BULL. AUSTRAL. MATH. SOC. 37B05, 54H20
VOL. 71 (2005) [399–404]

THE DYNAMICS OF AN ACTION OF $Sp(2n, Z)$

ANTHONY NIELSEN

S.G. Dani and S. Raghavan showed the linear action of $Sp(2n, \mathbb{Z})$ on the space of symplectic p-frames for $p \leqslant n$ is topologically transitive. We give an alternative proof, from the prime number theorem and the congruence subgroup theorem, and show the action of every finite index subgroup of $Sp(2n, \mathbb{Z})$ is topologically transitive.

1. INTRODUCTION

Recall that the symplectic groups $Sp(2n, \mathbb{R})$ and $Sp(2n, \mathbb{Z})$ are the subgroups of $SL(2n, \mathbb{R})$ and $SL(2n, \mathbb{Z})$ respectively of matrices A which satisfy $A^t JA = J$ where

$$J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

A *Euclidean p-frame over* $\mathbb{R}^{2n}$ is a p-tuple $(u_1, \dots, u_p)$ of linearly independent vectors in $\mathbb{R}^{2n}$. For $1 \leqslant p \leqslant n$, a *symplectic p-frame* is a Euclidean p-frame which satisfies $u_i^t J u_j = 0$ for all i, j when the u_i are written as column vectors. The *space of symplectic p-frames* is the subset of $(\mathbb{R}^{2n})^p$ of all symplectic p-frames with the relative topology. An action of a group G on a topological space X is *topologically transitive* if for each $g \in G$ the bijection g on X is a homeomorphism and for each pair of nonempty open sets $U, V \subseteq X$ there is some $g \in G$ such that $gU \cap V \neq \emptyset$. The action is *topologically k-transitive* if the action induced on X^k is topologically transitive.

Dani and Raghavan ([5]), based on Moore's ergodicity theorem, showed the linear action of $SL(n, \mathbb{Z})$ on $\mathbb{R}^n$ is topologically $(n-1)$-transitive and the action of $Sp(2n, \mathbb{Z})$ on the space of symplectic p-frames is topologically transitive. Our main result is an alternative proof in the $Sp(2n, \mathbb{Z})$ case which applies to the finite index subgroups.

THEOREM 1. *For $p \leqslant n$, the linear action on the space of symplectic p-frames of every finite index subgroup of $Sp(2n, \mathbb{Z})$ is topologically transitive.*

The proof, in Section 4, is a modification of the one used in [4] to show the actions on $\mathbb{R}^n$ of the finite index subgroups of $SL(n, \mathbb{Z})$ are topologically $(n-1)$-transitive. Sections 2 and 3 introduce the underlying theorems, the prime number theorem modulo m and the congruence subgroup theorem.

Received 17th November, 2004

2. Dirichlet's theorem

Dirichlet's theorem on primes in arithmetic progressions says, provided $m \geqslant 2$ and a and m are relatively prime, there are infinitely many primes equal to a modulo m, and if, for $x > 0$, $\pi_m(x, a)$ is the number of primes $\leqslant x$ equal to a modulo m and φ is the Euler totient function, then

$$\lim_{x\to\infty} \frac{\pi_m(x,a)\log x}{x} = \frac{1}{\varphi(m)}.$$

See [**1**, Chapter 7]. An easy corollary is

$$\lim_{k\to\infty} \frac{p(k,a)}{k\log k} = \varphi(m)$$

where $p(k, a)$ denotes the kth prime equal to a modulo m.

The following argument is due to Mendès France in the Math Review of [**6**]. It shows the quotients of primes are dense in the positive reals (originally proved by Sierpiński in [**9**]). If $x > 0$ and $\lfloor kx \rfloor$ is the integer part of kx, since $\lim_{k\to\infty} \lfloor kx\rfloor/kx = \lim_{k\to\infty} \log\lfloor kx\rfloor/\log kx = 1$,

$$1 = \lim_{k\to\infty} \frac{p(\lfloor kx\rfloor, a)}{\varphi(m)kx\log kx}.$$

Therefore

$$x = \lim_{k\to\infty} \frac{p(\lfloor kx\rfloor, a)}{\varphi(m)k\log k + \varphi(m)k\log x} = \lim_{k\to\infty} \frac{p(\lfloor kx\rfloor, a)}{\varphi(m)k\log k} = \lim_{k\to\infty} \frac{p(\lfloor kx\rfloor, a)}{p(k,a)}.$$

Lemma 1. *Let U, V be nonempty open sets in $\mathbb{R}^l$. For each $m \geqslant 2$ and $1 \leqslant i \leqslant l$, $U \times V$ contains a point of the form*

$$\frac{(r_1, \dots, r_i, \dots, r_l; s_1, \dots, s_i, \dots, s_l)}{\varphi(m)k\log k}$$

where the r_j and s_j are each $\pm m$ times a prime—except for r_i and s_i which are just $\pm$ a prime and equal to 1 modulo m—and the primes are all distinct.

