

*Pacific
Journal of
Mathematics*

ON A MODULAR FORM OF ZAREMBA'S CONJECTURE

NIKOLAY G. MOSHCHEVITIN AND ILYA D. SHKREDOV

Volume 309 No. 1

November 2020

ON A MODULAR FORM OF ZAREMBA'S CONJECTURE

NIKOLAY G. MOSHCHEVITIN AND ILYA D. SHKREDOV

We prove that for any prime p there is a divisible by p number $q = O(p^{30})$ such that for a certain positive integer a coprime with q the ratio a/q has bounded partial quotients. In the other direction we show that there is an absolute constant $C > 0$ such that for any prime p exist divisible by p number $q = O(p^C)$ and a number a , a coprime with q such that all partial quotients of the ratio a/q are bounded by two.

1. Introduction

Let a and q be two positive coprime integers, $0 < a < q$. By the Euclidean algorithm, a rational a/q can be uniquely represented as a regular continued fraction

$$(1) \quad \frac{a}{q} = [0; b_1, \dots, b_s] = \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \dots + \cfrac{1}{b_s}}}} \quad b_s \geq 2.$$

Assuming q is known, we use $b_j(a)$, $j = 1, \dots, s = s(a)$ to denote the partial quotients of a/q ; that is,

$$\frac{a}{q} := [0; b_1(a), \dots, b_s(a)].$$

Zaremba's famous conjecture [1972] posits that there is an absolute constant \mathfrak{k} with the following property: for any positive integer q there exists a coprime to q such that in the continued fraction expansion (1) all partial quotients are bounded:

$$b_j(a) \leq \mathfrak{k}, \quad 1 \leq j \leq s = s(a).$$

In fact, Zaremba conjectured that $\mathfrak{k} = 5$. For large prime q , even $\mathfrak{k} = 2$ should be enough, as conjectured by Hensley [1994; 1996]. This theme is rather popular, especially recently; see, e.g., [Bourgain and Kontorovich 2011; 2014; Frolenkov

This work is supported by the Russian Science Foundation under grant 19-11-00001.

MSC2020: 11B13, 11B75, 11E57, 11J70.

Keywords: continued fractions, Zaremba's conjecture, growth in groups.

and Kan 2014; Hensley 1989; 1996; Kan 2016; Kontorovich 2013; Korobov 1963; Moshchevitin 2007; Niederreiter 1986] and many others. The history of the question can be found, e.g., in [Moshchevitin et al. 2020]. Here we obtain the following “modular” version of Zaremba’s conjecture. The first theorem in this direction was proved by Hensley [1994] and after that in [Magee et al. 2014; 2019].

Theorem 1. *There is an absolute constant \mathfrak{k} such that for any prime number p there exist some positive integers $q = O(p^{30})$, $q \equiv 0 \pmod{p}$ and a , a coprime with q having the property that the ratio a/q has partial quotients bounded by \mathfrak{k} .*

Also, we can say something nontrivial about finite continued fractions with $\mathfrak{k} = 2$. It differs our paper from [Bourgain and Kontorovich 2011; 2014; Kan 2016; Magee et al. 2014; 2019].

Theorem 2. *There is an absolute constant $C > 0$ such that for any prime number p there exist some positive integers $q = O(p^C)$, $q \equiv 0 \pmod{p}$ and a , a coprime with q having the property that the ratio a/q has partial quotients bounded by 2.*

Our proof uses growth results in $\mathrm{SL}_2(\mathbb{F}_p)$ and some well-known facts about the representation theory of $\mathrm{SL}_2(\mathbb{F}_q)$. We study a combinatorial question about intersection of powers of a certain set of matrices $A \subseteq \mathrm{SL}_2(\mathbb{F}_q)$ with an arbitrary Borel subgroup and this seems like a new innovation.

In principle, results from [Hensley 1994] can be written in a form similar to Theorem 1 in an effective way but the dependence of q on p in [Hensley 1994] is rather poor. Thus Theorem 1 can be considered as an explicit version (with very concrete constants) of Hensley’s results as well as rather effective Theorem 2 from [Magee et al. 2019]. Also, the methods of [Hensley 1994; Magee et al. 2014; 2019] are very different from ours.

2. Definitions

Let G be a group with the identity 1. Given two sets $A, B \subset G$, define the *product set* of A and B as

$$AB := \{ab : a \in A, b \in B\}.$$

In a similar way we define the higher product sets, e.g., A^3 is AAA . Let $A^{-1} := \{a^{-1} : a \in A\}$. The Ruzsa triangle inequality [1996] says that

$$|C||AB| \leq |AC||C^{-1}B|$$

for any sets $A, B, C \subseteq G$. As usual, having two subsets A, B of a group G denote by

$$(2) \quad E(A, B) = \left| \{(a, a_1, b, b_1) \in A^2 \times B^2 : a^{-1}b = a_1^{-1}b_1\} \right|$$

the *common energy* of A and B . Clearly, $E(A, B) = E(B, A)$ and by the Cauchy–Schwarz inequality

$$(3) \quad E(A, B)|A^{-1}B| \geq |A|^2|B|^2.$$

We use representation function notations like $r_{AB}(x)$ or $r_{AB^{-1}}(x)$, which counts the number of ways $x \in \mathbf{G}$ can be expressed as a product ab or ab^{-1} with $a \in A$, $b \in B$, respectively. For example, $|A| = r_{AA^{-1}}(1)$ and $E(A, B) = r_{AA^{-1}BB^{-1}}(1) = \sum_x r_{A^{-1}B}^2(x)$. In this paper we use the same letter to denote a set $A \subseteq \mathbf{G}$ and its characteristic function $A : \mathbf{G} \rightarrow \{0, 1\}$. We write \mathbb{F}_q^* for $\mathbb{F}_q \setminus \{0\}$. The signs \ll and \gg are the usual Vinogradov symbols. All logarithms are to base 2.

3. On the representation theory of $SL_2(\mathbb{F}_p)$ and basis properties of its subsets

First of all, we recall some notions and simple facts from the representation theory; see, e.g., [Naimark 2010] or [Serre 1967]. For a finite group \mathbf{G} let $\widehat{\mathbf{G}}$ be the set of all equivalence classes of irreducible unitary representations of \mathbf{G} . It is well-known that size of $\widehat{\mathbf{G}}$ coincides with the number of all conjugacy classes of \mathbf{G} . For $\rho \in \widehat{\mathbf{G}}$ denote by d_ρ the dimension of this representation. We write $\langle \cdot, \cdot \rangle$ for the corresponding Hilbert–Schmidt scalar product $\langle A, B \rangle = \langle A, B \rangle_{HS} := \text{tr}(AB^*)$, where A, B are any two matrices of the same sizes. Put $\|A\| = \sqrt{\langle A, A \rangle}$. Clearly, $\langle \rho(g)A, \rho(g)B \rangle = \langle A, B \rangle$ and $\langle AX, Y \rangle = \langle X, A^*Y \rangle$. Also, we have $\sum_{\rho \in \widehat{\mathbf{G}}} d_\rho^2 = |\mathbf{G}|$.

