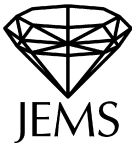
J. Eur. Math. Soc. 10, 987–1011



Jean Bourgain · Alex Gamburd

Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$: I

Received December 11, 2007

Abstract. We prove that the Cayley graphs of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ are expanders with respect to the projection of any fixed elements in $\mathrm{SL}_2(\mathbb{Z})$ generating a Zariski dense subgroup.

1. Introduction

Expanders are highly-connected sparse graphs widely used in computer science, in areas ranging from parallel computation to complexity theory and cryptography; recently they have also found some remarkable applications in pure mathematics; see [15, 17, 20] and references therein. Given an undirected d-regular graph $\mathcal{G}$ and a subset X of V, the *expansion* of X, $c(X)$, is defined to be the ratio $|\partial(X)|/|X|$, where $\partial(X) = \{y \in \mathcal{G} : \mathrm{dist}(y, X) = 1\}$. The *expansion coefficient* of a graph $\mathcal{G}$ is defined as follows:

$$c(\mathcal{G}) = \inf\left\{c(X) : |X| < \frac{1}{2}|\mathcal{G}|\right\}.$$

A family of d-regular graphs $\mathcal{G}_{n,d}$ forms a family of *C-expanders* if there is a fixed positive constant C such that

$$\liminf_{n\to\infty} c(\mathcal{G}_{n,d}) \geq C. \tag{1.1}$$

The *adjacency matrix* of $\mathcal{G}$, $A(\mathcal{G})$, is the $|\mathcal{G}|$ by $|\mathcal{G}|$ matrix, with rows and columns indexed by vertices of $\mathcal{G}$, such that the x, y entry is 1 if x and y are adjacent, and 0 otherwise.

Using the discrete analogue of the Cheeger–Buser inequality, proved by Alon and Milman, the condition (1.1) can be rewritten in terms of the second largest eigenvalue of the adjacency matrix $A(\mathcal{G}_{n,d})$ as follows:

$$\limsup_{n\to\infty} \lambda_1(A(\mathcal{G}_{n,d})) < d. \tag{1.2}$$

J. Bourgain: School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA; e-mail: bourgain@math.ias.edu

A. Gamburd: Department of Mathematics, University of California at Santa Cruz, 1156 High Street, Santa Cruz, CA 95064, USA, and School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA; e-mail: agamburd@ucsc.edu

Given a finite group G with a symmetric set of generators S, the *Cayley graph* $\mathcal{G}(G, S)$ is a graph which has elements of G as vertices and which has an edge from x to y if and only if $x = \sigma y$ for some $\sigma \in S$. Let S be a set of elements in $\mathrm{SL}_2(\mathbb{Z})$. If $\langle S \rangle$, the group generated by S, is a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, Selberg's theorem [22] implies (see e.g. [17, Theorem 4.3.2]) that $\mathcal{G}(\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}), \pi_N(S))$ (where $\pi_N(S)$ is the natural projection of S modulo N) form a family of expanders as $N \to \infty$. A basic problem, posed by Lubotzky [17, 18] and Lubotzky and Weiss [19], is to what extent expansion is a property of the family of groups alone, independent of the choice of generators. In [23] Shalom gave an example of an infinite-index subgroup in $\mathrm{PSL}_2(\mathbb{Z}[\omega])$ (where ω is a primitive third root of unity) yielding a family of $\mathrm{SL}_2(\mathbb{F}_p)$ expanders. In [12] it is proved that if S is a set of elements in $\mathrm{SL}_2(\mathbb{Z})$ such that the Hausdorff dimension of the limit set is greater than $5/6$, then $\mathcal{G}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), \pi_p(S))$ form a family of expanders (in fact, the proof given in [12] for prime modulus p easily generalizes to arbitrary modulus).

In [3] it is shown that $\mathcal{G}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), \pi_p(S))$, where p is a prime, form a family of expanders if S generates a nonelementary subgroup of $\mathrm{SL}_2(\mathbb{Z})$ (this is clearly a necessary condition); in [6] this result is extended to square-free moduli q. In the present paper we extend the results from [3, 6] to the case of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$, where p is a fixed prime and n tends to infinity; the question of uniform expansion bounds for this family was raised by Shalom in [24].

Theorem 1.1. *Let S be a symmetric set of elements in $\mathrm{SL}_2(\mathbb{Z})$ generating a Zariski dense subgroup. Let p be a fixed sufficiently large prime. The family of Cayley graphs $\mathcal{G}(\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}), \pi_{p^n}(S))$ forms a family of expanders.*

Remark. The prime p must be chosen sufficiently large to ensure that $\pi_p(S)$ generates $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

As in [3, 6], the proof, following the approach of Sarnak and Xue [21], is based on exploiting high multiplicity of nontrivial eigenvalues, together with the sharp upper bound on the number of short closed geodesics. The proof of the required multiplicity bound is presented in Section 7. As in [6], the starting point for the proof of the upper bound is the appropriate sum-product estimate—in our case we need the sum-product estimate for $\mathbb{Z}/p^n\mathbb{Z}$ recently established in [2]. In fact, we need a slight strengthening of a result in [2], presented in Section 2. The proof in [6] then proceeds by establishing the generalization of Helfgott's product theorem [14] in $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ for q square-free. In [14, 6] sum-product estimates enter via trace amplification. The proof in the present paper is different, relying on a "multi-scale" approach, reminiscent of the Solovay–Kitaev algorithm in quantum computation [11] (see [13] for an $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ analogue, yielding uniform polylog diameter bounds). The "multi-scale" structure in $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ is encapsulated in the identity

$$(I + QA)(I + QB) \equiv I + Q(A + B) \,(\mathrm{mod}\, Q^2),$$

which allows for immediate exploitation of the sum structure. The exploitation of the product structure is based on producing a large set of commuting elements, diagonalized in the appropriate basis, and then proceeding by conjugation. To execute this argument we need to produce elements outside of proper subvarieties, which is accomplished by

analyzing the random walk in $\mathrm{SL}_2(\mathbb{Z})$ based on the generating set S and using the expansion property modulo p (established in [3]). In Section 9 we outline an alternative approach, based on the theory of products of random matrices and generalizing to arbitrary rank. As in [3], the required upper bound is obtained from a measure convolution result (Section 3), which is established using noncommutative product-set estimates due to Tao [25, 26].

