n(m)$. In [5], the following two results were proved.

THEOREM 1. *An* m-*symplectic matrix is left-associated to exactly one matrix of the form*

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

where $Q_1, Q_2, S \in \Omega_n$, Q_1 *is in Hermite normal form,* $\det Q_1 > 0$, $Q_1 Q_2' = mI$, $S = [s_{ij}]$ *is symmetric,* $0 \le s_{ij} < m$ $(1 \le i, j \le n)$, *and* $SQ_2 \equiv 0 \pmod m$.

The Hermite normal form of a matrix in Ω_n is the unique form to which it can be reduced by premultiplication by a suitable $U \in \Omega_n$ with determinant unity. For a more detailed explanation, see [2, p. 32].

Received February 12, 1971.

This paper was written while the author was on leave of absence at the University of Illinois.

Michigan Math. J. 19 (1972).

THEOREM 2. *Every* m-*symplectic matrix is equivalent to exactly one matrix of the form*

$$\operatorname{diag}\{d_1, d_2, \cdots, d_{2n}\},$$

where

(4) $d_j > 0$ $(1 \leq j \leq 2n)$, $d_i \mid d_{i+1}$ $(1 \leq i < n)$, $d_k^2 \mid m$, and $d_k d_{n+k} = m$ $(1 \leq k \leq n)$.

The number of canonical forms in either case was also found in [5]. In the present paper, we obtain an alternate method of finding the number of canonical forms given in Theorem 1, by investigating certain subgroups of $\mathcal{M}_n$.

It is clear that if $M_1, M_2 \in \mathcal{M}_n(m)$ are left-associated, then they are also equivalent. Suppose, conversely, that $M_1, M_2 \in \mathcal{M}_n(m)$ are equivalent. Then there exist $U_1, U_2, V_1, V_2 \in \mathcal{M}_n$ such that

$$M_1 = U_1 D V_1, \qquad M_2 = U_2 D V_2,$$

where $D = \operatorname{diag}\{d_1, d_2, \cdots, d_{2n}\}$ satisfies conditions (4). Thus M_1 and M_2 are left-associated if and only if there exists $U \in \mathcal{M}_n$ such that the equivalent conditions

$$U_1 D V_1 = U U_2 D V_2, \qquad D^{-1}(U U_2)^{-1} U_1 D = V_2 V_1^{-1}, \qquad V_2 V_1^{-1} \in D^{-1} \mathcal{M}_n D \cap \mathcal{M}_n$$

are satisfied. Since $D^{-1}\mathcal{M}_n D \cap \mathcal{M}_n$ is a subgroup of $\mathcal{M}_n$, we can rephrase the third condition by saying that V_1 and V_2 belong to the same right coset of $D^{-1}\mathcal{M}_n D \cap \mathcal{M}_n$ in $\mathcal{M}_n$. Write

$$[\mathcal{M}_n : D^{-1}\mathcal{M}_n D \cap \mathcal{M}_n] = A_{2n}(d_1, d_2, \cdots, d_{2n}).$$

Then, for each set of positive integers $d_1, d_2, \cdots, d_{2n}$ satisfying (4), the number of matrices of the form UDV (with $U, V \in \mathcal{M}_n$) that are not left-associated is $A_{2n}(d_1, d_2, \cdots, d_{2n})$. Since nonequivalent matrices are not left-associated, we have the following result.

THEOREM 3. *Let* $h_n(m)$ *denote the number of canonical forms under the relation of being left-associated. Then*

$$h_n(m) = \sum A_{2n}(d_1, d_2, \cdots, d_{2n}),$$

where the summation is taken over all sets of positive integers $d_1, d_2, \cdots, d_{2n}$ *satisfying conditions* (4).

2. EVALUATION OF $h_n(m)$

It was shown in [5] that $h_n(m)$ is multiplicative, in other words, that $h_n(m_1 m_2) = h_n(m_1) h_n(m_2)$ if $(m_1, m_2) = 1$. It follows that to evaluate $h_n(m)$, we need only consider the case where $m = p^\alpha$ (p a prime). Here,

$$h_n(p^\alpha) = \sum A_{2n}(p^{\alpha_1}, p^{\alpha_2}, \cdots, p^{\alpha_{2n}}),$$

the summation being over all 2n-tuples $(\alpha_1, \alpha_2, \cdots, \alpha_{2n})$ of nonnegative integers satisfying the conditions

(5) $0 \leq \alpha_1 \leq \cdots \leq \alpha_n$, $2\alpha_i \leq \alpha$, and $\alpha_i + \alpha_{n+i} = \alpha$ $(1 \leq i \leq n)$.