For any $f : \mathbf{G} \rightarrow \mathbb{C}$ and $\rho \in \widehat{\mathbf{G}}$ define the matrix $\hat{f}(\rho)$, which is called the Fourier transform of f at ρ by the formula

$$(4) \quad \hat{f}(\rho) = \sum_{g \in \mathbf{G}} f(g)\rho(g).$$

Then the inverse formula takes place

$$(5) \quad f(g) = \frac{1}{|\mathbf{G}|} \sum_{\rho \in \widehat{\mathbf{G}}} d_\rho \langle \hat{f}(\rho), \rho(g^{-1}) \rangle,$$

and the Parseval identity is

$$(6) \quad \sum_{g \in \mathbf{G}} |f(g)|^2 = \frac{1}{|\mathbf{G}|} \sum_{\rho \in \widehat{\mathbf{G}}} d_\rho \|\hat{f}(\rho)\|^2.$$

The main property of the Fourier transform is the convolution formula

$$(7) \quad \widehat{f * g}(\rho) = \hat{f}(\rho)\hat{g}(\rho),$$

where the convolution of two functions $f, g : \mathbf{G} \rightarrow \mathbb{C}$ is defined as

$$(f * g)(x) = \sum_{y \in \mathbf{G}} f(y)g(y^{-1}x).$$

In terms of representations we can express the common energy of two sets $A, B \subseteq \mathbf{G}$, as defined in (2). Indeed, using (6) and (7), we derive

$$(8) \quad \mathbb{E}(A, B) = \sum_x (A^{-1} * B)(x) = \frac{1}{|\mathrm{SL}_2(\mathbb{F}_q)|} \sum_{\rho} d_{\rho} \|\widehat{A}^*(\rho) \widehat{B}(\rho)\|^2.$$

Finally, it is easy to check that for any matrices A, B one has $\|AB\| \leq \|A\|_o \|B\|$ and $\|A\|_o \leq \|A\|$, where the operator l^2 -norm $\|A\|_o$ is just the absolute value of the maximal singular value of A . In particular, this shows that $\|\cdot\|$ is indeed a matrix norm.

Now consider the group $\mathrm{SL}_2(\mathbb{F}_q)$ of matrices

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ab|cd), \quad a, b, c, d \in \mathbb{F}_q, \quad ad - bc = 1.$$

Clearly, $|\mathrm{SL}_2(\mathbb{F}_q)| = q^3 - q$. Denote by \mathbf{B} the standard Borel subgroup of all upper-triangular matrices from $\mathrm{SL}_2(\mathbb{F}_q)$, denote by $\mathbf{U} \subset \mathbf{B}$ the standard unipotent subgroup of $\mathrm{SL}_2(\mathbb{F}_q)$ of matrices $(1u|01)$, $u \in \mathbb{F}_q$ and denote by $\Delta \subset \mathbf{B}$ the subgroup of diagonal matrices. \mathbf{B} and all its conjugates form all maximal proper subgroups of $\mathrm{SL}_2(\mathbb{F}_p)$. Detailed description of the representation theory of $\mathrm{SL}_2(\mathbb{F}_q)$ can be found in [Naimark 2010, Chapter II, Section 5]. We formulate the main result from [Naimark 2010] concerning this theme.

Theorem 3. *Let $p > 2$ be a prime number and $q = p^n$. There are $q + 3$ nontrivial representations of $\mathrm{SL}_2(\mathbb{F}_q)$, namely:*

- $\frac{1}{2}(q - 3)$ representations T_{χ} of dimension $q + 1$ indexed via $\frac{1}{2}(q - 3)$ nontrivial multiplicative characters χ on \mathbb{F}_q^* , $\chi^2 \neq 1$.
- A representation \widetilde{T}_1 of dimension q .
- Two representations $T_{\chi_1}^+, T_{\chi_1}^-$ of dimension $\frac{1}{2}(q + 1)$, $\chi_1^2 = 1$.
- Two representations $S_{\pi_1}^+, S_{\pi_1}^-$ of dimension $\frac{1}{2}(q - 1)$.
- $\frac{1}{2}(q - 1)$ representations S_{π} of dimension $q - 1$ indexed via $\frac{1}{2}(q - 1)$ nontrivial multiplicative characters π on an arbitrary quadratic extension of \mathbb{F}_q , $\pi^2 \neq 1$.

By d_{\min} and d_{\max} denote the minimum and maximum over dimensions of all nontrivial representations of a group \mathbf{G} . Thus the result above tells us that in the case $\mathbf{G} = \mathrm{SL}_2(\mathbb{F}_q)$ these quantities differ roughly by a factor of two. Below we assume that $q \geq 3$.

Theorem 3 has two consequences, although, a slightly weaker result than Lemma 4 can be obtained via the classical theorem of Frobenius [1896]; see, e.g., [Shkredov 2018]. Originally, similar arguments were suggested in [Gowers 2008; Nikolov and Pyber 2011; Sarnak and Xue 1991].

Lemma 4. *Let $n \geq 3$ be an integer, $A \subseteq \mathrm{SL}_2(\mathbb{F}_q)$ be a set and $|A| \geq 2(q+1)^2 q^{2/n}$. Then $A^n = \mathrm{SL}_2(\mathbb{F}_q)$. Generally, if for some sets $X_1, \dots, X_n \subseteq \mathrm{SL}_2(\mathbb{F}_q)$ one has*

$$\prod_{j=1}^n |X_j| \geq (2q(q+1))^n (q-1)^2,$$

then $X_1 \dots X_n = \mathrm{SL}_2(\mathbb{F}_q)$.

Proof. Using (6) with $f = A$ (i.e., according our notation f is the characteristic function of the set A), we have for an arbitrary nontrivial representation ρ that

$$(9) \quad \|\widehat{A}\|_o < \left(\frac{|A| |\mathrm{SL}_2(\mathbb{F}_q)|}{d_{\min}} \right)^{1/2} = \left(\frac{|A|(q^3 - q)}{d_{\min}} \right)^{1/2}.$$

Hence for any $x \in \mathrm{SL}_2(\mathbb{F}_q)$ we obtain via formulae (5), (6) and estimate (9) that

$$r_{A^n}(x) > \frac{|A|^n}{|\mathrm{SL}_2(\mathbb{F}_q)|} - \left(\frac{|A|(q^3 - q)}{d_{\min}} \right)^{(n-2)/2} |A| \geq 0,$$

provided $|A|^n \geq 2^{n-2}(q+1)^n q^n (q-1)^2$. The second part of the lemma can be obtained similarly. This completes the proof. \square

Remark 5. It is easy to see (or consult Lemma 6 below) that bound (9) is sharp, e.g., take $A = B$.

For any function $f : G \rightarrow \mathbb{C}$ consider the Wiener norm of f defined as

$$(10) \quad \|f\|_W := \frac{1}{|G|} \sum_{\rho \in \widehat{G}} d_\rho \|\widehat{f}(\rho)\|.$$

Lemma 6. *Let G be a group and Γ be its subgroup. Then $\|\Gamma\|_W \leq 1$. Moreover, $\|B\|_W = 1$, further $\|\widehat{B}(\widetilde{T}_1)\| = \|\widehat{B}(\widetilde{T}_1)\|_o = |B|$ and the Fourier transform of B vanishes on all other nontrivial representations.*

Proof. Since Γ is a subgroup, we see using (6) twice that

$$\begin{aligned} |\Gamma|^2 &= |\{(\gamma_1, \gamma_2, \gamma_3) \in \Gamma^3 : \gamma_1 \gamma_2 = \gamma_3\}| = \frac{1}{|G|} \sum_{\rho \in \widehat{G}} d_\rho \langle \widehat{\Gamma}^2(\rho), \widehat{\Gamma}(\rho) \rangle \\ &\leq \frac{1}{|G|} \sum_{\rho} d_\rho \langle \widehat{\Gamma}(\rho), \widehat{\Gamma}(\rho) \rangle \|\widehat{\Gamma}(\rho)\|_o \leq \frac{|\Gamma|}{|G|} \sum_{\rho} d_\rho \langle \widehat{\Gamma}(\rho), \widehat{\Gamma}(\rho) \rangle = |\Gamma|^2, \end{aligned}$$

because, clearly, $\|\widehat{\Gamma}(\rho)\|_o \leq |\Gamma|$. This means that for any representation ρ either $\|\widehat{\Gamma}(\rho)\| = 0$ (and hence $\|\widehat{\Gamma}(\rho)\|_o = 0$) or $\|\widehat{\Gamma}(\rho)\| \geq \|\widehat{\Gamma}(\rho)\|_o = |\Gamma|$ (alternatively, one can use the usual calculations, namely, $\sum_{\gamma \in \Gamma} \rho(\gamma \gamma_*) = \sum_{\gamma \in \Gamma} \rho(\gamma) \cdot \rho(\gamma_*)$)

for any $\gamma_* \in \Gamma$ but then one needs to be careful with divisors of zero). Another application of (6) gives us

$$(11) \quad |\Gamma| = \frac{1}{|\mathbf{G}|} \sum_{\rho} d_{\rho} \|\widehat{\Gamma}(\rho)\|^2 \geq |\Gamma| \cdot \frac{1}{|\mathbf{G}|} \sum_{\rho} d_{\rho} \|\widehat{\Gamma}(\rho)\| = |\Gamma| \|\Gamma\|_W.$$

Hence $\|\Gamma\|_W \leq 1$ as required.

