BULL. AUSTRAL. MATH. SOC. 37B05, 54H20
VOL. 71 (2005) [359–365]

ON THE DYNAMICS OF THE LINEAR ACTION OF $SL(n, Z)$.

GRANT CAIRNS AND ANTHONY NIELSEN

Using Moore's ergodicity theorem, S.G. Dani and S. Raghavan proved that the linear action of $SL(n,\mathbb{Z})$ on $\mathbb{R}^n$ is topologically $(n-1)$-transitive; that is, topologically transitive on the Cartesian product of $n-1$ copies of $\mathbb{R}^n$. In this paper, we give a more direct proof, using the prime number theorem. Further, using the congruence subgroup theorem, we generalise the result to arbitrary finite index subgroups of $SL(n,\mathbb{Z})$.

1. INTRODUCTION

Recall that a continuous action of an abstract group G on a topological space X is *topologically transitive* if for all non-empty open sets $U, V \subseteq X$, there exists $g \in G$ such that $g(U) \cap V \neq \emptyset$. (By *continuous action* we mean that for each group element g, the corresponding map $g : X \to X$ is a homeomorphism). For many spaces (for example, second countable Baire spaces), this is equivalent to the existence of a dense orbit. For a natural number k, the action is said to be *topologically k-transitive* if the induced action of G on the k-fold Cartesian product X^k is topologically transitive. So topologically 1-transitive = topologically transitive, and topologically i-transitive $\Rightarrow$ topologically j-transitive for all $j < i$. Topological 2-transitivity is also called *weak topological mixing*.

The linear action of $SL(n,\mathbb{Z})$ on $\mathbb{R}^n$ in not topologically n-transitive, since the determinant is an invariant function on $(\mathbb{R}^n)^n$. S. G. Dani and S. Raghavan proved the following:

THEOREM. ([2]) *For all $n \geqslant 2$, the linear action of $SL(n,\mathbb{Z})$ on $\mathbb{R}^n$ is topologically $(n-1)$-transitive.*

Underlying the Dani–Raghavan result is Moore's ergodicity theorem. The object of this paper is to give an alternate, more direct proof of the Dani–Raghavan theorem, and to generalise it as follows:

THEOREM. *For all $n \geqslant 2$, the linear action on $\mathbb{R}^n$ of every finite index subgroup of $SL(n,\mathbb{Z})$ is topologically $(n-1)$-transitive.*

Received 25th August, 2004
We thank Pierre de la Harpe for his valuable comments and useful references.

Our proof uses the prime number theorem modulo m (see Section 2) and the congruence subgroup theorem; recall that the *principal congruence subgroups* of $SL(n, \mathbb{Z})$ are the kernels of the natural homomorphisms $SL(n, \mathbb{Z}) \to SL(n, \mathbb{Z}_m)$, and a *congruence subgroup* is a subgroup which contains a principal congruence subgroup. The congruence subgroup theorem ([**1**, **6**]) says that for $n > 2$, every finite index subgroup of $SL(n, \mathbb{Z})$ is a congruence subgroup. The main point in our proof is as follows.

Lemma 1. *For all $n \geqslant 2$, the linear action of every principal congruence subgroup of $SL(n, \mathbb{Z})$ on $\mathbb{R}^n$ is topologically $(n-1)$-transitive.*

The orbits on $\mathbb{Z}^n$ of the principal congruence subgroups are examined in Section 3 and Lemma 1 is established in Section 4. Lemma 1, together with the congruence subgroup theorem, establishes the theorem for all $n > 2$. The proof of the theorem is concluded in Section 5, where we show that the action of every finite index subgroup of $SL(2, \mathbb{Z})$ is topologically transitive.

We assume throughout the paper that $n \geqslant 2$. We use the same symbol ρ for each of the canonical projections $\mathbb{Z}^i \to \mathbb{Z}^i_m$ and for the natural homomorphism $SL(n, \mathbb{Z}) \to SL(n, \mathbb{Z}_m)$. We use I_n for the $n \times n$ identity matrix in both $SL(n, \mathbb{Z})$ and $SL(n, \mathbb{Z}_m)$.

