On the bounded generation of arithmetic SL_2

Bruce W. Jordan[a,1,2] **and Yevgeny Zaytman**[b,1]

[a]Department of Mathematics, Baruch College, The City University of New York, New York, NY 10010-5526; and [b]Center for Communications Research, Princeton, NJ 08540-1966

Edited by Kenneth A. Ribet, University of California, Berkeley, CA, and approved July 30, 2019 (received for review May 3, 2019)

Let K be a number field and S be a finite set of primes of K containing the archimedean valuations. Let $\mathcal{O}$ be the ring of S-integers in K. Morgan, Rapinchuck, and Sury [A. V. Morgan *et al.*, *Algebra Number Theory* 12, 1949–1974 (2018)] have proved that if the group of units $\mathcal{O}^\times$ is infinite, then every matrix in $SL_2(\mathcal{O})$ is a product of at most 9 elementary matrices. We prove that under the additional hypothesis that K has at least 1 real embedding or S contains a finite place we can get a product of at most 8 elementary matrices. If we assume a suitable generalized Riemann hypothesis, then every matrix in $SL_2(\mathcal{O})$ is the product of at most 5 elementary matrices if K has at least 1 real embedding, the product of at most 6 elementary matrices if S contains a finite place, and the product of at most 7 elementary matrices in general.

bounded generation | SL_2

1. Introduction

Let K be a number field and S be a finite set of primes of K containing the archimedean valuations. Denote by $\mathcal{O}=\mathcal{O}_S$ the ring of S-integers in K:

$$\mathcal{O}=\mathcal{O}_S=\{x\in K^\times \mid v(x)\geq 0 \text{ for all } v\notin S\}.$$

For $x\in\mathcal{O}$ we define the upper triangular matrix $U(x)$ and the lower triangular matrix $L(x)$ by

$$U(x):=\begin{bmatrix}1 & x\\ 0 & 1\end{bmatrix} \quad \text{and} \quad L(x):=\begin{bmatrix}1 & 0\\ x & 1\end{bmatrix}. \qquad [1]$$

The elementary matrices over $\mathcal{O}$ are the matrices $U(x)$, $L(x)$ for $x\in\mathcal{O}$.

Consider the case where K is the field of rational numbers $\mathbb{Q}$. Taking $\mathcal{O}=\mathbb{Z}$ we have that every $A\in SL_2(\mathbb{Z})$ is a product of elementary matrices, but the number required is unbounded. However, if we take $\mathcal{O}=\mathbb{Z}[1/p]$ for p prime, the situation is different. Every matrix $A\in SL_2(\mathbb{Z}[1/p])$ is a product of at most 5 elementary matrices as was proved by Vsemirnov (ref. 1, theorem 1.1).

The key difference between $\mathbb{Z}$ and $\mathbb{Z}[1/p]$ for this bounded generation question for SL_2 is their units: $\mathbb{Z}^\times=\langle\pm 1\rangle$ is finite whereas $\mathbb{Z}[1/p]^\times$ is infinite. Vaserštein (2) proved that if $\mathcal{O}$ has infinitely many units, then $SL_2(\mathcal{O})$ is generated by elementary matrices. Morgan, Rapinchuk, and Sury (ref. 3, theorem 1.1) recently proved an explicit general result on bounded generation:

Theorem 1.1 (Morgan, Rapinchuk, and Sury). *Assume that the group of units $\mathcal{O}^\times$ is infinite. Then every matrix in $SL_2(\mathcal{O})$ can be written as a product of at most 9 elementary matrices with the first one lower triangular.*

The lower triangular assertion follows from their proof (ref. 3, equation 21 and following text).

Here we prove 2 theorems on a matrix $A\in SL_2(\mathcal{O})$:

Theorem 1.2. *Suppose that S contains a finite place or suppose that the group of units $\mathcal{O}^\times$ is infinite and K has at least 1 real embedding. Then $A\in SL_2(\mathcal{O})$ can be written as the product of at most 8 elementary matrices with the first one lower triangular.*

Theorem 1.3. *Assume that the group of units $\mathcal{O}^\times$ is infinite and assume the Generalized Riemann Hypothesis 3.7. Then $A\in SL_2(\mathcal{O})$ can be written as the product of at most 5 elementary matrices if K has at least 1 real embedding, the product of at most 6 elementary matrices if S contains a finite place, and the product of at most 7 elementary matrices in general with the first one lower triangular in each case.*

We give diophantine applications of *Theorems 1.2* and *1.3* in ref. 4. These applications require us to know that the first matrix in our factorization into elementary matrices can be taken to be lower triangular. Hence we keep track of this here, whereas it is not a concern in ref. 3.