Now let us prove the second part of the lemma. We write I_n for the identity matrix and let Z_n be the zero matrix of size $n \times n$. Also, we write $\text{diag}(d_1, \dots, d_n)$ for the diagonal matrix with diagonal entries d_1, \dots, d_n . Finally, let $e(\cdot)$ be an additive character of \mathbb{F}_q . For $u_b \in \mathbf{U}$, $u_b = (1b|01)$, we have [Naimark 2010, pp. 121–123] that in a certain orthogonal basis $\widetilde{T}_1(u_b) = \text{diag}(1, e(b), \dots, e(q-1)b)$ and for $g_{\lambda} = (\lambda 0|0\lambda^{-1}) \in \Delta$ the matrix $\widetilde{T}_1(g_{\lambda})$ is the direct sum of I_1 and a permutation matrix of size $(q-1) \times (q-1)$. Clearly, $\mathbf{B} = \Delta \mathbf{U} = \mathbf{U} \Delta$ and hence $\widehat{\mathbf{B}}(\rho) = \widehat{\Delta}(\rho) \widehat{\mathbf{U}}(\rho)$ for any representation ρ . But from above $\widehat{\mathbf{U}}(\widetilde{T}_1)$ is the direct sum $qI_1 \oplus Z_{q-1}$. Further one can show that $\widehat{\Delta}(\widetilde{T}_1) = (q-1)I_1 \oplus 2 \cdot J$, where $J = (J_{ij})_{i,j=1}^{q-1}$ is a certain $(q-1) \times (q-1)$ matrix with all components equal one for i/j belonging to the set of quadratic residues. Such precise description of J is not really important for us, it is enough to see that $\widehat{\Delta}(\widetilde{T}_1)$ is a direct sum of $(q-1)I_1$ and a $(q-1) \times (q-1)$ matrix. Hence

$$\widehat{\mathbf{B}}(\widetilde{T}_1) = \widehat{\Delta}(\widetilde{T}_1) \widehat{\mathbf{U}}(\widetilde{T}_1) = q(q-1)I_1 \oplus Z_{q-1}.$$

Thus $\|\widehat{\mathbf{B}}(\widetilde{T}_1)\| = \|\widehat{\mathbf{B}}(\widetilde{T}_1)\|_o = |\mathbf{B}|$. Applying (11), we obtain

$$(12) \quad |\mathbf{B}| \geq \frac{|\mathbf{B}|^2}{|\text{SL}_2(\mathbb{F}_q)|} + \frac{q}{|\text{SL}_2(\mathbb{F}_q)|} \|\widehat{\mathbf{B}}(\widetilde{T}_1)\|^2 = \frac{|\mathbf{B}|^2}{|\text{SL}_2(\mathbb{F}_q)|} (1+q) = |\mathbf{B}|.$$

It follows that for any other representations Fourier coefficients of \mathbf{B} vanish. This completes the proof. \square

Lemma 6 gives us an alternative way to show that $A^3 \cap \mathbf{B} \neq \emptyset$. Indeed, just use estimate (9) and write

$$\begin{aligned} r_{A^3 \mathbf{B}}(1) &\geq \frac{|A|^3 |\mathbf{B}|}{|\text{SL}_2(\mathbb{F}_q)|} - \|\mathbf{B}\|_W \left(\frac{|A|(q^3 - q)}{d_{\min}} \right)^{3/2} \\ &= \frac{|A|^3 |\mathbf{B}|}{|\text{SL}_2(\mathbb{F}_q)|} - \left(\frac{|A|(q^3 - q)}{d_{\min}} \right)^{3/2} > 0, \end{aligned}$$

provided

$$(13) \quad |A| \gg q^{8/3}.$$

We improve this bound in the next section.

4. On intersections of the product set with the Borel subgroup

It was shown in the previous section (see Lemma 4) that for any $A \subseteq \text{SL}_2(\mathbb{F}_q)$ one has $A^3 = \text{SL}_2(\mathbb{F}_q)$, provided $|A|^3 \gg q^8$ and in the same way the last result holds for three different sets, namely, given $X, Y, Z \subseteq \text{SL}_2(\mathbb{F}_q)$ with $|X||Y||Z| \gg q^8$, we have $XYZ = \text{SL}_2(\mathbb{F}_q)$. It is easy to see that in this generality the last result is sharp. Indeed, let $X = SB, Y = BT$, where S, T are two sets of sizes $\sqrt{q}/2$ which are chosen as $|X| \sim |S||B|$ and $|Y| \sim |T||B|$ (e.g., take S, T from left/right cosets of B thanks to the Bruhat decomposition). Then $XY = SBT$, and hence $|XY| \leq |S||T||B| \leq |\text{SL}_2(\mathbb{F}_q)|/2$. Thus we take Z^{-1} to equal the complement to XY in $\text{SL}_2(\mathbb{F}_q)$ and we see that the product set XYZ does not contain 1 but $|X||Y||Z| \gg q^8$.

Nevertheless, in the ‘‘symmetric’’ case of the same set A this $8/3$ bound (13) can be improved; see Theorem 9 below. We need a simple lemma and the proof of this result, as well as the proof of Theorem 9 extensively play on noncommutative properties of $\text{SL}_2(\mathbb{F}_q)$.

Lemma 7. *Let $g \notin B$ be a fixed element from $\text{SL}_2(\mathbb{F}_q)$. Then for any x one has*

$$r_{B_gB}(x) \leq q - 1.$$

Proof. Let $g = (ab|cd)$ and $x = (\alpha\beta|\gamma\delta)$. By our assumption $c \neq 0$. We have

$$(14) \quad \begin{pmatrix} \lambda & u \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \mu & v \\ 0 & \mu^{-1} \end{pmatrix} = \begin{pmatrix} (\lambda a + uc)\mu & * \\ \mu c/\lambda & vc/\lambda + d/(\lambda\mu) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

In other words, $\mu = \lambda\gamma c^{-1} \neq 0$ (hence $\gamma \neq 0$ automatically) and from

$$\alpha = (\lambda a + uc)\mu = \lambda\gamma c^{-1}(\lambda a + uc)$$

we see that having λ we determine u uniquely (then, (14) gives us μ, v automatically). This completes the proof. □

Lemma 7 quickly implies a result on the Bruhat decomposition of $\text{SL}_2(\mathbb{F}_q)$.

Corollary 8. *Let $g \in \text{SL}_2(\mathbb{F}_q) \setminus B$. Then $B_gB = \text{SL}_2(\mathbb{F}_q) \setminus B$.*

Proof. Clearly, $B \cap B_gB = \emptyset$ because $g \in \text{SL}_2(\mathbb{F}_q) \setminus B$. On the other hand, by Lemma 7, we have

$$E(B, gB) = \sum_x r_{B_gB}^2(x) \leq (q - 1) \sum_x r_{B_gB}(x) = (q - 1)|B|^2.$$

Using the last bound and estimate (3), we obtain

$$|B_gB| \geq \frac{|B|^4}{E(B, gB)} \geq \frac{|B|^4}{(q - 1)|B|^2} = q^3 - q^2 = |\text{SL}_2(\mathbb{F}_q) \setminus B|.$$

This completes the proof. □

Using growth of products of \mathbf{B} as in the last corollary, one can combinatorially improve the constant $8/3$ (to do this combine Lemma 4 and bound (22) below). We suggest another method which uses the representation theory of $\mathrm{SL}_2(\mathbb{F}_q)$ more extensively and which allows to improve this constant further.