Proof: Choose a point $(x_1, \dots, x_{2n}; y_1, \dots, y_{2n})$ in $U \times V$ whose entries are all nonzero and distinct in absolute value. For the x_j other than x_i

$$\frac{|x_j|}{m} = \lim_{k\to\infty} \frac{p(\lfloor k|x_j|/m\rfloor, \pm 1)}{\varphi(m)k\log k},$$

where ± 1 agrees in sign with x_j, and likewise for the y_j other than y_i. For x_i and y_i similar equations hold but without $|x_i|$ or $|y_i|$ divided by m. For a sufficiently large k the primes in the numerators on the right are all distinct, and for a possibly larger k the quotients on the right, after those that correspond to negative x_j or y_j are multiplied by -1 and those that don't correspond to x_i or y_i are multiplied by m, form the desired $4n$-tuple in $U \times V$. ∎

3. The congruence subgroup theorem

Let ρ denote the maps $\mathbb{Z}^n \to \mathbb{Z}_m^n$ and $\mathbb{Z}^{n\times n} \to \mathbb{Z}_m^{n\times n}$ which reduce modulo m the entries of an n-tuple of integers and an $n \times n$ matrix of integers. For $n \geqslant 2$, the kernels of the group homomorphisms $\rho : SL(n,\mathbb{Z}) \to SL(n,\mathbb{Z}_m)$ are denoted $G_{n,m}$ and called the *principal congruence subgroups* of $SL(n,\mathbb{Z})$; a *congruence subgroup* is one which contains a principal congruence subgroup. The congruence subgroup theorem says, for $n \geqslant 3$, every finite index subgroup of $SL(n,\mathbb{Z})$ is a congruence subgroup. It was proved separately in [**3**] and [**8**]. A *principal congruence subgroup* of $Sp(2n,\mathbb{Z})$ is an intersection $Sp(2n,\mathbb{Z}) \cap G_{2n,m}$ for some m, and a *congruence subgroup* is one which contains a principal congruence subgroup. A version of the congruence subgroup theorem says that for $n \geqslant 2$ every finite index subgroup of $Sp(2n,\mathbb{Z})$ is a congruence subgroup ([**3**, Théorème 3]).

For $x \in \mathbb{Z}^n$ let $\gcd(x)$ mean the component-wise greatest common divisor. It is not difficult to show the orbit of x in $\mathbb{Z}^n$ under the obvious action of $SL(n,\mathbb{Z})$ is the $y \in \mathbb{Z}^n$ such that $\gcd(y) = \gcd(x)$. Humphreys in [**7**, Section 17.2] shows that the $G_{n,m}$-suborbit of x is the set of $y \in \mathbb{Z}^n$ such that $\gcd(y) = \gcd(x)$ and $\rho(y) = \rho(x)$.

4. Proof of the theorem

The following lemma is well known. See [**2**, Theorem 3.8].

Lemma 2. *Each symplectic p-frame $u = (u_1, \dots, u_p)$ forms the first p columns of some element in $Sp(2n,\mathbb{R})$.*

Proof: The vectors w which satisfy $w^t J u_i = 0$ for $1 \leqslant i \leqslant p$ make up the orthogonal complement of Ju relative to the standard inner product on $\mathbb{R}^{2n}$—a $(2n-p)$-dimensional subspace which contains u itself. Therefore, while $p < n$ we can extend u to a symplectic n-frame by induction.