2. Theorem 1.2

A. Reducing the First Row of a Matrix $A\in SL_2(\mathcal{O})$. Following ref. 3, section 4, let

$$\mathcal{R}(\mathcal{O})=\{(a,b)\in\mathcal{O}^2 \mid a\mathcal{O}+b\mathcal{O}=\mathcal{O}\}. \qquad [2]$$

The $(a,b)\in\mathcal{R}(\mathcal{O})$ are precisely the first rows of matrices in $SL_2(\mathcal{O})$. The effect on the first row of a matrix $A=\left[\begin{smallmatrix}a & b\\ * & *\end{smallmatrix}\right]\in SL_2(\mathcal{O})$ from right multiplying by an elementary matrix as in Eq. **1** is

$$AL(x)=\begin{bmatrix}a & b\\ * & *\end{bmatrix}\begin{bmatrix}1 & 0\\ x & 1\end{bmatrix}=\begin{bmatrix}a+bx & b\\ * & *\end{bmatrix}, \qquad [3]$$
$$AU(x)=\begin{bmatrix}a & b\\ * & *\end{bmatrix}\begin{bmatrix}1 & x\\ 0 & 1\end{bmatrix}=\begin{bmatrix}a & ax+b\\ * & *\end{bmatrix}$$

for $x\in\mathcal{O}$.

The following succinct notation using only the first rows of matrices is convenient:

Definition 2.1: For $x\in\mathcal{O}$ and $(a,b)\in\mathcal{R}(\mathcal{O})$, set $(a,b)\ell(x)=(a+bx,b)$ and $(a,b)u(x)=(a,ax+b)$.

Significance

Let $\mathcal{O}$ be the ring of integers in a number field with a finite number of prime ideals inverted. Whether every 2×2 matrix A with entries in $\mathcal{O}$ and $\det A=1$ is a product of a bounded number of elementary matrices $\left[\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}1 & 0\\ x & 1\end{smallmatrix}\right]$ for $x\in\mathcal{O}$ reflects the arithmetic of $\mathcal{O}$. If $\mathcal{O}$ has infinitely many units, we prove 2 theorems bounding the number of elementary matrices required.

Author contributions: B.W.J. and Y.Z. performed research and wrote the paper.

The authors declare no conflict of interest.

This article is a PNAS Direct Submission.

[1]B.W.J. and Y.Z. contributed equally to this work.

[2]To whom correspondence may be addressed. Email: bruce.jordan@baruch.cuny.edu.

Published online September 4, 2019.

If there exist $x_1, \dots, x_k \in \mathcal{O}$ with

$$(c,d) = \begin{cases} (a,b)\ell(x_1)u(x_2)\cdots\ell(x_k) & k \text{ odd} \\ (a,b)\ell(x_1)u(x_2)\cdots u(x_k) & k \text{ even} \end{cases} \quad [4]$$

for $(a,b),(c,d) \in \mathcal{R}(\mathcal{O})$, write $(a,b) \overset{k,\ell}{\Longrightarrow} (c,d)$. Similarly, if there exist $x_1, \dots, x_k \in \mathcal{O}$ with

$$(c,d) = \begin{cases} (a,b)u(x_1)\ell(x_2)\cdots u(x_k) & k \text{ odd} \\ (a,b)u(x_1)\ell(x_2)\cdots\ell(x_k) & k \text{ even} \end{cases} \quad [5]$$

for $(a,b),(c,d) \in \mathcal{R}(\mathcal{O})$, write $(a,b) \overset{k,u}{\Longrightarrow} (c,d)$. As in ref. 3, section 4, write $(a,b) \overset{k}{\Longrightarrow} (c,d)$ if $(a,b) \overset{k,\ell}{\Longrightarrow} (c,d)$ or $(a,b) \overset{k,u}{\Longrightarrow} (c,d)$.

B. The Proof of Theorem 1.2. First we need the following *Lemma 2.3*, which requires a definition.

Definition 2.2 (ref. 3, section 3.1): A prime $\mathfrak{q}$ of the number field K lying above the rational prime q is $\mathbb{Q}$-split if $q > 2$ and $K_{\mathfrak{q}} \cong \mathbb{Q}_q$.

Lemma 2.3 (cf. ref. 3, lemma 4.4). *Suppose K has at least 1 real embedding or S contains a finite place and $(a,b) \in \mathcal{R}(\mathcal{O})$. Then there exists $a' \in \mathcal{O}$ and infinitely many $\mathbb{Q}$-split prime principal ideals $\mathfrak{q}$ of $\mathcal{O}$ with a generator $\wp$ such that for any $m \equiv 1 \bmod \phi(a'\mathcal{O})$ we have $(a,b) \overset{3,u}{\Longrightarrow} (a', \wp^{2m})$.*

Proof: Let v be either a real place of K or a finite place in S. To simplify subsequent notation we use the convention that the valuation of an element $\alpha \in K$ with respect to a real place v is odd if α is negative with respect to v.