Theorem 9. *Let $A \subseteq \mathrm{SL}_2(\mathbb{F}_q)$ be a set, $|A| \geq 4q^{18/7}$. Then $A^3 \cap \mathbf{B} \neq \emptyset$. Generally, $A^n \cap \mathbf{B} \neq \emptyset$ provided $|A| \geq 4q^{2+4/(3n-2)}$.*

Proof. Let $g \notin \mathbf{B}$ and put $A_g^\varepsilon = A^\varepsilon \cap g\mathbf{B}$, where $\varepsilon \in \{1, -1\}$. Also, let $\Delta = \max_{\varepsilon, g \notin \mathbf{B}} |A_g^\varepsilon|$. Since we can assume $A \cap \mathbf{B} = \emptyset$, it follows that

$$(15) \quad \mathbb{E}(A, \mathbf{B}) = \sum_x r_{A^{-1}\mathbf{B}}^2(x) = \sum_{x \notin \mathbf{B}} r_{A^{-1}\mathbf{B}}^2(x) \leq \Delta |\mathbf{B}| |A|$$

and similarly for $\mathbb{E}(A^{-1}, \mathbf{B})$. On the other hand, from (8) and by the second part of Lemma 6, we see that

$$(16) \quad \begin{aligned} \Delta |\mathbf{B}| |A| \geq \mathbb{E}(A, \mathbf{B}) &= \frac{1}{|\mathrm{SL}_2(\mathbb{F}_q)|} \sum_{\rho} d_{\rho} \|\widehat{A}^*(\rho) \widehat{\mathbf{B}}(\rho)\|^2 \\ &= \frac{q}{|\mathrm{SL}_2(\mathbb{F}_q)|} \|\widehat{A}^*(\widetilde{T}_1) \widehat{\mathbf{B}}(\widetilde{T}_1)\|^2, \end{aligned}$$

and, again, similarly for $\|\widehat{A}(\widetilde{T}_1) \widehat{\mathbf{B}}(\widetilde{T}_1)\|^2$. Now consider the equation $b_1 a' a'' a b_2 = 1$ or, equivalently the equation $a'' a b_2 = (a')^{-1} b_1^{-1}$, where $a, a', a'' \in A$ and $b_1, b_2 \in \mathbf{B}$. Clearly, if $A^3 \cap \mathbf{B} = \emptyset$, then this equation has no solutions. Combining Lemma 6 with bound (16) and calculations as in the proof of Lemma 4, we see that this equation can be solved provided

$$\begin{aligned} &\frac{q}{|\mathrm{SL}_2(\mathbb{F}_q)|} |\langle \widehat{A}^2(\widetilde{T}_1) \widehat{\mathbf{B}}(\widetilde{T}_1), \widehat{A}^*(\widetilde{T}_1) \widehat{\mathbf{B}}^*(\widetilde{T}_1) \rangle| \\ &\leq \frac{q}{|\mathrm{SL}_2(\mathbb{F}_q)|} \|\widehat{A}^2(\widetilde{T}_1) \widehat{\mathbf{B}}(\widetilde{T}_1)\| \cdot \|\widehat{A}^*(\widetilde{T}_1) \widehat{\mathbf{B}}(\widetilde{T}_1)\| \\ &\leq \frac{q}{|\mathrm{SL}_2(\mathbb{F}_q)|} \|\widehat{A}(\widetilde{T}_1) \widehat{\mathbf{B}}(\widetilde{T}_1)\| \|\widehat{A}^*(\widetilde{T}_1) \widehat{\mathbf{B}}(\widetilde{T}_1)\| \|\widehat{A}\|_o \\ &\leq \Delta |\mathbf{B}| |A| \|\widehat{A}\|_o < \frac{|A|^3 |\mathbf{B}|^2}{|\mathrm{SL}_2(\mathbb{F}_q)|}. \end{aligned}$$

In other words, in view of (9) it is enough to have

$$(17) \quad |A|^4 \geq 2(q+1)^2 \Delta^2 \cdot |A| q (q+1)$$

or, equivalently,

$$(18) \quad 2q(q+1)^3 \Delta^2 \leq |A|^3.$$

Now let us obtain another bound which works well when Δ is large. Choose $g \notin B$ and $\varepsilon \in \{1, -1\}$ such that $\Delta = |A_g^\varepsilon|$. Using Lemma 7, we derive

$$(19) \quad E(B, A_g^\varepsilon) = \sum_x r_{BA_g^\varepsilon}^2(x) \leq \sum_x r_{BA_g^\varepsilon}(x)r_{BgB}(x) \leq (q-1)|B||A_g^\varepsilon|,$$

and hence by the Cauchy–Schwarz inequality, we get

$$(20) \quad |BA_g^\varepsilon| \geq \frac{|B|^2|A_g^\varepsilon|^2}{E(B, A_g^\varepsilon)} \geq \frac{|B||A_g^\varepsilon|}{q-1} = q\Delta.$$

Consider the equation $a_g(a'a'')^\varepsilon = b$, where $b \in B$, $a_g \in A_g^\varepsilon$ and $a', a'' \in A$. Clearly, if $A^3 \cap B = \emptyset$, then this equation has no solutions. To solve $a_g(a'a'')^\varepsilon = b$ it is enough to solve the equation $z(a'a'')^\varepsilon = 1$, where now $z \in BA_g^\varepsilon$. Applying the second part of Lemma 4 combining with (20), we obtain that it is enough to have

$$8q^3(q+1)^3(q-1)^2 \leq q\Delta|A|^2 \leq |BA_g^\varepsilon||A|^2$$

or, in other words,

$$(21) \quad 8q^2(q+1)^3(q-1)^2 \leq \Delta|A|^2.$$

Considering the second power of (21) and multiplying it with (18), we obtain

$$|A|^7 \geq 2^{14}q^{18} \geq 2^7q^5(q+1)^9(q-1)^4$$

as required.

In the general case inequality (18) can be rewritten as

$$|A|^n \geq 2^{n-2}\Delta^2(q+1)^nq^{n-2}$$

and using the second part of Lemma 4, we obtain an analogue of (21),

$$|A|^{n-1}\Delta \geq 2^nq^{n-1}(q+1)^n(q-1)^2.$$

Combining the last two bounds, we derive the required result. This completes the proof. □

Remark 10. It is easy to see that Theorem 9, as well as Lemma 7 (and also Lemma 6) take place for any Borel subgroup not just for the standard one.

Remark 11. It is easy to see that the arguments of the proof of Theorem 9 give the following combinatorial statement about left/right multiplication of an arbitrary set A by B (just combine bounds (15) and (20)), namely,

$$(22) \quad \max\{|AB|, |BA|\} \gg \min\{q^{3/2}|A|^{1/2}, |A|^2q^{-2}\}.$$

As we have seen by Theorem 9 we know that $A^n \cap B \neq \emptyset$ for large n but under the condition $|A| \gg q^{2+\varepsilon}$ for a certain $\varepsilon > 0$. For the purpose of the next section we need to break the described q^2 -barrier and we do this for prime q , using growth

in $\mathrm{SL}_2(\mathbb{F}_p)$. Let us recall quickly what is known about growth of generating sets in $\mathrm{SL}_2(\mathbb{F}_p)$. Helfgott [2008] obtained his famous result in this direction and we proved in [Rudnev and Shkredov 2018] the following form of Helfgott's result.