The generalization of Theorem 1.1 to $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ with $d > 2$ will be presented in [5].

2. The sum-product theorem in $\mathbb{Z}_q$, $q = p^n$

We consider $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, $q = p^n$, with $p \neq 2$ fixed. For $A \subset \mathbb{Z}_q$ and $r, s \in \mathbb{Z}_+$, we denote by $rA^{(s)}$ the r-fold sumset of the s-fold product set $A^{(s)}$ of A.

Recall the result from [2] (the Corollary on p. 6).

Proposition 2.1. *Given $\delta > 0$ and $\tau > 0$, there are $\varepsilon > 0$ and $r, s \in \mathbb{Z}_+$ such that the following holds. Let q be as above and $A \subset \mathbb{Z}_q$ satisfying*

$$|\pi_{q_1}(A)| > q_1^{\delta} \quad \text{for all } q_1 \mid q,\ q_1 > q^{\varepsilon}. \tag{2.1}$$

Then there is $Q \mid q$, $Q < q^{\tau}$, such that

$$rA^{(s)} \supset Q\mathbb{Z}_q. \tag{2.2}$$

We may derive from Proposition 2.1 the following consequence, where the assumption (2.1) has been weakened.

Proposition 2.2. *Given $\delta > 0$, there is $\varepsilon > 0$ and positive integers $r, s < C(\delta)$ such that if q is as above, $q_1 \mid q$, $q_1 < q^{\varepsilon}$ and $A \subset \mathbb{Z}_q$ satisfies*

$$|\pi_{q_1}(A)| > q_1^{\delta} \tag{2.3}$$

then

$$\pi_{q_4}(rA^{(s)} - rA^{(s)}) \supset q_5\mathbb{Z}_{q_4} \tag{2.4}$$

for some divisors $q_5 \mid q_4$, $q_4 \mid q$ with $q_4/q_5 > q_1^{\delta/4}$ and $\log q_4 < C(\delta)\log q_1$.

Proof. As will be clear from what follows, it is important that $\varepsilon < \varepsilon(\delta)$. We make the following construction.

Take $q_2 \mid q_1$ maximal such that

$$\max_{\xi \in \mathbb{Z}_{q_2}} |\{x \in \pi_{q_1}(A) : \pi_{q_2}(x) = \xi\}| > q_2^{-\delta/2}|\pi_{q_1}(A)|. \tag{2.5}$$

Since (2.3) implies that $q_1/q_2 > q_2^{-\delta/2}q_1^{\delta}$, it follows that $q_3 = q_1/q_2 > q_1^{\delta/2}$.

If $\xi \in \mathbb{Z}_{q_2}$ satisfies (2.5), it follows from the maximality of q_2 that if $q' \mid q_3$ we have

$$(q_2 q')^{-\delta/2}|\pi_{q_1}(A)| \geq \max_{\substack{\xi' \in \mathbb{Z}_{q_2 q'} \\ \pi_{q_2}(\xi')=\xi}} |\{x \in \pi_{q_1}(A) : \pi_{q_2 q'}(x) = \xi'\}|$$
$$\geq \frac{|\{x \in \pi_{q_1}(A) : \pi_{q_2}(x) = \xi\}|}{|\{\pi_{q_2 q'}(x) : x \in \pi_{q_1}(A),\ \pi_{q_2}(x) = \xi\}|}, \tag{2.6}$$

and hence by (2.5),

$$|\{\pi_{q_2 q'}(x) : x \in A,\ \pi_{q_2}(x) = \xi\}| > (q')^{\delta/2}. \tag{2.7}$$

Therefore, defining

$$B = \{x \in \mathbb{Z}_{q/q_2} : q_2 x \in A - A\},$$

we get

$$|\pi_{q'}(B)| \geq (q')^{\delta/2} \quad \text{if } q' \mid q_3. \tag{2.8}$$

We now apply Proposition 2.1 with modulus q_3 to the set $\pi_{q_3}(B)$, replacing δ by $\delta/2$ and letting $\tau = 1/2$, $\varepsilon = 0$. Thus by (2.2), there is $Q \mid q$, $Q < q_3^{1/2}$, such that for some $r, s \in \mathbb{Z}_+$, $r, s < C(\delta)$, we have

$$\pi_{q_3}(r B^{(s)}) \supset Q\mathbb{Z}_{q_3}, \tag{2.9}$$

and therefore

$$\pi_{q_2^s q_3}(r(A - A)^{(s)}) \supset Q q_2^s \mathbb{Z}_{q_2^s q_3}. \tag{2.10}$$

We assume here

$$(s + 1)\varepsilon < C(\delta)\varepsilon < 1, \tag{2.11}$$

so that $q_4 = q_2^s q_3 < q$. Setting $q_5 = Q q_2^s$, we thus have

$$q_5 \mid q_4 \quad \text{and} \quad q_4/q_5 > q_1^{\delta/4}, \tag{2.12}$$

and therefore, by (2.9), we obtain

$$\pi_{q_4}(r2^{s-1}A^{(s)} - r2^{s-1}A^{(s)}) \supset \pi_{q_4}(r(A - A)^{(s)}) \supset q_5\mathbb{Z}_{q_4}. \tag{2.13}$$

□

Remarks. (i) Proposition 2.1 (respectively 2.2) holds equally well if instead of a single subset $A \subset \mathbb{Z}_q$ we consider s distinct sets $A_1, \ldots, A_s \subset \mathbb{Z}_q$ satisfying condition (2.1) (respectively (2.3)).