Suppose therefore that E is the matrix diag $\{p^{\alpha_1}, p^{\alpha_2}, \cdots, p^{\alpha_{2n}}\}$ with $\alpha_1, \alpha_2, \cdots, \alpha_{2n}$ satisfying (5), and write K_n for the group $E^{-1}\mathcal{M}_n E \cap \mathcal{M}_n$. Also, let $\mathcal{M}_n[q]$ denote the *principal congruence subgroup* of $\mathcal{M}_n$ defined by

$$\mathcal{M}_n[q] = \{M \in \mathcal{M}_n : M \equiv I \pmod{q}\}.$$

It is well known [4, p. 58] that $\mathcal{M}_n[q]$ is a normal subgroup of $\mathcal{M}_n$ of finite index

$$[\mathcal{M}_n : \mathcal{M}_n[q]] = q^{n(2n+1)} \prod_{p \mid q} \prod_{k=1}^{n} (1 - p^{-2k}).$$

LEMMA 1. *If* $q = p^\beta$, *where* $\beta \geq \alpha$, *then* $\mathcal{M}_n[q] \subseteq K_n$.

The proof is entirely straightforward, and we omit it.

It is an immediate consequence of Lemma 1 that

$$[\mathcal{M}_n : K_n] = [\mathcal{M}_n : \mathcal{M}_n[q]] / [K_n : \mathcal{M}_n[q]]$$

when $q = p^\beta$ (as it will be throughout the remainder of the paper), and since $[\mathcal{M}_n : \mathcal{M}_n[q]]$ is known, the problem of determining

$$A_{2n}(p^{\alpha_1}, p^{\alpha_2}, \cdots, p^{\alpha_{2n}}) = [\mathcal{M}_n : K_n]$$

has been reduced to the evaluation of $[K_n : \mathcal{M}_n[q]]$. A matrix $M \in \Omega_{2n}$ is said to be *symplectic modulo* q if

$$M'JM \equiv J \pmod{q}.$$

If M is symplectic modulo q, then by Theorem 1 of [3] there exists an $N \in \mathcal{M}_n$ such that $N \equiv M \pmod{q}$.

LEMMA 2. $[K_n : \mathcal{M}_n[q]]$ *is the number of matrices* $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \Omega_{2n}$ *that are incongruent* (mod q) *and symplectic modulo* q, *and whose entries satisfy* (*in the obvious notation*) *the conditions*

$$(6) \qquad \begin{cases} a_{ij} \equiv 0 \pmod{p^{\alpha_j - \alpha_i}} & (1 \leq i \leq j \leq n), \\ b_{ij} \equiv 0 \pmod{p^{\alpha - \alpha_i - \alpha_j}} & (1 \leq i, j \leq n), \\ d_{ij} \equiv 0 \pmod{p^{\alpha_i - \alpha_j}} & (1 \leq j \leq i \leq n). \end{cases}$$

Proof. Suppose that $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \Omega_{2n}$ is symplectic modulo q and satisfies (6). Then there exists $N \in \mathcal{M}_n$ such that $N \equiv M \pmod{q}$. Since $\alpha_1, \alpha_2, \cdots, \alpha_n$ satisfy (5), it is easy to see that the entries of N also satisfy conditions (6), and by a simple exercise this implies that $N \in K_n$. To complete the proof, observe that $N_1, N_2 \in K_n$ lie in distinct cosets of $\mathcal{M}_n[q]$ in K_n if and only if $N_1 \not\equiv N_2 \pmod{q}$.

Let the set of matrices $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \Omega_{2n}$ that are symplectic modulo q and whose entries satisfy (6) be denoted by $L_n(\alpha; \alpha_1, \alpha_2, \cdots, \alpha_n)$, so that $M \in L_n(\alpha; \alpha_1, \alpha_2, \cdots, \alpha_n)$ implies the existence of an N in K_n such that $N \equiv M \pmod q$. Also, write $\ell_n(\alpha; \alpha_1, \alpha_2, \cdots, \alpha_n)$ for the number of matrices in $L_n(\alpha; \alpha_1, \alpha_2, \cdots, \alpha_n)$ that are incongruent (mod q). Then

$$\ell_n(\alpha; \alpha_1, \alpha_2, \cdots, \alpha_n) = [K_n : \mathcal{M}_n(q)],$$

by the lemma.

At this stage, assume that

$$(\alpha_1, \alpha_2, \cdots, \alpha_n) \equiv (\underbrace{a_1, \cdots, a_1}_{r_1 \text{ terms}}, \underbrace{a_2, \cdots, a_2}_{r_2 \text{ terms}}, \cdots, \underbrace{a_k, \cdots, a_k}_{r_k \text{ terms}}),$$

where $\alpha_1 = a_1 < a_2 < \cdots < a_k = \alpha_n$ and $r_1 + r_2 + \cdots + r_k = n$, $r_i \geq 1$.