2. A little number theory

Recall that the set of numbers of the form q/p, where p and q are prime, is dense in the positive reals; this was proved by Sierpiński in [**7**, p. 155] and Hobby and Silberger in [**3**]. In the Math Review of [**3**], Mendès France gave the following simple proof: it is a well known consequence of the prime number theorem that as k goes to infinity, the k-th prime p_k is approximately $k \log k$; more precisely, $\lim_{k\to\infty} p_k/(k \log k) = 1$. Thus for $x > 0$, one has

$$1 = \lim_{k\to\infty} \frac{p_{\lfloor kx \rfloor}}{\lfloor kx \rfloor \log \lfloor kx \rfloor} = \lim_{k\to\infty} \frac{p_{\lfloor kx \rfloor}}{kx \log kx},$$

and so

$$x = \lim_{k\to\infty} \frac{p_{\lfloor kx \rfloor}}{k \log kx} = \lim_{k\to\infty} \frac{p_{\lfloor kx \rfloor}}{k \log x + k \log k} = \lim_{k\to\infty} \frac{p_{\lfloor kx \rfloor}}{k \log k} = \lim_{k\to\infty} \frac{p_{\lfloor kx \rfloor}}{p_k},$$

where $\lfloor y \rfloor$ denotes the integer part of y.

We shall require an extension of Sierpiński's result. First recall the following result which was established by de la Vallée-Poussin (see for example [**5**]). For an integer $m \geqslant 2$, let $\pi_m(x, a)$ denote the number of primes $\leqslant x$ which are congruent to a modulo m.

Prime Number Theorem Modulo m. *For all $m \geqslant 2$, if a and m are relatively prime, then*

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

where φ is the Euler totient function.

Fix relatively prime integers $m \geqslant 2$ and a. Let $p(k,a)$ denote the k-th prime that is congruent to a modulo m. Setting $x = p(k,a)$ (so $\pi_m(x,a) = k$), the Prime Number Theorem Modulo m gives

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

Therefore

$$\begin{aligned} 0 &= \lim_{k\to\infty} \frac{\log\varphi(m) + \log k + \log\log p(k,a) - \log p(k,a)}{\log p(k,a)} \\ &= \lim_{k\to\infty} \frac{\log k}{\log p(k,a)} - 1. \end{aligned}$$

Hence, using (1) again,

$$\lim_{k\to\infty} \frac{p(k,a)}{k\log k} = \varphi(m). \tag{2}$$

Let $y > 0$. Imitating Mendès France's argument, equation (2) gives

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

and so

$$\begin{aligned} y &= \lim_{k\to\infty} \frac{p(\lfloor ky\rfloor,a)}{\varphi(m)k\log k + \varphi(m)k\log y} \\ &= \lim_{k\to\infty} \frac{p(\lfloor ky\rfloor,a)}{\varphi(m)k\log k}. \end{aligned}$$

To draw the conclusion that we shall require later, we need some notation. For each $i = 1,\ldots,n-1$, let X_i be the set of points $(x_1,\ldots,x_n) \in \mathbb{Z}^n$ such that:

1. x_i is congruent to 1 modulo m,
2. x_j is congruent to 0 modulo m for all $j \neq i$,
3. x_i and x_{i+1} are relatively prime.

LEMMA 2. *For each $i = 1,\ldots,n-1$, the set of points of the form $(x,y)/s$, where $s \in \mathbb{N}$, $x,y \in X_i$, is dense in $\mathbb{R}^{2n}$.*

PROOF: Let z_1, z_2 be nonzero reals. Set $w_1 = z_1, w_2 = z_2/m$, and for $i = 1,2$ set

$$a_{i,k} = \begin{cases} p(\lfloor kw_i\rfloor,1); & \text{if } w_i \geqslant 0 \\ -p(\lfloor -kw_i\rfloor,-1); & \text{otherwise.} \end{cases}$$

Arguing as above,

$$(w_1,w_2) = \lim_{k\to\infty} \frac{1}{\varphi(m)k\log k}(a_{1,k},a_{2,k}),$$

https://doi.org/10.1017/S0004972700038351 Published online by Cambridge University Press

and so

$$(z_1, z_2) = \lim_{k\to\infty} \frac{1}{\varphi(m)k\log k}(a_{1,k}, ma_{2,k}).$$

Here $a_{1,k}$ is congruent to 1 modulo m, and $ma_{2,k}$ is congruent to 0 modulo m. Moreover, provided $|w_1|$ and $|w_2|$ are distinct, $a_{1,k}$ and $ma_{2,k}$ are relatively prime. Thus, it is not difficult to see that since the denominator $\varphi(m)k\log k$ is independent of z_1, z_2, the required result holds in the case $n = 2$. The result for arbitrary n then follows easily. ∎