(ii) In Section 5 we will actually rely on Proposition 2.1 and the initial construction in the proof of Proposition 2.2.

3. Measure convolution

The following result is proven using the noncommutative Balog–Szemerédi–Gowers theorem due to Tao (see [25, 26]). The argument is analogous to the one in the proof of Proposition 2 in [3].

Lemma 3.1. *Let G be a finite group, $N = |G|$. Suppose $\mu \in \mathcal{P}(G)$ is a symmetric probability measure on G and assume*

$$\|\mu\|_\infty < N^{-\gamma}, \tag{3.1}$$

$$\|\mu\|_2 > N^{-1/2+\gamma} \tag{3.2}$$

with $\gamma > 0$ an arbitrary given constant. Assume further that

$$\|\mu * \mu\|_2 > N^{-\varepsilon}\|\mu\|_2 \tag{3.3}$$

with $0 < \varepsilon < \varepsilon(\gamma)$. Then there exists a subset $H \subset G$ with the following properties:

$$\begin{aligned} &H = H^{-1} \text{ and there exists a subset } X \subset G,\ |X| < N^{\varepsilon'},\\ &\text{such that } H.H \subset X.H \text{ and } H.H \subset H.X; \end{aligned} \tag{3.4}$$

$$\mu(x_0 H) > N^{-\varepsilon'} \quad \text{for some } x_0 \in G; \tag{3.5}$$

$$|H| < N^{1-\gamma} \tag{3.6}$$

and where $\varepsilon' \sim \varepsilon$.

Remark. In [26], any H satisfying (3.4) is called an $N^{\varepsilon'}$-approximate subgroup of G. In particular, H satisfies the product set estimates

$$|H^{(s)}| = |\underbrace{H \dots H}_{s\text{-fold}}| < q^{(s-1)\varepsilon'}|H| \quad \text{for } s \geq 1. \tag{3.7}$$

Our measure μ will be obtained as a convolution $\mu = \nu^{(\ell)} = \underbrace{\nu * \cdots * \nu}_{\ell\text{-fold}}$, where ν is a symmetric probability measure on G, $|\mathrm{supp}\ \nu| < C$ and $\ell \sim \log N$.

Assume μ satisfies (3.1)–(3.3) and take $H \subset G$ satisfying (3.4)–(3.6). Fix $\ell_0 < \ell$ and write

$$N^{-\varepsilon'} \overset{(3.5)}{<} \mu(x_0 H) = \sum_{y \in G} \nu^{(\ell-\ell_0)}(y)\nu^{(\ell_0)}(y^{-1}x_0 H),$$

implying

$$\nu^{(\ell_0)}(x_1 H) > N^{-\varepsilon'} \quad \text{for some } x_1 \in G. \tag{3.8}$$

Hence

$$\begin{aligned} \nu^{(2\ell_0)}(H.H) &\geq \sum_{y \in x_1 H, z \in H^{-1}H} \nu^{(\ell_0)}(y)\nu^{(\ell_0)}(zy^{-1}) \geq \sum_{y \in x_1 H,\, w \in H} \nu^{(\ell_0)}(y)\nu^{(\ell_0)}(w^{-1}x_1^{-1}) \\ &= [\nu^{(\ell_0)}(x_1 H)]^2 \overset{(3.8)}{>} N^{-2\varepsilon'}. \end{aligned} \tag{3.9}$$

4. Random walks in $\mathrm{SL}_2(\mathbb{Z})$

Fix a symmetric set $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, $|\Gamma| = 2k$, generating a free group. We consider the probability measure

$$\nu = \frac{1}{2k} \sum_{g \in \Gamma} \delta_g.$$

We denote by $\mathrm{Mat}_2(R)$ the two by two matrices with entries in the ring R, and by $\mathrm{SL}_2(q)$ the group $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$. For $q \in \mathbb{Z}_+$, let $\pi_q : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(q)$ be the quotient map. Let $\pi_q[\nu]$ be the image measure of ν on $\mathrm{SL}_2(q)$; when there is no possibility of confusion we will denote it again by ν.

Lemma 4.1. *Let $f = f(g_1, \dots, g_r)$ be a given polynomial on $\mathrm{Mat}_2(\mathbb{Z})^r$, with integer coefficients (we identify $\mathrm{Mat}_2(\mathbb{Z})$ with $\mathbb{Z}^4$). Assume that f does not vanish identically on $\mathrm{SL}_2(\mathbb{Z})^r$. Then*

$$\sum_{f(g_1,\dots,g_r)=0} \nu^{(\ell)}(g_1) \cdots \nu^{(\ell)}(g_r) < c_f e^{-c_\Gamma \ell}. \tag{4.1}$$

Proof. We will use the expansion property of $\pi_P[\nu]$ for P prime (see [3]); see Section 9 for an argument relying only on the Zariski density of $\langle \mathrm{supp}\, \nu \rangle \subset \mathrm{SL}_2(\mathbb{Z})$ and generalizing to arbitrary rank.