THEOREM 4.

$$[K_n : \mathcal{M}_n[q]] = \begin{cases} q^{n(2n+1)} p^{-\alpha n(n+1)/2} \prod_{j=1}^{n} p^{2(n+1-j)\alpha_j} \prod_{i=1}^{k} \left\{ \prod_{j=1}^{r_i} (1 - p^{-j}) \right\} & \text{if } 2\alpha_n < \alpha, \\ q^{n(2n+1)} p^{-\alpha n(n+1)/2} \prod_{j=1}^{n} p^{2(n+1-j)\alpha_j} \prod_{i=1}^{k-1} \left\{ \prod_{j=1}^{r_i} (1 - p^{-j}) \right\} \cdot \prod_{j=1}^{r_k} (1 - p^{-2j}) & \\ \qquad \text{if } 2\alpha_n = \alpha. \end{cases}$$

Proof. Let $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in L_n(\alpha; \alpha_1, \alpha_2, \cdots, \alpha_n)$. Then, since

$$(a_{11}, \cdots, a_{1n}, b_{11}, \cdots, b_{1n}, q) = 1,$$

there exist integers $\lambda_1, \lambda_2, \cdots, \lambda_{2n}$ such that

$$\lambda_1 a_{11} + \cdots + \lambda_n a_{1n} + \lambda_{n+1} b_{11} + \cdots + \lambda_{2n} b_{1n} \equiv 1 \pmod q$$

with $(\lambda_1, q) = 1$ (see [1, Lemma 2]). Write

$$U_1 = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 & 0 \\ \lambda_2 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \lambda_{n-1} & 0 & \cdots & 1 & 0 \\ \lambda_n & 0 & \cdots & 0 & \lambda_1^{-1} \end{bmatrix},$$

where λ_1^{-1} is the inverse of $\lambda_1 \pmod q$, and let V_1 be a matrix such that $U_1 V_1' \equiv I \pmod q$. Such a matrix exists, since $\det U_1 \equiv 1 \pmod q$. Further, let

$$X \equiv \lambda_1^{-1} \begin{bmatrix} \lambda_{n+2} - \lambda_2 \\ \lambda_{n+3} - \lambda_3 \\ \cdots \\ \lambda_{2n} - \lambda_n \end{bmatrix} \pmod q,$$

and choose s so that

$$s \equiv \lambda_1^{-1}(\lambda_{n+1} - [\lambda_2, \lambda_3, \cdots, \lambda_n]X) \pmod q.$$

Then $S = \begin{bmatrix} s & X' \\ X & I \end{bmatrix}$ is symmetric and

$$SU_1 \equiv \begin{bmatrix} \lambda_{n+1} & \\ \lambda_{n+2} & \\ \cdots & * \\ \lambda_{2n} & \end{bmatrix} \pmod q.$$

It follows that $M_1 = \begin{bmatrix} U_1 & 0 \\ SU_1 & V_1 \end{bmatrix}$ is symplectic modulo q and

$$MM_1 \equiv \begin{bmatrix} 1 & * \\ * & * \end{bmatrix} \pmod q.$$

Note that since U_1 is a lower-triangular matrix, V_1 may be taken to be upper-triangular, and hence the entries of M_1 satisfy conditions (6); that is, $M_1 \in L_n(\alpha; \alpha_1, \alpha_2, \cdots, \alpha_n)$ and there exists an $M_2 \in K_n$ such that $M_2 \equiv M_1 \pmod q$. Thus

$$MM_2 \equiv \begin{bmatrix} 1 & * \\ * & * \end{bmatrix} \pmod q \qquad (M_2 \in K_n).$$

Suppose that the first row of MM_2 is congruent to

$$(1, a_{12}', \cdots, a_{1n}', b_{11}', \cdots, b_{1n}') \pmod q,$$

so that

$$(7) \qquad a_{1j}' \equiv 0 \pmod{p^{\alpha_j - \alpha_1}} \quad \text{and} \quad b_{1j}' \equiv 0 \pmod{p^{\alpha - \alpha_j - \alpha_1}}.$$