If u is a symplectic n-frame, the orthogonal complement of $J(u_1, \dots, u_n)$ has dimension n and is contained in the orthogonal complement of $J(u_2, \dots, u_n)$ which has dimension $n+1$. So there is $u_{n+1} \in \mathbb{R}^{2n}$ with $u_{n+1}^t J u_1 = -1$ and $u_{n+1}^t J u_i = 0$ for $2 \leqslant i \leqslant n$. It must be that u_{n+1} is linearly independent of $u_1, \dots, u_n$, else $u_1^t J u_{n+1}$ would be zero. Now, the orthogonal complement of $J(u_1, \dots, u_{n+1})$ has dimension $n-1$ and is contained in the orthogonal complement of $J(u_1, u_3, \dots, u_{n+1})$ which has dimension n. So there is u_{n+2} with $u_{n+2}^t J u_2 = -1$ and $u_{n+2}^t J u_i = 0$ for $i = 1$ and $3 \leqslant i \leqslant n+1$ and linearly independent of $u_1, \dots, u_{n+1}$; and so on. Arranged as columns, $u_1, \dots, u_{2n}$ form an element in $Sp(2n,\mathbb{R})$. ∎

Lemma 3. *Let $u = (u_1, \dots, u_p)$ be a symplectic p-frame contained in an open set U of $(\mathbb{R}^{2n})^p$. Then there are p open sets U_i of $\mathbb{R}^{2n}$ with $u_i \in U_i$, $U_1 \times \cdots \times U_p \subseteq U$, and such that the following holds: if $1 \leqslant q < p$ and $w = (w_1, \dots, w_q)$ is a symplectic q-frame with $w_i \in U_i$ for each i, there is $w_{q+1} \in U_{q+1}$ which makes $(w_1, \dots, w_{q+1})$ a symplectic $(q+1)$-frame.*

https://doi.org/10.1017/S0004972700038399 Published online by Cambridge University Press

PROOF: We shall define a continuously differentiable function $f : (\mathbb{R}^{2n})^q \times \mathbb{R}^{2n} \to \mathbb{R}^{2n}$. Take an element in $Sp(2n,\mathbb{R})$ with $u_1,\ldots,u_q$ as its first q columns and then replace those columns with variable columns x_i, $1 \leqslant i \leqslant q$. Call the resulting matrix A. If y is another variable column, f takes $(x_1,\ldots,x_q;y)$ to

$$A^tJy + e_{n+q+1}$$

where e_{n+q+1} is the element in the usual basis for $\mathbb{R}^{2n}$. Notice $f(u_1,\ldots,u_q;u_{q+1}) = 0$ and the Jacobian

$$\frac{\partial(f_1,\ldots,f_{2n})}{\partial(y_1,\ldots,y_{2n})}$$

evaluated at $(u_1,\ldots,u_q;u_{q+1})$ is $\det A = 1$. Therefore, by the implicit function theorem, there is an open neighbourhood V of $(u_1,\ldots,u_q)$ in $(\mathbb{R}^{2n})^q$ and a continuously differentiable function $g : V \to \mathbb{R}^{2n}$ such that $g(u_1,\ldots,u_q) = u_{q+1}$ and

$$f\big(x_1,\ldots,x_q;g(x_1,\ldots,x_q)\big) = 0 \text{ for all } (x_1,\ldots,x_q) \in V.$$

Now choose open neighbourhoods U_i of each of the u_i of u sufficiently small that $U_1\times\cdots\times U_p \subseteq U$ and each $(x_1,\ldots,x_p) \in U_1\times\cdots\times U_p$ is a Euclidean p-frame. Set $q = p-1$ and let g be the function as above which takes $(u_1,\ldots,u_{p-1})$ to u_p. Make $U_1,\ldots,U_{p-1}$ smaller, if necessary, so that g maps $U_1\times\cdots\times U_{p-1}$ into U_p: if $(w_1,\ldots,w_{p-1})$ is a symplectic $(p-1)$-frame in $U_1\times\cdots\times U_{p-1}$, $\big(w_1,\ldots,w_{p-1};g(w_1,\ldots,w_{p-1})\big)$ is a symplectic p-frame. Next, set $q = p-2$ and repeat—this time make $U_1,\ldots,U_{p-2}$ smaller still, if necessary, so that the new g maps $U_1\times\cdots\times U_{p-2}$ into U_{p-1}. Once q reaches 1 the U_i will be as required. ∎

For the next lemma it helps to think of a symplectic matrix in terms of its columns. If $x \in \mathbb{R}^{2n}$ let $\underline{x}$ be the first half of x, that is, the first n-tuple, and $\overline{x}$ be the second. The product x^tJy can be written $\underline{x}\cdot\overline{y} - \overline{x}\cdot\underline{y}$. If $x_1,\ldots,x_{2n}$ are the columns of a matrix, it is symplectic if $\underline{x_i}\cdot\overline{x_j} - \overline{x_i}\cdot\underline{x_j}$ is 0 for $j > i$ except for $j = n+i$ when it must be 1. Alternatively, if the matrix in block form is $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, the conditions are $A^tC - C^tA = 0$, $A^tD - C^tB = I$, $B^tD - D^tB = 0$. In particular, $Sp(2,\mathbb{Z}) = SL(2,\mathbb{Z})$.