3. The orbits of the principal congruence subgroups

We remark that, although we won't use this fact, it is not difficult to show that the greatest common divisor function is a complete invariant for the linear action of $SL(n,\mathbb{Z})$ on $\mathbb{Z}^n$. The description of the orbits of the principal congruence subgroups require more work; we limit ourselves here to giving a result that we need for the proof of the theorem (see [**4**, Chapter 17] for more details). Let m be a natural number and consider the natural homomorphism $\rho : SL(n,\mathbb{Z}) \to SL(n,\mathbb{Z}_m)$. Let $G_{n,m}$ denote the principal congruence subgroup $\ker\rho$. Put $S_1 = SL(n,\mathbb{Z})$ and for each $2 \leqslant k \leqslant n-1$, let S_k be the subgroup of $SL(n,\mathbb{Z})$ of elements having the block form

$$A = \begin{pmatrix} I_{k-1} & B \\ 0 & C \end{pmatrix}$$

where $C \in SL(n-k+1,\mathbb{Z})$ and B is arbitrary. For each $1 \leqslant k \leqslant n-1$, let $G_k = S_k \cap G_{n,m}$. Let $\{e_1, \dots, e_n\}$ be the usual basis for $\mathbb{Z}^n$.

Lemma 3. *Let $m \geqslant 2$ and let $1 \leqslant i \leqslant n-1$. If $x = (x_1, \dots, x_n) \in X_i$, then there exists $A \in G_i$ such that $Ax = e_i$.*

Proof: First consider the case $n = 2$, with $i = 1$. We have $\gcd(x) = 1$ and $\rho x = (1,0)$. Let

$$C' = \begin{pmatrix} a & b \\ -x_2 & x_1 \end{pmatrix}$$

where $ax_1 + bx_2 = 1$. In $SL(2,\mathbb{Z}_m)$, $\rho C'$ has the form $\begin{pmatrix} 1 & \widehat{b} \\ 0 & 1 \end{pmatrix}$ where $0 \leqslant \widehat{b} \leqslant m-1$. So

$$B = \begin{pmatrix} 1 & -\widehat{b} \\ 0 & 1 \end{pmatrix} \in SL(2,\mathbb{Z})$$

satisfies $\rho(BC') = I_2$. Denote BC' by $C_{(x_1,x_2)}$; it belongs to G_1 and takes x to e_1, as required.

For $n > 2$, consider the matrix

$$C = \begin{pmatrix} I_{i-1} & & 0 \\ & C_{(x_i,x_{i+1})} & \\ 0 & & I_{n-i-1} \end{pmatrix} \in G_i.$$

https://doi.org/10.1017/S0004972700038351 Published online by Cambridge University Press

C takes $(x_1, \dots, x_n)$ to $(x_1, \dots, x_{i-1}, 1, 0, x_{i+2}, \dots, x_n)$. Let $F = (f_{jk})$ be the $n \times n$ matrix with

$$f_{jk} = \begin{cases} -x_j; & k = i, j \neq i, i+1 \\ 0; & \text{otherwise,} \end{cases}$$

and let $E = I_n + F$ and $A = EC$. Clearly, $E \in G_i$, so $A \in G_i$. And by construction, $Ax = e_i$. ∎

4. Proof of Lemma 1

Consider nonempty open sets U_i, V_i, $i \in \{1, \dots, n-1\}$ in $\mathbb{R}^n$. By Lemma 2, the open set $U_1 \times V_1 \subseteq \mathbb{R}^{2n}$ contains a point of the form $(x_1, y_1)/s_1$, where $s_1 \in \mathbb{N}$ and $x_1, y_1 \in X_1$. So by Lemma 3, there are $A_1, B_1 \in G_1$ with $A_1 x_1 = B_1 y_1 = e_1$. That is,

$$e_1/s_1 \in (A_1 U_1) \cap (B_1 V_1).$$

Next, by Lemma 2, pick $(x_2, y_2)/s_2 \in A_1 U_2 \times B_1 V_2$ so that $s_2 \in \mathbb{N}$ and $x_2, y_2 \in X_2$. Applying Lemma 3 again, there are $A_2, B_2 \in G_2$ with

$$e_2/s_2 \in (A_2 A_1 U_2) \cap (B_2 B_1 V_2).$$

Continue until we have

$$e_{n-1}/s_{n-1} \in (A_{n-1} \dots A_2 A_1 U_{n-1}) \cap (B_{n-1} \dots B_2 B_1 V_{n-1}).$$

Since $A_j, B_j \in G_j$ for all $j \in \{1, \dots, n-1\}$, the A_j and B_j all fix e_i, for all $j > i$. Therefore, for all $i \in \{1, \dots, n-1\}$, we have

$$e_i/s_i \in A_{n-1} \dots A_{i+1}(A_i \dots A_2 A_1 U_i) \cap B_{n-1} \dots B_{i+1}(B_i \dots B_2 B_1 V_i).$$

Multiplying on the left by $B_1^{-1} \dots B_{n-1}^{-1}$ we see that $DU_i \cap V_i \neq \emptyset$ for all $i \in \{1, \dots, n-1\}$, where

$$D = B_1^{-1} B_2^{-1} \dots B_{n-1}^{-1} A_{n-1} \dots A_2 A_1 \in G_{n,m}.$$

Hence the action of $G_{n,m}$ is $(n-1)$-transitive.