Fix a prime P such that

$$\ell > \log P > c_\Gamma \ell, \tag{4.2}$$

$$\max_{z \in \mathrm{SL}_2(P)} \pi_p[\nu^{(\ell)}](z) < 2/P^3 \tag{4.3}$$

(we use here the result from [3]).

Define

$$S = \{(z_1, \dots, z_r) \in \mathrm{SL}_2(P)^r : f(z_1, \dots, z_r) = 0 \,(\mathrm{mod}\, P)\}.$$

It follows from our assumption on f that for P large enough

$$|S| < c_f P^{3r-1}. \tag{4.4}$$

Since $f(g_1, \dots, g_r) = 0$ implies $f(g_1, \dots, g_r) \equiv 0 \,(\mathrm{mod}\, P)$, the left side of (4.1) is bounded by

$$\sum_{(z_1,\dots,z_r) \in S} \pi_P[\nu^{(\ell)}](z_1) \cdots \pi_P[\nu^{(\ell)}](z_r) \overset{(4.3)}{<} \frac{2^r}{P^{3r}} |S| \overset{(4.4)}{<} \frac{C_f}{P} \overset{(4.2)}{<} C_f e^{-c_\Gamma \ell}. \qquad \square$$

There is the obvious consequence:

Corollary 4.1. *Let $f = f(g_1, \dots, g_r)$ be as in Lemma 4.1. Then for*

$$\ell < c(\Gamma, f) \log q \tag{4.5}$$

we have

$$\sum_{f(g_1,\dots,g_r) \equiv 0 \,(\mathrm{mod}\, q)} \nu^{(\ell)}(g_1) \cdots \nu^{(\ell)}(g_r) < C_f e^{-c_\Gamma \ell}. \tag{4.6}$$

We now apply the considerations from Section 3 with $G = \mathrm{SL}_2(q)$ (hence $|G| \sim q^3$) to obtain the following corollary. We use the same notation.

Corollary 4.2. *Let $f_i = f_i(g_1, \dots, g_r)$ $(1 \le i \le j)$ be a given set of polynomials each satisfying the assumptions of Lemma* 4.1. *Let ε be as in* (3.3)*, and (assuming q large and ε small enough) take ℓ_0 satisfying*

$$c(\Gamma, f) \log q > \ell_0 > C_f + rC_\Gamma \varepsilon \log q. \tag{4.7}$$

There are elements $z_1, \dots, z_r \in H.H \cap \{\pi_q(g) : \|g\| < C_\Gamma^{\ell_0}\}$ such that

$$f_i(z_1, \dots, z_r) \neq 0 \quad \text{for } i = 1, \dots, j.$$

Proof. Considering $f = \prod_{i=1}^{j} f_i$, we may take $j = 1$.

If the conclusion fails to hold, then from (3.9) and (4.6), assuming ℓ_0 satisfies (4.5), we have

$$C_f e^{-c_\Gamma \ell_0} > \sum_{f(z_1,\dots,z_r)=0} \nu^{(\ell_0)}(z_1) \cdots \nu^{(\ell_0)}(z_r) \ge [\nu^{(\ell_0)}(H.H)]^r > q^{-2r\varepsilon'}, \tag{4.8}$$

contradicting the second inequality in (4.7). □

Corollary 4.3. *There are elements $g_1, g_2, g_3 \in H.H$ satisfying*

$$\|g_i\| < q^{C\varepsilon}, \tag{4.9}$$

$$\det(1, g_1, g_2, g_3) \neq 0. \tag{4.10}$$

Proof. Apply Corollary 4.2 with $r = 3$ considering the polynomial $f(g_1, g_2, g_3) = \det(1, g_1, g_2, g_3)$, which obviously satisfies the condition of Lemma 4.1 . □

Note that if $g \in \mathrm{Mat}_2(q)$ satisfies

$$\mathrm{Tr}\, g = \mathrm{Tr}\, g_1 g = \mathrm{Tr}\, g_2 g = \mathrm{Tr}\, g_3 g = 0 \,(\mathrm{mod}\, q)$$

then

$$\det(1, g_1, g_2, g_3) \cdot g = 0 \,(\mathrm{mod}\, q).$$

Hence, if $\{g_1, g_2, g_3\}$ satisfy (4.9), (4.10), it follows that the map

$$\mathrm{Mat}_2(q) \to \mathbb{Z}_q^4 : g \mapsto (\mathrm{Tr}\, g, \mathrm{Tr}\, g_1 g, \mathrm{Tr}\, g_2 g, \mathrm{Tr}\, g_3 g) \tag{4.11}$$

has multiplicity at most $q^{C\varepsilon}$.

Proposition 4.1. *Let $a_1, \dots, a_j \in \mathbb{Z}$, and let $q_0 \mid q$ and $\xi_1, \dots, \xi_j \in \mathrm{Mat}_2(\mathbb{Z})$ be such that*

$$\pi_{q_0}(\xi_i) \neq 0 \quad (1 \le i \le j). \tag{4.12}$$

Let $q_1 \mid q$, $q_1 > q^{C\varepsilon} q_0$. There is $g \in H.H$, $\|g\| < q^{C\varepsilon}$, satisfying

$$\mathrm{Tr}\, \xi_i g \neq a_i \,(\mathrm{mod}\, q_1) \quad \text{for } i = 1, \dots, j. \tag{4.13}$$