Theorem 12. *Let $A \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ be a set, $A = A^{-1}$ which generates the whole group. Then $|AAA| \gg |A|^{1+1/20}$.*

Thus in the case of an arbitrary symmetric generating set and a prime number p Theorem 12 combined with Theorem 9, allow to obtain some bounds which guarantee that $A^n = \mathrm{SL}_2(\mathbb{F}_p)$. For example, if A generates $\mathrm{SL}_2(\mathbb{F}_p)$, $A = A^{-1}$, and $|A| \gg p^{2-\epsilon}$, $\epsilon < \frac{2}{21}$, then $A^n \cap B \neq \emptyset$ for $n \geq (84 - 42\epsilon)/(2 - 21\epsilon)$. On the other hand, the methods from [Helfgott 2008; Rudnev and Shkredov 2018] allow us to obtain the following result about generation of $\mathrm{SL}_2(\mathbb{F}_p)$ via large and not necessary symmetric sets (the condition of nonsymmetry of A is rather crucial for us, see the next section).

Theorem 13. *Let $A \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ be a generating set, $p \geq 5$ and $|A| \gg p^{2-\epsilon}$, $\epsilon < \frac{2}{25}$. Then $A^n \cap B \neq \emptyset$ for $n \geq (100 - 50\epsilon)/(2 - 25\epsilon)$. Also, $A^n = \mathrm{SL}_2(\mathbb{F}_p)$, provided $n \geq 144/(2 - 25\epsilon)$.*

Proof. Put $K = |AAA|/|A|$. We can assume that, say, $|A| \leq p^{2+2/35}$ because otherwise one can apply Theorem 9. We call an element $g \in \mathrm{SL}_2(\mathbb{F}_p)$ regular if $\mathrm{tr}(g) \neq 0, \pm 2$ and let \mathcal{C}_g be the correspondent conjugate class, namely,

$$\mathcal{C}_g = \{s \in \mathrm{SL}_2(\mathbb{F}_p) : \mathrm{tr}(s) = \mathrm{tr}(g)\}.$$

Let T be a maximal torus such that there is $g \in T \cap A^{-1}A$ and $g \neq 1$. By [Rudnev and Shkredov 2018, Lemma 5] such torus T_* , containing a regular element g , exists, otherwise $K \gg |A|^{2/3}$. Firstly, suppose that for a certain $h \in A$ the torus $T' = hTh^{-1}$ has no such property, i.e., there are no nontrivial elements from $A^{-1}A \cap T'$. Then for the element $g' = hgh^{-1} \in T'$ (in the case $T = T_*$ the element g' is regular) the projection $a \rightarrow ag'a^{-1}$, $a \in A$ is one-to-one. Hence $|A^2A^{-1}AA^{-2} \cap \mathcal{C}_g| \geq |A|$. By [Rudnev and Shkredov 2018, Lemma 11], we have $|S \cap \mathcal{C}_g| \ll |S^{-1}S|^{2/3} + p$ for any set S and regular g . Using the Ruzsa triangle inequality, we obtain

$$\begin{aligned} (23) \quad & |(A^2A^{-1}AA^{-2})^{-1}(A^2A^{-1}AA^{-2})| \\ & \leq |A|^{-1}|A^2A^{-1}AA^{-3}||A^3A^{-1}AA^{-2}| \\ & = |A|^{-1}|A^3A^{-1}AA^{-2}|^2|A|^{-1}(|A|^{-1}|A^3A^{-2}||A^2A^{-2}|)^2 \\ & \leq |A|^{-1}(|A|^{-3}|A^4||A^3|^3)^2 \leq K^{12}|A| \end{aligned}$$

and hence

$$|A| \ll |(A^2A^{-1}AA^{-2})^{-1}(A^2A^{-1}AA^{-2})|^{2/3} + p \ll K^8|A|^{2/3}.$$

This gives us $K \gg |A|^{1/24}$.

In the complementary second case (see [Rudnev and Shkredov 2018]) thanks to the fact that A is a generating set, we suppose that for *any* $h \in \text{SL}_2(\mathbb{F}_p)$ there is a nontrivial element from $A^{-1}A$ belonging to the torus hTh^{-1} . Then $A^{-1}A$ is partitioned between these tori and hence again by [Rudnev and Shkredov 2018, Lemma 11], as well as the Ruzsa triangle inequality, we obtain

$$\begin{aligned} |(AA^{-1}AA^{-1})^{-1}(AA^{-1}AA^{-1})| &\leq |A|^{-1}|A^2A^{-1}AA^{-1}|^2 \\ &\leq |A|^{-1}(|A|^{-1}|A^2A^{-2}||A^2A^{-1}|)^2 \\ &\leq |A|^{-1}(|A|^{-3}|A^3|^4)^2 \leq K^8|A| \end{aligned}$$

and whence

$$\begin{aligned} K^2|A| \geq |A^{-1}A| &\geq \sum_{h \in \text{SL}_2(\mathbb{F}_p)/N(T_*)} |A^{-1}A \cap hT_*h^{-1}| \\ &\gg p^2 \cdot \frac{|A|}{|(AA^{-1}AA^{-1})^{-1}(AA^{-1}AA^{-1})|^{2/3}} \\ &\geq p^2|A|^{1/3}K^{-16/3}, \end{aligned}$$

where $N(T)$ is the normalizer of any torus T , $|N(T)| \asymp |T| \asymp p$. Hence thanks to our assumption $|A| \leq p^{2+2/35}$, we have $K \gg p^{3/11}|A|^{-1/11} \gg |A|^{1/24}$. In other words, we always obtain $|AAA| \gg p^{2+(2-25\epsilon)/24}$. After that apply Theorem 9 to find that $A^n \cap B \neq \emptyset$ for $n \geq (100 - 50\epsilon)/(2 - 25\epsilon)$. If we use Lemma 4 instead of Theorem 9, then we obtain $A^n = \text{SL}_2(\mathbb{F}_p)$, provided $n \geq 144/(2 - 25\epsilon)$. This completes the proof. \square

Thus for sufficiently small $\epsilon > 0$ one can take $n = 51$ to get $A^n \cap B \neq \emptyset$ (and $n = 73$ to obtain $A^n = \text{SL}_2(\mathbb{F}_p)$). In the next section we improve this bound for a special set A but nevertheless the arguments of the proof of Theorem 13 will be used in the proof of Theorem 2 from the Introduction.

We finish this section showing that generating sets A of sizes close to p^2 (actually, the condition $|A| = \Omega(p^{3/2+\epsilon})$ is enough) with small tripling constant $K = |A^3|/|A|$ avoid all Borel subgroups.

Lemma 14. *Let $A \subseteq \text{SL}_2(\mathbb{F}_p)$ be a generating set, $p \geq 5$ and $K = |A^3|/|A|$. Then for any Borel subgroup B_* one has $|A \cap B_*| \leq 2pK^{5/3}|A|^{1/3}$.*

Proof. We obtain the result for the standard Borel subgroup B and after that apply the conjugation to prove our lemma in full generality. Let $\gamma \in \mathbb{F}_p^*$ be any number and l_γ be the line

$$l_\gamma = \{(\gamma u | 0 \gamma^{-1}) : u \in \mathbb{F}_p\} \subset \text{SL}_2(\mathbb{F}_p).$$

By [Rudnev and Shkredov 2018, Lemma 7], we have $|A \cap l_\gamma| \leq 2|A^3 A^{-1} A|^{1/3}$. Using the last bound, as well as the Ruzsa triangle inequality, we obtain

$$\begin{aligned} |A \cap B| &\leq \sum_{\gamma \in \mathbb{F}_p^*} |A \cap l_\gamma| \leq 2p|A^3 A^{-1} A|^{1/3} \\ &\leq 2p(|A^4||A^{-2}A|/|A|)^{1/3} \leq 2pK^{5/3}|A|^{1/3}. \end{aligned}$$

This completes the proof. □

Remark 15. Examining the proof of Lemma 7 from [Rudnev and Shkredov 2018] one can equally write $|A \cap l_\gamma| \leq 2|A^3 A^{-2}|^{1/3}$ and hence by the calculations above $|A \cap B_*| \leq 2pK^{4/3}|A|^{1/3}$. Nevertheless, this better estimate has no influence to the final bound in Theorem 1.