Let $b' \in \mathcal{O}$ be an odd prime congruent to $b \bmod a$ that has odd valuation with respect to v. Such a b' exists by Dirichlet's theorem. Note that $(a,b) \overset{1,u}{\Longrightarrow} (a,b')$.

For a prime w of K, denote by $(*,*)_w$ the local (quadratic) Hilbert symbol at w. Find a prime a' congruent to $a \bmod b'$ such that $(a',b')_{v_i} = 1$ for all places v_i in S and above 2 and ∞ except v and $(a',b')_v = (a',b')_{b'\mathcal{O}}$. That such an a' exists follows from Dirichlet's theorem and the fact that b' has odd valuation with respect to v. Note that a' and b' are relatively prime and $(a,b') \overset{1,\ell}{\Longrightarrow} (a',b')$.

Observe that by the reciprocity law $(a',b')_{a'\mathcal{O}} = 1$; i.e., $b' \equiv x^2 \bmod (a'\mathcal{O})$ for some residue x. Let $\wp$ be an odd, degree-1 prime congruent to $x \bmod a'\mathcal{O}$. Such $\wp$ generate infinitely many prime ideals $\mathfrak{q} = (\wp)$ by the generalization of Dirichlet's theorem to $\mathbb{Q}$-split primes (ref. 3, theorem 3.3). Then for all $m \equiv 1 \bmod \phi(a'\mathcal{O})$ we have $(a',b') \overset{1,u}{\Longrightarrow} (a', \wp^{2m})$. Hence we are done. □

Proof of Theorem 1.2: Suppose S contains a finite place or $\#\mathcal{O}^\times = \infty$ and K has at least 1 real embedding. Let $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathcal{O})$. Proceed as in the proof of ref. 3, section 4, only use *Lemma 2.3* instead of ref. 3, lemma 4.4. Thus we do not need to use ref. 3, lemma 4.3 and we end up showing $(a,b) \overset{7}{\Longrightarrow} (1,0)$ instead of $(a,b) \overset{8}{\Longrightarrow} (1,0)$ as in ref. 3, equation 21. Hence A is the product of 8 elementary matrices beginning with a lower triangular matrix. □

3. Theorem 1.3

A. Division Chains.

Definition 3.1 (cf. ref. 5, section 2): Let $(a,b) \in \mathcal{R}(\mathcal{O})$ as in Eq. **2**. A division chain of length k starting with (a,b) is a sequence of equations

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ &\vdots \\ r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} \\ r_{k-2} &= q_k r_{k-1} + r_k \end{aligned} \quad [6]$$

with $q_i \in \mathcal{O}$, $1 \le i \le k$. The division chain is terminating if $r_k = 0$. Note that since a and b are relatively prime, in the terminating case r_{k-1} must be a unit.

Remark 3.2: The division chains of *Definition 3.1* are closely related to the row reductions of *Definition 2.1*. The division chain in Eq. **6** of length k starting with $(a,b) \in \mathcal{R}(\mathcal{O})$ is equivalent to

$$(a,b) \overset{k,\ell}{\Longrightarrow} \begin{cases} (r_{k-1}, r_k) \text{ if } k \text{ is even} \\ (r_k, r_{k-1}) \text{ if } k \text{ is odd.} \end{cases}$$

The following lemma is elementary:

Lemma 3.3. *We have $b \equiv v \bmod a$ for $v \in \mathcal{O}^\times$ if and only if there exists a terminating division chain of length 2 starting with (b,a).*

B. Terminating Division Chains of Length 2. Consider the matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathcal{O}). \quad [7]$$

Assume in this subsection that there is a terminating division chain of length 2 starting with (b,a). Therefore, by *Lemma 3.3*, we have $b \equiv v \bmod a$, or $b - v = ax$ for $x \in \mathcal{O}$, with a unit $v \in \mathcal{O}^\times$.

Proposition 3.4.

$$AU(-x)L(v^{-1}(1-a))U(-v) = L(w)$$

for some $w \in \mathcal{O}$.