Proof. Fix $\xi \in \mathrm{Mat}_2(\mathbb{Z})$, $\pi_{q_0}(\xi) \neq 0$. Take $\ell_0 \sim \varepsilon \log q$ and define

$$S = \{g \in \mathrm{Mat}_2(\mathbb{Z}) : \|g\| < C^{\ell_0} \text{ and } \mathrm{Tr}\,\xi g = a \pmod{q_1}\}. \tag{4.14}$$

It follows that for $g_0, g_1, g_2, g_3, g_4 \in S$ we have

$$\det(g_1 - g_0, g_2 - g_0, g_3 - g_0, g_4 - g_0) \cdot \xi = 0 \pmod{q_1}. \tag{4.15}$$

Assuming

$$C^{4\ell_0} q_0 < q_1, \tag{4.16}$$

we conclude from our assumption on ξ that

$$\det(g_1 - g_0, g_2 - g_0, g_3 - g_0, g_4 - g_0) = 0. \tag{4.17}$$

Choosing the constant C in (4.14) appropriately, it follows from (4.1) that

$$[\nu^{(2\ell_0)}(S)]^5 < Ce^{-c\ell_0}. \tag{4.18}$$

Hence, for appropriate choice of ℓ_0,

$$\nu^{(2\ell_0)}(S) < q^{-C\varepsilon}. \tag{4.19}$$

Recalling also (3.9), the conclusion easily follows. □

Remark. Here and in the sequel, all constants may depend on Γ.

There is the following variant of Proposition 4.1.

Proposition 4.2. *Let $q_0 \mid q$ and $\xi_1, \ldots, \xi_j \in \mathrm{Mat}_2(\mathbb{Z})$ be such that*

$$\pi_{q_0}(\xi_i) \neq 0 \quad (1 \leq i \leq j). \tag{4.20}$$

Let $q_1 \mid q$, $q_1 > q^{C\varepsilon} q_0$. For

$$C\varepsilon \log q < \ell_1 < \ell \tag{4.21}$$

we have

$$|\{g \in H.H : \|g\| < C^{\ell_1} \text{ and } \mathrm{Tr}\,\xi_i g \neq a_i \pmod{q_1}\}| > e^{c\ell_1}. \tag{4.22}$$

Proof. For $\ell_0 < \ell_1 < \ell$ and ℓ_0 as in the proof of Proposition 4.1, write

$$\begin{aligned}\sum_{\mathrm{Tr}\,\xi g \equiv 0 \pmod{q_1}} \nu^{(2\ell_1)}(g) &= \sum_{g_1} \nu^{(2\ell_1 - 2\ell_0)}(g_1) \sum_{\mathrm{Tr}\,\xi g \equiv 0 \pmod{q_1}} \nu^{(2\ell_0)}(g_1^{-1} g) \\ &\leq \max_{g_1 \in \mathrm{SL}_2(\mathbb{Z})} \sum_{\mathrm{Tr}\,\xi g_1 g' \equiv 0 \pmod{q_1}} \nu^{(2\ell_0)}(g') \\ &< q^{-C\varepsilon}\end{aligned} \tag{4.23}$$

(by (4.19)). By (3.9) (applied with ℓ_1)

$$\nu^{(2\ell_1)}(H.H) > q^{-2\varepsilon'} > q^{-\frac{1}{2}C\varepsilon}. \tag{4.24}$$

Hence, from (4.23), (4.24),

$$\nu^{(2\ell_1)}\{g \in H.H : \mathrm{Tr}\,\xi_1 g \neq a_i \pmod{q_1} \text{ for } i = 1, \ldots, j\} > q^{-C\varepsilon}, \tag{4.25}$$

and since Γ generates a free group, applying Kesten's theorem [16], (4.22) follows. □

Proposition 4.3. *Let $\xi \in \mathrm{Mat}_2(\mathbb{Z})$ be such that*

$$\mathrm{Tr}\,\xi = 0, \tag{4.26}$$

$$\pi_p(\xi) \neq 0. \tag{4.27}$$

There are $g_1, g_2 \in H.H$ satisfying

$$\|g_i\| < q^{C\varepsilon}, \tag{4.28}$$

$$\det(1, \xi, g_1\xi g_1^{-1}, g_2\xi g_2^{-1}) \neq 0 \,(\mathrm{mod}\, q_0) \quad \textit{for some } q_0 \mid q,\ q_0 < q^{C\varepsilon}. \tag{4.29}$$

Remark. An important point to note here is that ξ is only subject to assumptions (4.26), (4.27), while $\|\xi\|$ may be arbitrarily large (in particular, $\|\xi\|$ may be larger than $q^{C\varepsilon}$).

Proof of Proposition 4.3. Fix $q_1 \mid q$, $q_1 = q^{C\varepsilon}$, to be specified below. We distinguish two cases.

Case 1: $\det\xi \neq 0 \,(\mathrm{mod}\, q_1)$. It will suffice to find $g_1, g_2 \in H.H$ such that (4.28) holds and

$$\det(1, \xi, g_1\xi g_1^{-1} - g_1^{-1}\xi g_1, g_2\xi g_2^{-1} - g_2^{-1}\xi g_2) \neq 0 \,(\mathrm{mod}\, q_0). \tag{4.30}$$

Since

$$g\xi g^{-1} - g^{-1}\xi g = (\mathrm{Tr}\, g)[g, \xi],$$

we impose the conditions

$$\mathrm{Tr}\, g_1 \neq 0 \,(\mathrm{mod}\, q_2), \tag{4.31}$$

$$\mathrm{Tr}\, g_2 \neq 0 \,(\mathrm{mod}\, q_2), \tag{4.32}$$

$$\det(1, \xi, [g_1, \xi], [g_2, \xi]) \neq 0 \,(\mathrm{mod}\, q_2). \tag{4.33}$$