Let U_2 be the unimodular matrix

$$U_2 = \begin{bmatrix} 1 & -a'_{12} & \cdots & a'_{1n} \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{bmatrix},$$

and let $T = [t_{ij}] \in \Omega_n$ be the *symmetric* matrix defined by

$$t_{11} = -(b'_{11} + b'_{12}a'_{12} + \cdots + b'_{1n}a'_{1n}), \quad t_{1j} = -b'_{1j} \quad (1 < j \leq n),$$

$$t_{ij} = \delta_{ij} p^{\alpha - 2\alpha_j} \quad (1 < i, j \leq n) \quad (\delta_{ij} \text{ is the Kronecker delta}).$$

Then $M_3 = \begin{bmatrix} U_2 & U_2 T \\ 0 & U_2'^{-1} \end{bmatrix} \in \mathscr{M}_n$; in fact, careful examination shows that $M_3 \in K_n$; that is, the entries of M_3 satisfy condition (6). For if $U_2 T = [t'_{ij}]$, then

$$t'_{11} = -b'_{11}, \quad t'_{1j} = -b'_{1j} - a'_{1j} p^{\alpha - 2\alpha_j} \quad (1 < j \leq n), \quad t'_{i1} = -b'_{1i} \quad (1 < i \leq n),$$

$$t'_{ij} = \delta_{ij} p^{\alpha - 2\alpha_j} \quad (1 < i, j \leq n),$$

and as a result of (7) we easily see that $t'_{ij} \equiv 0 \pmod{p^{\alpha - \alpha_i - \alpha_j}}$ $(1 \leq i, j \leq n)$. We also see that the entries of U_2 and $U_2'^{-1}$ satisfy the required conditions. Hence $M M_2 M_3 \equiv \begin{bmatrix} 1 & 0 \\ * & * \end{bmatrix} \pmod q$, with $M_2 M_3 \in K_n$.

However, $M M_2 M_3$ is symplectic modulo q, and hence

$$(8) \qquad MM_4 \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ Z' & A_1 & 0 & B_1 \\ c & X & 1 & Y \\ W' & C_1 & 0 & D_1 \end{bmatrix} \pmod q,$$

where $M_4 = M_2 M_3 \in K_n$, $A_1, B_1, C_1, D_1 \in \Omega_{n-1}$, and X, Y, Z, W are row vectors of dimension n - 1. Since $MM_4 \in L_n(\alpha; \alpha_1, \alpha_2, \cdots, \alpha_n)$, it is readily verified that $\begin{bmatrix} A_1 & B_1 \\ C_1 & D_1 \end{bmatrix} \in L_{n-1}(\alpha; \alpha_2, \cdots, \alpha_n)$ and

$$(9) \qquad [X \;\; Y] \equiv [Z \;\; W] \begin{bmatrix} -C_1 & -D_1 \\ A_1 & B_1 \end{bmatrix} \pmod q;$$

in other words, X and Y are uniquely determined (mod q) by A_1, B_1, C_1, D_1, Z, and W.

An analysis of the construction of M_4 shows that it depends only on the *first* row of M, so that if the first row of $N \in L_n(\alpha; \alpha_1, \alpha_2, \cdots, \alpha_n)$ is congruent (mod q) to the first row of M, then $NM_4 \equiv \begin{bmatrix} 1 & 0 \\ * & * \end{bmatrix} \pmod q$. It follows that,

corresponding to each $\begin{bmatrix} A_1 & B_1 \\ C_1 & D_1 \end{bmatrix}$ in $L_{n-1}(\alpha; \alpha_2, \cdots, \alpha_n)$, each set of row vectors X, Y, Z, W of dimension n - 1 related by (9), and any preassigned first row of M, the other rows of M are uniquely determined (mod q). Thus

$$q^{2n-1}\, \ell_{n-1}(\alpha; \alpha_2, \cdots, \alpha_n) \tag{10}$$

is the number of incongruent (mod q) matrices in $L_n(\alpha; \alpha_1, \cdots, \alpha_n)$ whose first rows are congruent (mod q) (since there are q^{2n-1} choices for Z, W, and c).

We now examine the number of possible incongruent (mod q) choices of a first row of a matrix in $L_n(\alpha; \alpha_1, \cdots, \alpha_n)$. This is the number of 2n-tuples $(a_{11}, \cdots, a_{1n}, b_{11}, \cdots, b_{1n})$ of integers in a complete system of residues (mod q) such that

$$\begin{cases} (a_{11}, a_{12}, \cdots, a_{1n}, b_{11}, b_{12}, \cdots, b_{1n}, q) = 1 \\ \text{and} \\ a_{1j} \equiv 0 \pmod{p^{\alpha_j - \alpha_1}}, \quad b_{1j} \equiv 0 \pmod{p^{\alpha - \alpha_1 - \alpha_j}} \qquad (1 \le j \le n). \end{cases} \tag{11}$$

Case (i). $2\alpha_n < \alpha$.