Remark 16. Bounds for intersections of $A \subseteq \text{SL}_2(\mathbb{F}_q)$, $K = |A^3|/|A|$ with gB_* , where $g \notin B_*$ are much simpler and follow from Lemma 7 (also, see Remark 10). Indeed, by this result putting $A_* = A \cap gB_*$, we have

$$K|A| \geq |AA| \geq |A_*A_*| \geq \frac{|A_*|^4}{E(A_*^{-1}, A_*)} \geq \frac{|A_*|^4}{E(A_*^{-1}, gB_*)} \geq \frac{|A_*|^2}{q-1}$$

without any assumptions on generating properties of A .

5. On Zaremba’s conjecture

In this section we apply methods of the proofs of Theorems 9, 13 to Zaremba’s conjecture but also we use the specific of this problem, i.e., the special form of the correspondent set of matrices from $\text{SL}_2(\mathbb{F}_p)$.

Denote by $F_M(Q)$ the set of all *rational* numbers $\frac{u}{v}$, $(u, v) = 1$ from $[0, 1]$ with all partial quotients in (1) not exceeding M and with $v \leq Q$:

$$F_M(Q) = \left\{ \frac{u}{v} = [0; b_1, \dots, b_s] : (u, v) = 1, 0 \leq u \leq v \leq Q, b_1, \dots, b_s \leq M \right\}.$$

By F_M denote the set of all *irrational* numbers from $[0, 1]$ with partial quotients less than or equal to M . From [Hensley 1992] we know that the Hausdorff dimension w_M of the set F_M satisfies

$$(24) \quad w_M = 1 - \frac{6}{\pi^2} \frac{1}{M} - \frac{72}{\pi^4} \frac{\log M}{M^2} + O\left(\frac{1}{M^2}\right), \quad M \rightarrow \infty,$$

however here we need a simpler result from [Hensley 1989], which states that

$$(25) \quad 1 - w_M \asymp \frac{1}{M}$$

with absolute constants in the sign \asymp . Explicit estimates for dimensions of F_M for certain values of M can be found in [Jenkinson 2004; Jenkinson and Pollicott 2001]

and in other papers. For example, see [Jenkinson and Pollicott 2001],

$$w_2 = 0.5312805062772051416244686 \dots$$

Hensley [1989; 1990] gave the bound

$$(26) \quad |F_M(Q)| \asymp_M Q^{2w_M}.$$

Now we are ready to prove Theorem 1 from the Introduction. One has

$$(27) \quad \begin{pmatrix} 0 & 1 \\ 1 & b_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & b_s \end{pmatrix} = \begin{pmatrix} p_{s-1} & p_s \\ q_{s-1} & q_s \end{pmatrix},$$

where $p_s/q_s = [0; b_1, \dots, b_s]$ and $p_{s-1}/q_{s-1} = [0; b_1, \dots, b_{s-1}]$. It is clear that $p_{s-1}q_s - p_sq_{s-1} = (-1)^s$. Let $Q = p - 1$ and consider the set $F_M(Q)$. Any $u/v \in F_M(Q)$ corresponds to a matrix from (27) such that $b_j \leq M$. The set $F_M(Q)$ splits into ratios with even s and with odd s , in other words $F_M(Q) = F_M^{\text{even}}(Q) \sqcup F_M^{\text{odd}}(Q)$. Let $A \subseteq \text{SL}_2(\mathbb{F}_p)$ be the set of matrices of the form above with even s . It is easy to see from (26), multiplying if it is needed the set $F_M^{\text{odd}}(Q)$ by $(01|1b)^{-1}$, $1 \leq b \leq M$ that $|F_M^{\text{even}}(Q)| \gg_M |F_M(Q)| \gg_M Q^{2w_M}$. It is easy to check that if for a certain n one has $A^n \cap B \neq \emptyset$, then q_{s-1} from (27) equals zero modulo p and hence there is $u/v \in F_M((2p)^n)$ such that $v \equiv 0 \pmod{p}$. In a similar way, we can easily assume that for any $g = (ab|cd) \in A$ all entries a, b, c, d are nonzero (and hence by the construction they are nonzero modulo p); see, e.g., [Hensley 1994, p. 46] (the same paper [Hensley 1994] contains the fact that A is a generating subset of $\text{SL}_2(\mathbb{F}_p)$). Analogously, we can suppose that all $g \in A$ are regular, that is, $\text{tr}(g) \neq 0, \pm 2$. Let $K = |AAA|/|A|$ and $\tilde{K} = |AA|/|A| = K^\alpha$, $0 \leq \alpha \leq 1$.

We need to estimate from below cardinality of the set of all possible traces of A , that is, cardinality of the set of sums $q_s + p_{s-1}$ (this expression is called ‘‘cyclical continuant’’). Fix p_{s-1} and q_s . Then $p_{s-1}q_s - 1 = p_sq_{s-1}$ and thus p_s is a divisor of $p_{s-1}q_s - 1$. In particular, the number of such p_s is at most p^ε for any $\varepsilon > 0$. But now knowing the pair (p_s, q_s) , we determine the correspondent matrix (27) from A uniquely. Hence the number of different pairs (p_{s-1}, q_s) is at least $\Omega_M(p^{-\varepsilon}|F_M(Q)|)$ and thus the number of different traces of all matrices from A is $\Omega_M(p^{-1-\varepsilon}|A|)$. This holds both in \mathbb{Z} and in \mathbb{F}_p because for any fixed $\lambda \in \mathbb{F}_p$ the equation $p_{s-1} + q_s \equiv \lambda \pmod{p}$ has at most p solutions. Actually, one can refine the term p^ε in $\Omega_M(p^{-1-\varepsilon}|A|)$ but it has no effect on the final bound and so below we just ignore it.

Now recall [Rudnev and Shkredov 2018, Lemma 12], which is a variant of the Helfgott map [2008] from [Murphy 2017] (we have already used similar arguments in the proof of Theorem 13). For the sake of the completeness we give the proof of a ‘‘statistical’’ version of this result.

Lemma 17. *Let G be any group and $A \subseteq G$ be a finite set. Then for an arbitrary $g \in G$, there is $A_0 \subseteq A$, $|A_0| \geq |A|/2$ such that for any $a_0 \in A_0$ the following holds:*

$$(28) \quad |A|/2 \leq |\text{Conj}(g) \cap AgA^{-1}| \cdot |\text{Centr}(g) \cap a_0^{-1}A|.$$

Here $\text{Conj}(g)$ is the conjugacy class and $\text{Centr}(g)$ is the centralizer of g in G .