We take q_2 such that

$$q_2^3 \mid q_0 \quad \text{and} \quad q_1^6 \mid q_2. \tag{4.34}$$

Assume (4.33) fails to hold, thus $\det(1, \xi, [g_1, \xi], [g_2, \xi]) = 0 \,(\mathrm{mod}\, q_2)$. Then there are $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $(\alpha, \beta, \gamma, \delta) = 1$ and

$$\alpha + \beta\xi + \gamma[g_1, \xi] + \delta[g_2, \xi] = 0 \,(\mathrm{mod}\, q_2). \tag{4.35}$$

Since

$$\mathrm{Tr}\,\xi = \mathrm{Tr}[g_1, \xi] = \mathrm{Tr}[g_2, \xi] = \mathrm{Tr}\,\xi[g_1, \xi] = \mathrm{Tr}\,\xi[g_2, \xi] = 0$$

and $\mathrm{Tr}\,\xi^2 = -2\det\xi$, we deduce from (4.35) that

$$\alpha = 0 \,(\mathrm{mod}\, q_2) \quad \text{and} \quad \beta = 0 \left(\mathrm{mod}\, \frac{q_2}{q_1}\right).$$

Hence

$$\gamma[g_1, \xi] + \delta[g_2, \xi] = 0 \left(\mathrm{mod}\, \frac{q_2}{q_1}\right),$$

implying

$$\gamma \operatorname{Tr}([g_1, \xi]g_2) = 0 \left(\operatorname{mod} \frac{q_2}{q_1} \right).$$

In order to get a contradiction, we require

$$[g_1, \xi] \neq 0 \,(\operatorname{mod} q_1), \tag{4.36}$$

$$[g_2, \xi] \neq 0 \,(\operatorname{mod} q_1), \tag{4.37}$$

$$\operatorname{Tr}([g_1, \xi]g_2) \neq 0 \,(\operatorname{mod} q_1^2). \tag{4.38}$$

Summarizing, we need g_1, g_2 to satisfy (4.31), (4.32), (4.36), (4.37), (4.38). This is accomplished by applying Proposition 4.1. First take $g_1 \in H.H$, $\|g_1\| < q^{C\varepsilon}$, satisfying (4.31), (4.36). Then take $g_2 \in H.H$, $\|g_2\| < q^{C\varepsilon}$, and such that (4.32), (4.37) hold. This is possible indeed if $q_1 > q^{C\varepsilon}$.

Case 2: $\det \xi = 0 \,(\operatorname{mod} q_1)$. Thus $\xi^2 = 0 \,(\operatorname{mod} q_1)$. Recalling (4.27), take $e \in \{(1, 0), (0, 1)\}$ such that $\pi_p(\xi e) \neq 0$. Making a base change $T : (e_1, e_2) \mapsto (\xi e, e)$, we obtain

$$T^{-1} \xi T = \tilde{\xi} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} (\operatorname{mod} q_1). \tag{4.39}$$

Setting also $\tilde{g} = T^{-1} g T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we have $(\operatorname{mod} q_1)$

$$\tilde{g}\tilde{\xi}(\tilde{g})^{-1} = a^2 \tilde{\xi} + c \begin{pmatrix} -a & 0 \\ -c & a \end{pmatrix}. \tag{4.40}$$

Hence

$$\begin{aligned} &\det(1, \xi, g_1 \xi g_1^{-1}, g_2 \xi g_2^{-1}) \\ &\quad = \det(1, \tilde{\xi}, \tilde{g}_1 \tilde{\xi} (\tilde{g}_1)^{-1}, \tilde{g}_2 \tilde{\xi} (\tilde{g}_2)^{-1}) = 2c_1 c_2 (a_1 c_2 - a_2 c_1) \,(\operatorname{mod} q_1). \end{aligned} \tag{4.41}$$

Assume $e = (1, 0)$. Hence

$$\xi_{2,1} \neq 0 \,(\operatorname{mod} p).$$

For $i = 1, 2$ we have

$$c_i = \langle \tilde{g}_i e_1, e_2 \rangle = \langle g_i T e_1, (T^{-1})^* e_2 \rangle = \frac{1}{\xi_{21}} \left\langle g_i \begin{pmatrix} \xi_{11} \\ \xi_{21} \end{pmatrix}, \begin{pmatrix} \xi_{21} \\ -\xi_{11} \end{pmatrix} \right\rangle \tag{4.42}$$

and

$$a_1 c_2 - a_2 c_1 = \frac{1}{\xi_{21}} \det \left(g_2 \begin{pmatrix} \xi_{11} \\ \xi_{21} \end{pmatrix}, g_1 \begin{pmatrix} \xi_{11} \\ \xi_{21} \end{pmatrix} \right). \tag{4.43}$$

Take $g_1 \in H.H$, $\|g_1\| < g^{C\varepsilon}$, such that

$$\left\langle g_1 \begin{pmatrix} \xi_{11} \\ \xi_{21} \end{pmatrix}, \begin{pmatrix} \xi_{21} \\ -\xi_{11} \end{pmatrix} \right\rangle \neq 0 \,(\operatorname{mod} q_3) \tag{4.44}$$

with $q_3 \mid q$, $q_3 < q^{C\varepsilon}$.