Here $\alpha - \alpha_1 - \alpha_j \neq 0$ for any j, since $\alpha_1 + \alpha_j \le 2\alpha_n$, and it is obvious that (11) is satisfied if and only if $(a_{11}, \cdots, a_{ir_1}, q) = 1$ and

$$a_{1j} \equiv 0 \pmod{p^{\alpha_j - \alpha_1}}, \quad b_{1j} \equiv 0 \pmod{p^{\alpha - \alpha_1 - \alpha_j}} \qquad (1 \le j \le n).$$

Since the number of incongruent (mod q) solutions of $(a_{11}, \cdots, a_{1r_1}, q) = 1$ is $q^{r_1}(1 - p^{-r_1})$, it follows immediately that the number of incongruent (mod q) solutions of (11) is

$$q^{r_1}(1 - p^{-r_1}) \prod_{j > r_1} p^{\beta - \alpha_j + \alpha_1} \prod_{j=1}^{n} p^{\beta - \alpha + \alpha_1 + \alpha_j}.$$

We can simplify the last expression to

$$q^{2n}(1 - p^{-r_1}) p^{2n\alpha_1 - n\alpha}.$$

Thus, by (10),

$$\ell_n(\alpha; \alpha_1, \cdots, \alpha_n) = q^{4n-1}(1 - p^{-r_1}) p^{2n\alpha_1 - n\alpha}\, \ell_{n-1}(\alpha; \alpha_2, \cdots, \alpha_n),$$

and an easy induction argument proves the first part of the theorem.

Case (ii). $2\alpha_n = \alpha$.

The induction argument used above works until we reach the stage $\ell_{r_k}(\alpha; \alpha_n, \cdots, \alpha_n)$. Observe that when $2\alpha_1 = 2\alpha_2 = \cdots = 2\alpha_n = \alpha$, the number of solutions of (11) is precisely $q^{2n}(1 - p^{-2n})$. Thus, putting $n = r_k$, we obtain the formula

$$\ell_{r_k}(\alpha; \alpha_n, \cdots, \alpha_n) = q^{4r_k-1}(1 - p^{-2r_k})\,\ell_{r_k-1}(\alpha; \alpha_n, \cdots, \alpha_n)$$

$$= q^{r_k(2r_k+1)} \prod_{j=1}^{r_k} (1 - p^{-2j})$$

by induction. This completes the proof.

The following is an immediate consequence of Lemma 1 and Theorem 4.

COROLLARY 1.

$$[\mathcal{M}_n : K_n]$$

$$= \begin{cases} p^{\alpha n(n+1)/2} \prod_{j=1}^{n} p^{-2(n+1-j)\alpha_j} \dfrac{\prod_{j=1}^{n} (1 - p^{-2j})}{\prod_{i=1}^{k} \left\{ \prod_{j=1}^{r_i} (1 - p^{-j}) \right\}} & \text{if } 2\alpha_n < \alpha, \\ p^{\alpha n(n+1)/2} \prod_{j=1}^{n} p^{-2(n+1-j)\alpha_j} \dfrac{\prod_{j=1}^{n} (1 - p^{-2j})}{\prod_{j=1}^{r_k} (1 - p^{-2j}) \cdot \prod_{i=1}^{k-1} \left\{ \prod_{j=1}^{r_i} (1 - p^{-j}) \right\}} & \text{if } 2\alpha_n = \alpha. \end{cases}$$

Since $[\mathcal{M}_n : K_n] = A_{2n}(p^{\alpha_1}, p^{\alpha_2}, \cdots, p^{\alpha_{2n}})$ and

$$h_n(p^\alpha) = \sum A_{2n}(p^{\alpha_1}, p^{\alpha_2}, \cdots, p^{\alpha_{2n}}),$$

the summation being over all 2n-tuples $(\alpha_1, \alpha_2, \cdots, \alpha_{2n})$ of nonnegative integers satisfying (5), we can calculate $h_n(m)$ in a finite number of steps.

REFERENCES

1. N. J. Fine and I. Niven, *The probability that a determinant be congruent to* a (mod m). Bull. Amer. Math. Soc. 50 (1944), 89-93.

2. C. C. MacDuffee, *The theory of matrices.* Chelsea Publ. Co., New York, 1946.

3. M. Newman and J. R. Smart, *Symplectic modulary groups.* Acta Arith. 9 (1964), 83-89.

4. C. L. Siegel, *Symplectic geometry.* Amer. J. Math. 65 (1943), 1-86.

5. E. Spence, m-*symplectic matrices.* Trans. Amer. Math. Soc. (to appear).

University of Glasgow
Glasgow, Scotland