PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 122, Number 2, October 1994

GENERATORS FOR ALL PRINCIPAL CONGRUENCE SUBGROUPS OF $\mathrm{SL}(n, Z)$ WITH $n \geq 3$

B. SURY AND T. N. VENKATARAMANA

(Communicated by Ronald M. Solomon)

ABSTRACT. We show that there is a uniform bound for the numbers of generators for all *principal* congruence subgroups of $\mathrm{SL}(n, Z)$ for $n \geq 3$. On the other hand, we show that the numbers are unbounded if we work with all arithmetic subgroups of $\mathrm{SL}(n, Z)$.

INTRODUCTION

It is a classical result that $\mathrm{SL}(n, Z)$ is finitely generated, and hence, so are all its subgroups of finite index. More generally, lattices in real semisimple Lie groups are well known to be finitely generated. One could ask whether there is a uniform bound on the number of generators required to generate any arithmetic subgroup of a real semisimple group. We will first show that this is too much to expect, by giving examples in the case of even $\mathrm{SL}(n; R)$. On the other hand, we shall show that such a uniform bound on the number of generators exists for all *principal congruence subgroups* of $\mathrm{SL}(n, Z)$ for $n \geq 3$. Though we address the group $\mathrm{SL}(n, Z)$ for simplicity, it is not difficult to see that the proof of the existence of a uniform bound carries over to S-arithmetic groups which strongly satisfy the congruence subgroup property (CSP), i.e., whose congruence kernel is actually trivial.

NONEXISTENCE EXAMPLE

Consider $\Gamma = \mathrm{SL}(2n, Z)$, $n \geq 2$. Given any integer $r > 0$, we show that there is a subgroup Δ of finite index in Γ, which cannot be generated by less than r elements. We write C for the center $\{\pm I\}$ of Γ, where I denotes the identity matrix. Let $p_1, \ldots, p_r$ be any r distinct odd primes, and we consider the principal congruence subgroups

$$\Gamma(p_i) = \{\gamma \in \Gamma\colon\ \gamma \equiv I \bmod p_i\}.$$

By the strong approximation property [K], the natural homomorphism

$$\pi_r\colon\ \Gamma \to \prod_{i=1}^{r} \mathrm{SL}(2n, Z/p_i)$$

Received by the editors January 15, 1993.
1991 *Mathematics Subject Classification.* Primary 20H05, 20G30.
Key words and phrases. Congruence subgroup, finite generation.

is surjective. Indeed, Γ is dense in $\prod_{\text{all } p} \mathrm{SL}(2n, Z_p)$ and the subgroup U of $\prod_{\text{all } p} \mathrm{SL}(2n, Z_p)$ which maps to the identity under the surjective map

$$\prod_{\text{all } p} \mathrm{SL}(2n, Z_p) \to \prod_{i=1}^{r} \mathrm{SL}(2n, Z/p_i)$$

is open. So $\Gamma \cdot U = \prod_{\text{all } p} \mathrm{SL}(2n, Z_p)$ which proves that Γ itself surjects to the finite product. Let us look at the subgroup $\Delta := \pi_r^{-1}(C^r)$ of finite index in Γ. Here $C = \{\pm I\}$. Since Δ surjects onto C^r, the minimal number of generators for Δ is at least the minimal number for C^r, which is r.

Remarks. (i) A similar trick may be used for $\mathrm{SL}(2n+1, Z)$.

(ii) In the above example, we can even replace $\mathrm{SL}(2n, Z)$ by a torsion-free subgroup Γ_0 of finite index (which exists, in general, by a result of Selberg). For, by the CSP, $\Gamma_0 \supset \Gamma(m)$ for some integer m, and we can replace C^r and Δ in the example by

$$C^r \times \{I\}^{w(m)} \subset \prod_{i=1}^{r} \mathrm{SL}(2n, Z/p_i) \times \prod_{p/m} \mathrm{SL}(2n, Z/p)$$

and $\Delta \cap \Gamma_0$, respectively. We have written $w(m)$ for the number of prime divisors of m.

Existence theorem

Let $\Gamma := \mathrm{SL}(n, Z)$, $n \geq 3$. There exists a number $f(n)$ such that each principal congruence subgroup $\Gamma(m)$ of Γ is generated by at most $f(n)$ elements.