Next, take $g_2 \in H.H$, $\|g_2\| < q^{C\varepsilon}$, with

$$\left\langle g_2 \begin{pmatrix} \xi_{11}, \\ \xi_{21} \end{pmatrix}, \begin{pmatrix} \xi_{21} \\ -\xi_{11} \end{pmatrix} \right\rangle \neq 0 \,(\mathrm{mod}\, q_3), \tag{4.45}$$

$$\det\left(g_2 \begin{pmatrix} \xi_{11} \\ \xi_{21} \end{pmatrix}, g_1 \begin{pmatrix} \xi_{11} \\ \xi_{21} \end{pmatrix} \right) \neq 0 \,(\mathrm{mod}\, q_3). \tag{4.46}$$

Recalling (4.41), take $q_1 > q_3^3$.

This completes the proof of Proposition 4.3. □

5. Sets of commuting elements

We first obtain a large set of commuting elements by an argument similar to that in Section 4.1 of [14]. Take $g_1, g_2, g_3 \in H.H$ satisfying (4.9)–(4.11). We set $g_0 = 1$.

From Proposition 4.2 applied with $q_0 = p$, $\{\xi_1, \ldots, \xi_4\} = \{1, g_1, g_2, g_3\}$, we get

$$|\{g \in H.H : \|g\| < C^{\ell_1} \text{ and } \mathrm{Tr}\, g_i g \neq \pm 2 \,(\mathrm{mod}\, q_1)\}| > e^{c\ell_1}. \tag{5.1}$$

Here $q_1 \mid q$, $q_1 = p^{r_1} < q^{C\varepsilon}$ and $C\varepsilon \log q < \ell_1 \leq n$.

Since the map $\mathrm{Mat}_2(q) \to \mathbb{Z}_q^4 : g \mapsto (\mathrm{Tr}\, g_i g)_{0 \leq i \leq 3}$ has multiplicity at most $q^{C\varepsilon}$, it follows from (5.1) that for some $i \in \{0, 1, 2, 3\}$ we have

$$|\{\mathrm{Tr}\, g_i g : g \in H.H, \|g\| < C^{\ell_1} \text{ and } \pi_{q_1}(g_i g) \neq \pm 1\}| > (q^{-C\varepsilon} e^{c\ell_1})^{1/4} > e^{c\ell_1}. \tag{5.2}$$

This yields elements $(h_\alpha)_{1 \leq \alpha \leq \beta}$ in $H^{(4)}$, $\beta > e^{c\ell_1}$, satisfying

$$\|h_\alpha\| < q^{C\varepsilon} C^{\ell_1} < C^{2\ell_1}, \tag{5.3}$$

$$\mathrm{Tr}\, h_\alpha \neq \mathrm{Tr}\, h_{\alpha'} \quad \text{for } \alpha \neq \alpha', \tag{5.4}$$

$$\mathrm{Tr}\, h_\alpha \neq \pm 2 \,(\mathrm{mod}\, q_1) \quad \text{for each } \alpha. \tag{5.5}$$

By (5.4), the conjugacy classes

$$C_\alpha = \{g h_\alpha g^{-1} : g \in H\} \subset H^{(6)}$$

are disjoint. Hence we may specify some α such that

$$|C_\alpha| < \frac{1}{\beta} |H^{(6)}| < e^{-c\ell_1} q^{C\varepsilon} |H| < e^{-\frac{c}{2}\ell_1} |H|. \tag{5.6}$$

Set $h = h_\alpha$. Considering the map $g \mapsto ghg^{-1}$, it follows from (5.6) that there is $\bar{g} \in H$ such that

$$|\{g \in H : ghg^{-1} = \bar{g} h (\bar{g})^{-1}\}| > e^{\frac{c}{2}\ell_1}. \tag{5.7}$$

Hence the set

$$S = \{g \in H.H : gh = hg (\mathrm{mod}\, q)\} \tag{5.8}$$

satisfies

$$|S| > e^{c\ell_1}, \tag{5.9}$$

where

$$\operatorname{Tr} h \neq \pm 2 \,(\mathrm{mod}\, q_1). \tag{5.10}$$

Diagonalize h, considering, if necessary, a quadratic extension $K = \mathbb{Q}[\zeta]$ with ζ a quadratic unit. Denote by O the algebraic integers in K and, distinguishing the inert and split case, let $\mathcal{P}$ be a prime ideal dividing (p). Replace $\mathbb{Z}_q$ by the residue ring $O/\mathcal{P}^n$. A suitable base change brings h in diagonal form

$$h = \begin{pmatrix} \lambda_0 & 0 \\ 0 & \lambda_0^{-1} \end{pmatrix},$$

where λ_0 is a unit in O and $\lambda_0 \pm 1 \notin \mathcal{P}^{r_1}$ by (5.10), and also

$$\lambda_0 - \frac{1}{\lambda_0} \notin \mathcal{P}^{2r_1}. \tag{5.11}$$

Since $g \in S$ commutes with $h \,(\mathrm{mod}\, \mathcal{P}^n)$, it follows from (5.11) that in this basis

$$g = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \,(\mathrm{mod}\, \mathcal{P}^{n-2r_1}) \tag{5.12}$$

with $\lambda \in O$. We may clearly assume that

$$g \equiv 1 \,(\mathrm{mod}\, \mathcal{P}) \quad \text{for } g \in S. \tag{5.13}$$

Hence $\lambda \equiv 1 \,(\mathrm{mod}\, \mathcal{P})$ in (5.12) and the map $\lambda \mapsto \lambda^2 - 1/\lambda^2$ has bounded multiplicity. Defining

$$T = \{\lambda^2 - 1/\lambda^2 : g \in S\} \subset O, \tag{5.14}$$

it follows from the preceding that

$$|\pi_{\mathcal{P}^{n-2r_1}}(T)| > |S|/|\mathcal{P}|^{2r_1} > q^{-C\varepsilon}|S| \overset{(5.9)}{>} e^{\frac{c}{2}\ell_1}. \tag{5.15}$$