LEMMA 4. *Let $r = (r_1,\ldots,r_{2n})$ have the properties in the statement of Lemma 1 for some $i \leqslant n$, and assume also $r_{n+1},\ldots,r_{n+i-1} = 0$. Then there is a matrix in $Sp(2n,\mathbb{Z}) \cap G_{2n,m}$ with $e_1,\ldots,e_{i-1},r$ its first i columns.*

PROOF: First consider the case $i < n$; so $n \geqslant 2$. Let $k = n-(i-1)$ and

$$r = (\underline{r},\overline{r}) = (r_1,\ldots,r_i,\ldots,r_n,0,\ldots,0,r_{n+i},\ldots,r_{2n}).$$

The k-tuple $(r_i,\ldots,r_n)$ reduces modulo m to $(1,0,\ldots,0)$ and has gcd 1. Therefore, by Section 3, there is an element $A' \in G_{k,m}$ whose first column is $(r_i,\ldots,r_n)$. Use A'

to construct $A \in G_{n,m}$ with $e_1, \dots, e_{i-1} \in \mathbb{R}^n$ and $\underline{r}$ its first i columns. Let C be the symmetric matrix with ith column and row $A^t\overline{r}$ and zeros elsewhere. By the construction of A, the first $i-1$ entries of $A^t\overline{r}$ are zero, and

$$\begin{pmatrix} A & 0 \\ (A^{-1})^t C & (A^{-1})^t \end{pmatrix} \in Sp(2n, \mathbb{Z}) \cap G_{2n,m}$$

meets the requirements. Now consider the case $i = n$. Because (r_n, r_{2n}) reduces to $(1,0)$ and has gcd 1 there is $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_{2,m}$ with $a = r_n$ and $c = r_{2n}$. A matrix which meets the requirements is

$$\begin{pmatrix} 1 & & & r_1 & & & & \\ & 1 & & r_2 & & & 0 & \\ & & \ddots & \vdots & & & & \\ & & & r_n & -br_1 & -br_2 & \dots & b \\ & & & 0 & 1 & & & \\ & & & \vdots & & 1 & & \\ & 0 & & & & & \ddots & \\ & & & r_{2n} & -dr_1 & -dr_2 & \dots & d \end{pmatrix}.$$

□

The proof of the main theorem follows.

PROOF: Since $Sp(2, \mathbb{Z}) = SL(2, \mathbb{Z})$ the theorem for $n = 1$ is proved in [4]. For $n \geqslant 2$ it suffices to show the actions of the principal congruence subgroups of $Sp(2n, \mathbb{Z})$ are topologically transitive. Let $m \geqslant 2$ and $u = (u_1, \dots, u_p)$, $v = (v_1, \dots, v_p)$ be symplectic p-frames contained in open sets U, V respectively of $(\mathbb{R}^{2n})^p$. We are after a matrix in $Sp(2n, \mathbb{Z}) \cap G_{2n,m}$ which takes a symplectic p-frame in U to a symplectic p-frame in V. For $u \in U$ and $v \in V$ let U_i and V_i, $1 \leqslant i \leqslant p$, be the open sets of $\mathbb{R}^{2n}$ given by Lemma 3.