Proof: Multiplying matrices verifies that

$$AU(-x)L(v^{-1}(1-a))U(-v) =: B = \begin{bmatrix} 1 & 0 \\ * & * \end{bmatrix}.$$

But the entry B_{22} must be 1 since $B \in \mathrm{SL}_2(\mathcal{O})$. Hence $B = L(w)$ for some $w \in \mathcal{O}$. □

Theorem 3.5. *Let A be as in* Eq. **7** *and assume there is a terminating division chain of length 2 starting with (b,a). Then A can be written as a product of at most 4 elementary matrices with the first one lower triangular.*

Proof: From *Proposition 3.4* we have

$$A = L(w)U(-v)^{-1}L(v^{-1}(1-a))^{-1}U(-x)^{-1}. \quad [8]$$

But for any $s \in \mathcal{O}$ we have $U(s)^{-1} = U(-s)$ and $L(s)^{-1} = L(-s)$. Hence Eq. **8** becomes

$$A = L(w)U(v)L(v^{-1}(a-1))U(x). \quad \square$$

C. General Matrices in $\mathrm{SL}_2(\mathcal{O})$.

Theorem 3.6. *Let A be as in* Eq. **7**. *If there exists a terminating division chain of length $k > 1$ starting at*

$$\begin{cases} (a,b) & \text{if} \quad k \text{ is odd} \\ (b,a) & \text{if} \quad k \text{ is even}, \end{cases}$$

then A can be written as the product of at most $k+2$ elementary matrices with the first one lower triangular.

Proof: We proceed by induction on k. The $k=2$ case is *Theorem 3.5*.

Suppose k is odd. Then by the definition of a terminating division chain there exists $y \in \mathcal{O}$ such that

$$a - r = by$$

and (b, r) has a terminating division chain of length $k-1$. Then

$$AL(-y) = \begin{bmatrix} r & b \\ * & * \end{bmatrix}$$

is the product of $k+1$ elementary matrices with the first one lower triangular by the induction hypothesis.

The k even case is handled similarly; only switch the roles of a and b as well as multiply by $U(-y)$ instead of $L(-y)$. □

Note that this construction is similar to that used in ref. 5, corollary 2.3 except ours is more efficient, so we end up with $k+2$ rather than the $k+4$ elementary matrices produced by the construction of ref. 5, pp. 496–498. This accounts for why our numbers are 2 smaller than theirs.

D. The Generalized Riemann Hypothesis and the Proof of Theorem 1.3. The relevant Riemann hypothesis is most clearly stated in ref. 6, theorem 3.1.

Riemann Hypothesis 3.7. *The ζ function of $K(\zeta_n, \sqrt[n]{\mathcal{O}^\times})$ satisfies the Riemann hypothesis for all integers $n > 0$.*

Proof of Theorem 1.3: Let $\mathcal{O}$ be the S-integers in K and $(a, b) \in \mathcal{R}(\mathcal{O})$ as in Eq. **2**. Assume *Hypothesis 3.7*. Then by ref. 5, theorem 2.2 there is a terminating division chain of length 5 starting with (a, b). If S contains at least 1 finite prime, then there is a terminating division chain of length 4 starting with (a, b) by ref. 5, theorem 2.9, attributed to Lenstra. If K has a real place, then ref. 5, theorem 2.14 shows that there is a terminating division chain of length 3 starting with (a, b). Now apply *Theorem 3.6*. □

Morgan, Rapinchuk, and Sury (ref. 3, proposition 5.1) show that if $p > 7$ is a prime, then not every matrix in $\mathrm{SL}_2(\mathbb{Z}[1/p])$ is a product of 4 elementary matrices. Hence the bound of 5 elementary matrices if K has a real embedding in *Theorem 1.3* assuming *Hypothesis 3.7* would be strict.

ACKNOWLEDGMENTS. We sincerely thank the referee for corrections and improvements to the paper.

1. M. Vsemirnov, Short unitriangular factorizations of $\mathrm{SL}_2(\mathbb{Z}[1/p])$. *Q. J. Math.* **65**, 279–290 (2014).
2. L. N. Vaserštein, The group SL_2 over Dedekind rings of arithmetic type. *Mat. Sb. (N.S.)* **89**, 313–322 (1972).
3. A. V. Morgan, A. S. Rapinchuk, B. Sury, Bounded generation of SL_2 over rings of S-integers with infinitely many units. *Algebra Number Theory* **12**, 1949–1974 (2018).
4. B. W. Jordan, Y. Zaytman, Integral points on varieties defined by matrix factorization into elementary matrices. arXiv:1901.09433 (27 January 2019).
5. G. Cooke, P. J. Weinberger, On the construction of division chains in algebraic number rings, with applications to SL_2. *Comm. Algebra* **3**, 481–524 (1975).
6. H. W. Lenstra Jr, On Artin's conjecture and Euclid's algorithm in global fields. *Invent. Math.* **42**, 201–224 (1977).