5. Proof of theorem for $n = 2$

Let G be a finite index subgroup of $SL(2, \mathbb{Z})$, and let U_1, U_2 be nonempty open subsets of $\mathbb{R}^2$. We shall show that there exists $g \in G$ such that $g(U_1) \cap U_2 \neq \emptyset$. The idea is to construct parabolic matrices $P_1, P_2 \in G$ and a point v close to the origin such that $P_i(v) \in U_i$ for each i. Then the matrix $g = P_2 P_1^{-1}$ does the job. See Figure 1.

First note that replacing G by its core if necessary, we may assume that G is a normal subgroup of $SL(2, \mathbb{Z})$. Second, since G has finite index, there exists a positive

https://doi.org/10.1017/S0004972700038351 Published online by Cambridge University Press

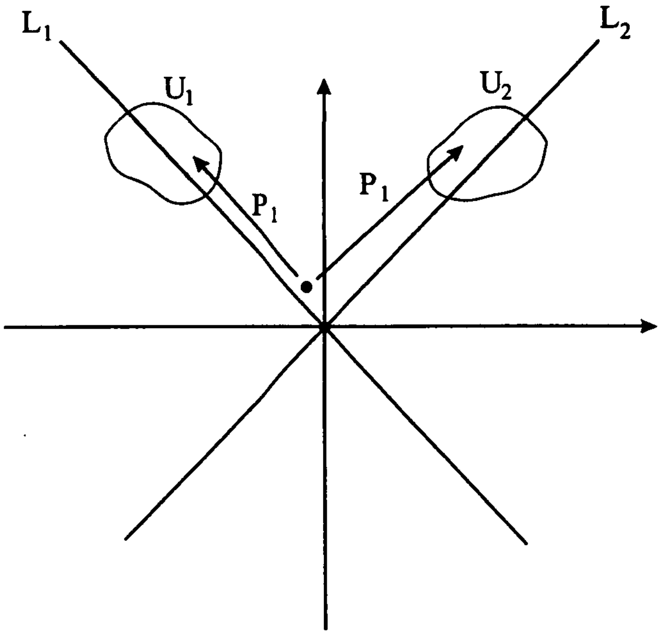

Figure 1

integer m such that the matrix $P = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ belongs to G. Let L_x denote the x-axis in $\mathbb{R}^2$, and for $r > 0$ and $c \in \mathbb{R}^2$, let $D_r(c)$ denote the open disc of radius r centred at c. We shall require the following simple geometric result, which we state without proof:

Lemma 4. *Let W be an open subset of $\mathbb{R}^2$ and suppose that W contains a point $w \in L_x$. Then there exists $\varepsilon > 0$ such that for all $z \in D_\varepsilon(0)\backslash L_x$, there exists $k \in \mathbb{Z}$ for which $P^k(z) \in W$.*

By Lemma 2, there exists a point in U_1 of the form $(x, y)/s$, where $s \in \mathbb{N}$ and x, y are relatively prime. Choose $a, b \in \mathbb{Z}$ such that $ax + by = 1$ and set

$$B = \begin{pmatrix} a & b \\ -y & x \end{pmatrix}.$$

Then $B \in SL(2, \mathbb{Z})$ and as G is normal, $A_1 = B^{-1}PB \in G$. The matrix A_1 is parabolic and fixes pointwise the line L_1 passing through the origin and the point (x, y). Notice that $B(U_1)$ contains the point $(1, 0)/s \in L_x$. Applying Lemma 4 to $W = B(U_1)$, we obtain an open neighbourhood V_1 of 0 such that for all $v \in V_1\backslash L_1$, there exists $k(v) \in \mathbb{Z}$ for which $A_1^{k(v)}(v) \in U_1$. Similarly, there is a line L_2 passing through the origin and a point in U_2, a matrix $A_2 \in G$, and an open neighbourhood V_2 of 0 such that for all

$v \in V_2 \backslash L_2$, there exists $l(v) \in \mathbb{Z}$ for which $A_2^{l(v)}(v) \in U_2$. Let

$$v \in V_1 \cap V_2 \backslash (L_1 \cup L_2), P_1 = A_1^{k(v)}, P_2 = A_2^{l(v)}$$

and set $u = P_1(v) \in U_1$. Choosing $g = P_2 P_1^{-1}$, we have $g(u) \in U_2$; so $g(U_1) \cap U_2 \neq \emptyset$, as required.

References

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

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

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

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

[5] G.J.O. Jameson, *The prime number theorem* (Cambridge University Press, Cambridge, 2003).

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

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

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