By Lemma 1, with $i = 1$ and $l = 2n$, there is a point of the form

$$\frac{(r_1, \dots, r_{2n}; s_1, \dots, s_{2n})}{\varphi(m) k \log k}$$

in $U_1 \times V_1$ with r_1 and s_1 equal to 1 modulo m and the other entries equal to 0 modulo m. Lemma 4 says there are $A_1, B_1 \in Sp(2n, \mathbb{Z}) \cap G_{2n,m}$ with $A_1 r = B_1 s = e_1$. If t_1 is the denominator above and $t_1 w_1 = (r_1, \dots, r_{2n})$, A_1 takes a symplectic 1-frame, $w_1 \in U_1$, to e_1/t_1. Likewise, B_1 takes a symplectic 1-frame in V_1 to e_1/t_1. We claim that the open sets $A_1 U_2$ and $B_1 V_2$ both meet the subspace $\{\, x \in \mathbb{R}^{2n} \mid x_{n+1} = 0 \,\}$. Indeed, by the choice of the U_i there is $w_2' \in U_2$ such that (w_1, w_2') is a symplectic 2-frame, and

$$0 = t_1 (A_1 w_1)^t J (A_1 w_2') = e_1^t J (A_1 w_2') = (A_1 w_2')_{n+1};$$

and similarly for $B_1 V_2$.

https://doi.org/10.1017/S0004972700038399 Published online by Cambridge University Press

Next, using Lemma 1 again, with $i = 2$ and $l = 2n - 1$, choose a point of the above form in $A_1U_2 \times B_1V_2$, this time with r_2 and s_2 equal to 1 modulo m, $r_{n+1} = s_{n+1} = 0$, and the other entries equal to 0 modulo m. Let t_2 be the denominator. By Lemma 4 there are $A_2, B_2 \in Sp(2n, \mathbb{Z}) \cap G_{2n,m}$ which fix e_1 and with $A_2r = B_2s = e_2$. If $t_2A_1w_2 = (r_1, \ldots, r_{2n})$ this time, (w_1, w_2) is a symplectic 2-frame in $U_1 \times U_2$: A_2A_1 takes it to $(e_1/t_1, e_2/t_2)$. Likewise, B_2B_1 takes a symplectic 2-frame in $V_1 \times V_2$ to $(e_1/t_1, e_2/t_2)$. Again, there is $w_3' \in U_3$ such that (w_1, w_2, w_3') is a symplectic 3-frame. It follows that $A_2A_1U_3$ meets the subspace $\{\, x \in \mathbb{R}^{2n} \mid x_{n+1} = x_{n+2} = 0 \,\}$, and the same is true of $B_2B_1V_3$.

In the next step we choose a point of the above form in $A_2A_1U_3 \times B_2B_1V_3$, and so on. We get A_3 and B_3 such that $A_3A_2A_1$ and $B_3B_2B_1$ take symplectic 3-frames in $U_1 \times U_2 \times U_3$ and $V_1 \times V_2 \times V_3$ respectively to $(e_1/t_1, e_2/t_2, e_3/t_3)$. The process continues till we get A_p, B_p. The matrix we are after is $B_1^{-1} \cdots B_p^{-1} A_p \cdots A_1$; it takes $(w_1, \ldots, w_p) \in U_1 \times \cdots \times U_p$ to a symplectic p-frame in $V_1 \times \cdots \times V_p$. $\square$

References

[1] T.M. Apostol, *Introduction to analytic number theory* (Springer-Verlag, New York, 1976).

[2] E. Artin, *Geometric algebra* (Interscience Publishers, Inc., New York-London, 1957).

[3] H. Bass, M. Lazard, and J.-P. Serre, 'Sous-groupes d'indice fini dans $\mathbf{SL}(n, \mathbf{Z})$', *Bull. Amer. Math. Soc.* **70** (1964), 385–392.

[4] G. Cairns and A. Nielsen, 'On the dynamics of the linear action of SL(n,Z)', *Bull. Austral. Math. Soc.* **71** (2005), 359–365.

[5] S.G. Dani and S. Raghavan, 'Orbits of Euclidean frames under discrete linear groups', *Israel J. Math.* **36** (1980), 300–320.

[6] D. Hobby and D.M. Silberger, 'Quotients of primes', *Amer. Math. Monthly* **100** (1993), 50–52.

[7] J.E. Humphreys, *Arithmetic groups*, Lecture Notes in Mathematics **789** (Springer-Verlag, Berlin, 1980).

[8] J.L. Mennicke, 'Finite factor groups of the unimodular group', *Ann. of Math. (2)* **81** (1965), 31–37.

[9] W. Sierpiński, *Elementary theory of numbers*, Monografie Matematyczne **42** (Państwowe Wydawnictwo Naukowe, Warsaw, 1964).

Department of Mathematics
La Trobe University
Melbourne
Australia 3086
e-mail: A.Nielsen@latrobe.edu.au