Proof. First, we shall construct a finite set $\Sigma \subset \mathrm{SL}(n, Z)$, such that the various conjugates $\{gXg^{-1};\ g \in \Sigma,\ X \in n^+\}$ generate, as a Z-module, all the integral matrices $\mathrm{sl}(n, Z)$ of trace zero. Here n^+ denotes strictly upper triangular integral matrices. Since $\mathrm{sl}(n, Z)$ has a Z-basis

$$\{E_{ij},\ i \neq j\} \cup \{E_{ii} - E_{i+1,i+1},\ 1 \leq i < n\},$$

where E_{lm} denotes the matrix with the entry 1 at the (l, m)th place and zero elsewhere, and since $\{E_{ij},\ i > j\}$ are clearly obtained from finitely many conjugates of $\{E_{ij},\ i < j\} \subset n^+$, we only have to get $E_{i,i} - E_{i+1,i+1}$, $1 \leq i < n$. But, consider

$$g = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & \ddots & & & & 0 & \\ & & & -1 & 0 & & & \\ & & & 1 & -1 & & & \\ & 0 & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}.$$

Evidently, $gE_{i,i+1}g^{-1} - E_{i,i+1} + E_{i+1,i} = E_{i,i} - E_{i+1,i+1}$. Therefore, we have established the existence of a finite set Σ as claimed. Note that $|\Sigma| \leq \frac{n(n+1)}{2}$.

To proceed with the proof, let us consider a principal congruence subgroup $\Gamma(m)$ of Γ. Let $U^+(m) = \{u \in \Gamma(m)\colon u \text{ is upper triangular, unipotent}\}$. Clearly, $U^+(m)$ is generated by a finite number $g(n)$ of elements in it, where $g(n)$ does not depend on m. In fact, $g(n) \leq \frac{n(n-1)}{2}$. We define $E(m)$ to be the subgroup of $\Gamma(m)$ generated by the conjugates $\{{}^gU^+(m),\ g \in \Sigma\}$. We note that the number of generators of $E(m) \leq |\Sigma| \cdot g(n)$.

Our main contention is that $E(m) = \Gamma(m)$. *This will prove the theorem with* $f(n) = |\Sigma| \cdot g(n)$. The proof will be in two steps.

Step 1. $E(m) \supset \Gamma(m^l)$ for some $l \gg 0$.

Step 2. $\Gamma(m) \subset E(m)\Gamma(m^2)$.

Clearly, the two steps prove $E(m) = \Gamma(m)$, for, applying Step 2 repeatedly gives $\Gamma(m) \subset E(m)\Gamma(m^l) \subset E(m)$ by Step 1.

Proof of Step 1. Let $\overline{E(m)}$ denote the closure of $E(m)$ in the congruence completion $\mathrm{SL}_n(\hat{Z}) = \prod_{\text{all } p} \mathrm{SL}_n(Z_p)$ of Γ. Now, the group generated by $\{{}^gU^+(Z_p),\ g \in \Sigma\}$ is the whole of $\mathrm{SL}_n(Z_p)$. To see this, we notice that since $\mathrm{SL}_n(Z_p)$ is generated by the elementary matrices and the diagonals, we only have to show that diagonals in $\mathrm{SL}_n(Z_p)$ can be obtained. Once again, it is enough to get diagonals of the form $d_i(t) = \mathrm{diag}(1, \ldots, 1, t, t^{-1}, 1, \cdot, 1)$ with t as the ith diagonal entry, since $\mathrm{diag}(t_1, \ldots, t_n) = d_1(t_1) \cdot d_2(t_1t_2) \cdots d_{n-1}(t_1 \cdots t_{n-1})$. The matrices $d_i(t)$ are obtained as $X_{ij}(t)X_{ji}(-t^{-1})X_{ij}(t)X_{ij}(-1)X_{ji}(1)X_{ij}(-1)$. We have written $X_{ij}(t)$ for the matrix $I + tE_{ij}$. Since $E(m) \supset {}^gU^+(m)$ for all g in Σ, since U^+ satisfies the strong approximation property [K], and since $\{{}^gU^+(Z_p),\ g \in \Sigma\}$ generates the whole of $\mathrm{SL}_n(Z_p)$, we have