Proof. Let $\varphi : A \rightarrow \text{Conj}(g) \cap AgA^{-1}$ be the Helfgott map $\varphi(a) := aga^{-1}$. One sees that $\varphi(a) = \varphi(b)$ if and only if

$$b^{-1}ag = gb^{-1}a.$$

In other words, $b^{-1}a \in \text{Centr}(g) \cap A^{-1}A$. Clearly, then

$$(29) \quad |A| = \sum_{c \in \text{Conj}(g) \cap AgA^{-1}} |\{a \in A : \varphi(a) = c\}| \\ \leq 2 \sum_{c \in \text{Conj}(g) \cap AgA^{-1} : |\{a \in A : \varphi(a) = c\}| \geq |A|/(2|\text{Conj}(g) \cap AgA^{-1}|)} |\{a \in A : \varphi(a) = c\}|.$$

For $c \in \varphi(A) \subseteq \text{Conj}(g) \cap AgA^{-1}$ put $A(c) = \varphi^{-1}(c) \subseteq A$ and let

$$A_0 = \bigsqcup_{c : |A(c)| \geq |A|/(2|\text{Conj}(g) \cap AgA^{-1}|)} A(c).$$

In other words, estimate (29) gives us

$$|A_0| = \sum_c |A(c)| \geq |A|/2.$$

But for any $b \in A_0$ one has $|\text{Centr}(g) \cap b^{-1}A| \geq |A|/(2|\text{Conj}(g) \cap AgA^{-1}|)$ as required. This completes the proof of the lemma. \square

Now summing inequality (28) over all $g \in A$ with different traces, we obtain in view of the Ruzsa triangle inequality that

$$(30) \quad |A|^2 p^{-1} \ll_M |AAA^{-1}| \cdot \max_{g \in A} |\text{Centr}(g) \cap a_0^{-1}(g)A| \\ \leq K \tilde{K} |A| \cdot \max_{g \in A} |\text{Centr}(g) \cap a_0^{-1}(g)A|.$$

Here for every $g \in A$ we have taken a concrete $a_0(g) \in A_0(g)$ but in view of Lemma 17 it is known that there are a lot of them and we will use this fact a little bit later. Now by [Helfgott 2008, Lemma 4.7], we see that

$$|(a_0^{-1}(g)A)g_*(a_0^{-1}(g)A)g_*^{-1}(a_0^{-1}(g)A)^{-1}| \gg |\text{Centr}(g) \cap a_0^{-1}(g)A|^3,$$

where $g_* = (ab|cd)$ is any element from A such that $abcd \neq 0$ in the basis where g has the diagonal form. Thanks to Lemma 14 and Remark 16 we can choose $g_* = a_0(g)$, otherwise $|A| \ll p^{3/2} K^{5/2}$. In the last case if, say, $|A| \gg p^{2-1/35}$, then

$K \gg p^{33/175}$ and hence $|A^3| \gg p^{2+4/25}$. Using Theorem 9, we see that one can take $n = 27$ and this is better than we want to prove. Then with this choice of g_* , we have by the Ruzsa triangle inequality

$$|A^2 g_*^{-1} A^{-1}| \leq |A^2 A^{-2}| \leq K^2 |A|,$$

and hence $|\text{Centr}(g) \cap a_0^{-1}(g)A| \ll K^{2/3} |A|^{1/3}$. Substituting the last bound into (30), we get

$$(31) \quad |A|^2 p^{-1} \ll_M K \tilde{K} |A| \cdot K^{2/3} |A|^{1/3}$$

and hence

$$(32) \quad K \gg_M (|A|^2 p^{-3})^{1/(5+3\alpha)} \gg p^{4w_M/(5+3\alpha)-3/(5+3\alpha)}.$$

In other words, $|AAA| \gg_M p^{2+(w_M(14+6\alpha)-13-6\alpha)/(5+3\alpha)}$. Take M sufficiently large such that $w_M(14+6\alpha) - 13 - 6\alpha > 0$. Using Theorem 9, we see that for any

$$(33) \quad n \geq \frac{w_M(28+12\alpha) - 6}{w_M(14+6\alpha) - 13 - 6\alpha}$$

one has $A^n \cap B \neq \emptyset$. On the other hand, from (32), we get

$$|AA| = |A|K^\alpha \gg p^{2+(w_M(10+10\alpha)-10-9\alpha)/(5+3\alpha)}.$$

Suppose that $w_M(10+10\alpha) - 10 - 9\alpha > 0$. It can be done if $\alpha > 0$ and if we take sufficiently large M . Applying Theorem 9 one more time, we derive that for any

$$(34) \quad n \geq \frac{2}{3} \cdot \frac{w_M(20+20\alpha) - 6\alpha}{w_M(10+10\alpha) - 10 - 9\alpha}$$

one has $A^n \cap B \neq \emptyset$. Comparing (33) and (34), we choose α optimally when

$$\alpha^2(120w_M^2 - 12w_M - 72) + \alpha(400w_M^2 - 368w_M + 6) + 280w_M^2 + 180 - 500w_M = 0$$

and it gives

$$18\alpha^2 + 19\alpha - 20 = 0$$

and whence $\alpha = \frac{1}{36}(-19 + \sqrt{1801}) + o_M(1)$ as $M \rightarrow +\infty$. Hence from (33), say, we obtain $n \geq \frac{1}{3}(47 + \sqrt{1801}) + o_M(1) > 29.81 + o_M(1)$. Taking sufficiently large M , we can choose $n = 30$. If $\alpha = 0$, then for sufficiently large M estimate (33) allows us to take $n = 23$. This completes the proof. \square

Combining the arguments above with Theorems 9, 13, we obtain Theorem 2 from the Introduction. Actually, if we apply the second part of Theorem 13, then we generate the whole $SL_2(\mathbb{F}_p)$ (and this differs our method from [Magee et al. 2019], say). Because in the case $k = 2$ we use results about growth in $SL_2(\mathbb{F}_p)$ for relatively small asymmetric set A ($|A| \gg p^{2w_2} \gg p^{1.062}$) our absolute constant C is large. It is easy to see that the arguments of this section on trace of the set A

begin to work for $w_M > \frac{3}{4}$ (see Lemma 14, as well as estimates (30), (31)) and in this case the constant C can be decreased, although it remains rather large.

Acknowledgement

We thank I.D. Kan for useful discussions and remarks.

References

- [Bourgain and Kontorovich 2011] J. Bourgain and A. Kontorovich, “On Zaremba’s conjecture”, *C. R. Math. Acad. Sci. Paris* **349**:9-10 (2011), 493–495. MR Zbl
- [Bourgain and Kontorovich 2014] J. Bourgain and A. Kontorovich, “On Zaremba’s conjecture”, *Ann. of Math. (2)* **180**:1 (2014), 137–196. MR Zbl
- [Frobenius 1896] G. Frobenius, “Über Gruppencharaktere”, *Sitzungsber. Preuss. Akad. Wiss. Berlin* **1896** (1896), 985–1021. Zbl
- [Frolenkov and Kan 2014] D. A. Frolenkov and I. D. Kan, “A strengthening of a theorem of Bourgain–Kontorovich, II”, *Mosc. J. Comb. Number Theory* **4**:1 (2014), 78–117. MR Zbl
- [Gowers 2008] W. T. Gowers, “Quasirandom groups”, *Combin. Probab. Comput.* **17**:3 (2008), 363–387. MR Zbl
- [Helfgott 2008] H. A. Helfgott, “Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$ ”, *Ann. of Math. (2)* **167**:2 (2008), 601–623. MR Zbl
- [Hensley 1989] D. Hensley, “The distribution of badly approximable numbers and continuants with bounded digits”, pp. 371–385 in *Théorie des nombres* (Quebec, 1987), edited by J.-M. De Koninck and C. Levesque, de Gruyter, Berlin, 1989. MR Zbl
- [Hensley 1990] D. Hensley, “The distribution of badly approximable rationals and continuants with bounded digits, II”, *J. Number Theory* **34**:3 (1990), 293–334. MR Zbl
- [Hensley 1992] D. Hensley, “Continued fraction Cantor sets, Hausdorff dimension, and functional analysis”, *J. Number Theory* **40**:3 (1992), 336–358. MR Zbl
- [Hensley 1994] D. Hensley, “The distribution mod n of fractions with bounded partial quotients”, *Pacific J. Math.* **166**:1 (1994), 43–54. MR Zbl
- [Hensley 1996] D. Hensley, “A polynomial time algorithm for the Hausdorff dimension of continued fraction Cantor sets”, *J. Number Theory* **58**:1 (1996), 9–45. MR Zbl
- [Jenkinson 2004] O. Jenkinson, “On the density of Hausdorff dimensions of bounded type continued fraction sets: the Texan conjecture”, *Stoch. Dyn.* **4**:1 (2004), 63–76. MR Zbl
- [Jenkinson and Pollicott 2001] O. Jenkinson and M. Pollicott, “Computing the dimension of dynamically defined sets: E_2 and bounded continued fractions”, *Ergodic Theory Dynam. Systems* **21**:5 (2001), 1429–1445. MR Zbl
- [Kan 2016] I. D. Kan, “A strengthening of a theorem of Bourgain and Kontorovich, IV”, *Izv. Ross. Akad. Nauk Ser. Mat.* **80**:6 (2016), 103–126. In Russian; translated in *Izv. Math.* **80**:6 (2016), 1094–1117. MR Zbl
- [Kontorovich 2013] A. Kontorovich, “From Apollonius to Zaremba: local-global phenomena in thin orbits”, *Bull. Amer. Math. Soc. (N.S.)* **50**:2 (2013), 187–228. MR Zbl
- [Korobov 1963] N. M. Korobov, Теоретико-числовые методы в приближенном анализе, Gosudarstv. Izdat. Fiz.-Mat. Lit., Moscow, 1963. MR