$$(*) \qquad \overline{E(m)} \supset \prod_{p \nmid m} \mathrm{SL}_n(Z_p) \times \prod_{p/m} E_p$$

where E_p are open subgroups of finite indices in $\mathrm{SL}_n(Z_p)$. But, the congruence subgroup property [BMS] shows that $E(m)$ is closed in $\mathrm{SL}_n(Z)$ for the congruence topology, which combined with the fact that its closure in $\mathrm{SL}_n(\hat{Z})$ equals $\overline{E(m)}$ gives $\overline{E(m)} \cap \mathrm{SL}_n(Z) = E(m)$.[1] (For $E(m) \supset \Gamma(r)$ for some r. Given any $g \in \overline{E(m)} \cap \mathrm{SL}_n(Z)$, there is a sequence $g_n \in E(m)$ such that $g_n \to g$ in the congruence topology, i.e., $g_n^{-1}g \in \Gamma(r)$ for some $n \gg 0$. This shows $g \in g_n \cdot \Gamma(r) \subset E(m)$.)

But then $(*)$ gives $E(m) = \overline{E(m)} \cap \mathrm{SL}_n(Z) \supset \Gamma(m^r)$.

Proof of Step 2. Consider

$$\pi\colon \Gamma(m) \to \mathrm{SL}_n(Z/m^2Z),$$
$$I + mA \mapsto I + m\overline{A}$$

where $\overline{A}$ is A modulo m.

We need to show that $\pi(E(m)) = \pi(\Gamma(m))$. Let us note that $g = I + mA \in \Gamma(m) \Rightarrow \mathrm{tr}\, A \equiv 0 \bmod m$, and hence $\pi(\Gamma(m)) \subset \{I + mA\colon A \in M_n(Z/mZ), \mathrm{tr}\, A = 0\}$. Now, if $u \in U^+(m)$, then $u = I + mA$, $A \in n^+$. So $E(m) \supset$ Group generated by $\{I + m \cdot {}^g n^+,\ g \in \Sigma\}$.

Thus, $\pi(E(m)) \supset \{I + m \cdot A\colon A \in M_n(Z/mZ), \mathrm{tr}\, A = 0\}$ if we know that the matrices in $\mathrm{sl}(n, Z)$ surject mod m to all of $\{A \in M_n(Z/mZ), \mathrm{tr}\, A = 0\}$.

[1] We thank the referee for pointing out that the CSP for $\mathrm{SL}(n, Z)$ implies $\bar{\Gamma} \cap \mathrm{SL}(n, Z) = \Gamma$ *for* Γ *of finite index.*

But this is true because of the following reasoning. We only have to show that any diagonal matrix $A = \operatorname{diag}(a_1, \ldots, a_n) \in M_n(Z/mZ)$ of trace zero is in the image. But then it is clear that if $D_i := E_{i,i} - E_{i+1,i+1}$, then

$$A = a_1D_1 + (a_1 + a_2)D_2 + \cdots + (a_1 + \cdots + a_{n-1})D_{n-1}$$

modulo m. This completes the proof of Step 2 and hence, of the theorem.

Note added in proof. The anonymous referee points out that (in regards to the nonexistence example) Mann and Segal [Proc. London Math. Soc. **61** (1990)] have shown that if there is a bound for the number of generators for all subgroups of finite index in a finitely generated linear group, then the group is virtually solvable.

Acknowledgments

We are indebted to Kumar Murty for raising the question on the existence of a uniform bound for all arithmetic groups. Our special thanks go to A. S. Rapinchuk for pointing out the counterexample to the general question. We would also like to thank the anonymous referee whose comments made the manuscript more readable.

References

[B-M-S] H. Bass, J. Milnor, and J.-P. Serre, *Solution of the congruence subgroup problem for* SL_n $(n \geq 3)$ *and* Sp_{2n} $(n \geq 2)$, Inst. Hautes Études Sci. Publ. Math. **33** (1967), 421–499.

[K] M. Kneser, *Strong approximation*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, RI, 1966, pp. 187–196.

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Bombay 400005, India

E-mail address: sury@tifrvax.bitnet