- [Magee et al. 2014] M. Magee, H. Oh, and D. Winter, “Expanding maps and continued fractions”, preprint, 2014. arXiv
- [Magee et al. 2019] M. Magee, H. Oh, and D. Winter, “Uniform congruence counting for Schottky semigroups in $SL_2(\mathbb{Z})$ ”, *J. Reine Angew. Math.* **753** (2019), 89–135. MR Zbl
- [Moshchevitin 2007] N. G. Moshchevitin, “Sets of the form $\mathcal{A} + \mathcal{B}$ and finite continued fractions”, *Mat. Sb.* **198**:4 (2007), 95–116. In Russian; translated in *Sb. Math.* **198**:3-4 (2007), 537–557. MR Zbl
- [Moshchevitin et al. 2020] N. G. Moshchevitin, B. Murphy, and I. Shkredov, “Popular products and continued fractions”, *Israel J. Math.* **238**:2 (2020), 807–835. MR Zbl
- [Murphy 2017] B. Murphy, “Upper and lower bounds for rich lines in grids”, 2017. To appear in *Amer. J. Math.* arXiv
- [Naimark 2010] M. A. Naimark, Теорија представлениј групп, Fizmatlit, Moscow, 2010.
- [Niederreiter 1986] H. Niederreiter, “Dyadic fractions with small partial quotients”, *Monatsh. Math.* **101**:4 (1986), 309–315. MR Zbl
- [Nikolov and Pyber 2011] N. Nikolov and L. Pyber, “Product decompositions of quasirandom groups and a Jordan type theorem”, *J. Eur. Math. Soc.* **13**:4 (2011), 1063–1077. MR Zbl
- [Rudnev and Shkredov 2018] M. Rudnev and I. D. Shkredov, “On growth rate in $SL_2(\mathbb{F}_p)$, the affine group and sum-product type implications”, preprint, 2018. arXiv
- [Ruzsa 1996] I. Z. Ruzsa, “Sums of finite sets”, pp. 281–293 in *Number theory* (New York, 1991–1995), edited by D. V. Chudnovsky et al., Springer, 1996. MR Zbl
- [Sarnak and Xue 1991] P. Sarnak and X. X. Xue, “Bounds for multiplicities of automorphic representations”, *Duke Math. J.* **64**:1 (1991), 207–227. MR Zbl
- [Serre 1967] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, Paris, 1967. MR Zbl
- [Shkredov 2018] I. D. Shkredov, “On asymptotic formulae in some sum-product questions”, *Tr. Mosk. Mat. Obs.* **79**:2 (2018), 271–334. In Russian; translated in *Trans. Moscow Math. Soc.* **79** (2018), 231–281.
- [Zaremba 1972] S. K. Zaremba, “La méthode des ‘bons treillis’ pour le calcul des intégrales multiples”, pp. 39–119 in *Applications of number theory to numerical analysis* (Montreal, 1971), edited by S. K. Zaremba, Academic, New York, 1972. MR Zbl

Received November 18, 2019. Revised August 12, 2020.

NIKOLAY G. MOSHCHEVITIN
 STEKLOV MATHEMATICAL INSTITUTE
 MOSCOW
 RUSSIA
 moshchevitin@gmail.com

ILYA D. SHKREDOV
 STEKLOV MATHEMATICAL INSTITUTE
 MOSCOW
 RUSSIA
 ilya.shkredov@gmail.com

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

EDITORS

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Matthias Aschenbrenner
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
matthias@math.ucla.edu

Daryl Cooper
Department of Mathematics
University of California
Santa Barbara, CA 93106-3080
cooper@math.ucsb.edu

Jiang-Hua Lu
Department of Mathematics
The University of Hong Kong
Pokfulam Rd., Hong Kong
jhlu@maths.hku.hk

Paul Balmer
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
balmer@math.ucla.edu

Wee Teck Gan
Mathematics Department
National University of Singapore
Singapore 119076
matgwt@nus.edu.sg

Sorin Popa
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
popa@math.ucla.edu

Paul Yang
Department of Mathematics
Princeton University
Princeton NJ 08544-1000
yang@math.princeton.edu

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Kefeng Liu
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
liu@math.ucla.edu

Jie Qing
Department of Mathematics
University of California
Santa Cruz, CA 95064
qing@cats.ucsc.edu

PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org

SUPPORTING INSTITUTIONS

ACADEMIA SINICA, TAIPEI
CALIFORNIA INST. OF TECHNOLOGY
INST. DE MATEMÁTICA PURA E APLICADA
KEIO UNIVERSITY
MATH. SCIENCES RESEARCH INSTITUTE
NEW MEXICO STATE UNIV.
OREGON STATE UNIV.

STANFORD UNIVERSITY
UNIV. OF BRITISH COLUMBIA
UNIV. OF CALIFORNIA, BERKELEY
UNIV. OF CALIFORNIA, DAVIS
UNIV. OF CALIFORNIA, LOS ANGELES
UNIV. OF CALIFORNIA, RIVERSIDE
UNIV. OF CALIFORNIA, SAN DIEGO
UNIV. OF CALIF., SANTA BARBARA

UNIV. OF CALIF., SANTA CRUZ
UNIV. OF MONTANA
UNIV. OF OREGON
UNIV. OF SOUTHERN CALIFORNIA
UNIV. OF UTAH
UNIV. OF WASHINGTON
WASHINGTON STATE UNIVERSITY

These supporting institutions contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its contents or policies.


See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2020 is US \$520/year for the electronic version, and \$705/year for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2020 Mathematical Sciences Publishers

PACIFIC JOURNAL OF MATHEMATICS

Volume 309 No. 1 November 2020

- Lie 2-algebras of vector fields 1
DANIEL BERWICK-EVANS and EUGENE LERMAN
- Lower regularity solutions of the biharmonic Schrödinger equation in a quarter plane 35
ROBERTO DE A. CAPISTRANO-FILHO, MÁRCIO CAVALCANTE
and FERNANDO A. GALLEGO
- The arithmetic Hodge index theorem and rigidity of dynamical systems over function fields 71
ALEXANDER CARNEY
- On the vanishing of the theta invariant and a conjecture of Huneke and Wiegand 103
OLGUR CELIKBAS
- Algebraic and geometric properties of flag Bott–Samelson varieties and applications to representations 145
NAOKI FUJITA, EUNJEONG LEE and DONG YOUP SUH
- On a modular form of Zaremba’s conjecture 195
NIKOLAY G. MOSHCHEVITIN and ILYA D. SHKREDOV
- The first nonzero eigenvalue of the p -Laplacian on differential forms 213
SHOO SETO
- Global regularity of the Navier–Stokes equations on 3D periodic thin domain with large data 223
NA ZHAO



0030-8730(202011)309:1;1-J