Next, let $\xi \in \mathrm{Mat}_2(O)$ and write

$$g\xi g^{-1} - g^{-1}\xi g = (\operatorname{Tr} g)[g, \xi] = (\lambda^2 - 1/\lambda^2) \begin{pmatrix} 0 & \xi_{12} \\ -\xi_{21} & 0 \end{pmatrix} \,(\mathrm{mod}\, \mathcal{P}^{n-2r_1});$$

hence

$$g\xi g^{-1} - g^{-1}\xi g = (\lambda^2 - 1/\lambda^2)[\xi, h'] \,(\mathrm{mod}\, \mathcal{P}^{n-2r_1}), \tag{5.16}$$

where

$$h' = \frac{2h - (\operatorname{Tr} h)1}{(\lambda_0 - 1/\lambda_0)} \in \mathrm{Mat}_2(O).$$

This statement is independent of the choice of the basis.

Take $\ell_1 = n$. The conclusion is that we obtain an element $h' \in \mathrm{Mat}_2(\mathbb{Z})$, $\pi_p(h')$ not a multiple of the identity, and a subset $A \subset \mathbb{Z}_q$ satisfying, by (5.15),

$$|A| > q^c, \tag{5.17}$$

and such that if $\xi \in \mathrm{Mat}_2(\mathbb{Z})$ and $x \in A$, we have

$$x[\xi, h'] \in \mathcal{H}_\xi^{(2)} - \mathcal{H}_\xi^{(2)} \left(\mathrm{mod}\ \frac{q}{q_1^2}\right), \tag{5.18}$$

where for $s \geq 1$,

$$\mathcal{H}_\xi^{(s)} = \{g\xi g^{-1} : g \in H^{(s)}\}, \tag{5.19}$$

and $q_1 < q^{C\varepsilon}$.

Note also that in (5.18) we may replace h' by any conjugate $kh'k^{-1}$ with $k \in H^{(s)}$, provided we replace $\mathcal{H}_\xi^{(2)}$ by $\mathcal{H}_\xi^{(2+s)}$.

In the preceding construction, we may replace q by $\bar{q} = q^\delta$, where $\delta \gg \varepsilon$. Note that, according to (3.4), $\bar{H} = \pi_{\bar{q}}(H)$ is an approximate group in $\mathrm{SL}_2(\mathbb{Z}_{\bar{q}})$ and, letting $\bar{x}_0 = \pi_{\bar{q}}(x_0)$, we have, using (3.5),

$$\pi_{\bar{q}}[\nu]^{(\ell)}(\bar{x}_0.\bar{H}) = \sum_{\pi_{\bar{q}}(g)\in\bar{x}_0\bar{H}} \nu^{(\ell)}(g) \geq \sum_{\pi_q(g)\in x_0 H} \nu^{(\ell)}(g) = \pi_q[\nu]^{(\ell)}(x_0 H) > q^{-C\varepsilon}. \tag{5.20}$$

We obtain an element $h' \in \mathrm{Mat}_2(\mathbb{Z})$ and a subset $A \subset \mathbb{Z}_{\bar{q}}$ such that

$$\pi_p(h') \text{ is not a multiple of the identity,} \tag{5.21}$$

$$|A| > (\bar{q})^c, \tag{5.22}$$

$$x[\xi, h'] \in \mathcal{H}_\xi^{(2)} - \mathcal{H}_\xi^{(2)} \left(\mathrm{mod}\ \frac{\bar{q}}{q_1}\right) \text{ for } x \in A,\ \xi \in \mathrm{Mat}_2(\mathbb{Z}) \text{ and } q_1 < q^{C\varepsilon}. \tag{5.23}$$

Applying the initial construction in the proof of Proposition 2.2 to the set A, we clearly obtain $Q \mid q$ and a subset $B \subset \mathbb{Z}_Q$ satisfying the conditions

$$Q > (\bar{q})^c, \tag{5.24}$$

$$|\pi_{q'}(B)| > (q')^c \quad \text{for } q' \mid Q. \tag{5.25}$$

For $x \in B$ and $\xi \in \mathrm{Mat}_2(\mathbb{Z})$,

$$x\frac{\bar{q}}{Q}[h', \xi] \in 2\mathcal{H}_\xi^{(2)} - 2\mathcal{H}_\xi^{(2)}\ (\mathrm{mod}\, \bar{q}). \tag{5.26}$$

In order to apply the sum-product theorem in $\mathbb{Z}_{p^m}$, we need to iterate (5.26), which we rewrite as

$$\frac{\bar{q}}{Q}(x[h', \xi] + Qw_x) \in 2\mathcal{H}_\xi^{(2)} - 2\mathcal{H}_\xi^{(2)} \tag{5.27}$$

for some $w_x \in \mathrm{Mat}_2(\mathbb{Z})$ (depending on x and ξ).

Denote by $h_1, h_2, \ldots$ the conjugates of h' of the form $kh'k^{-1}$ with $k \in H.H$.

Rewriting (5.27) as

$$\frac{\bar{q}}{Q}(x_1[h_1,\xi]+Qw_1)\in 2\mathcal{H}_\xi^{(2)}-2\mathcal{H}_\xi^{(2)} \tag{5.28}$$

for $x_1\in B$, set

$$\xi_1=x_1[h_1,\xi]+Qw_1; \tag{5.29}$$

then, by (5.28),

$$\frac{\bar{q}}{Q}\xi_1\in 2\mathcal{H}_\xi^{(2)}-2\mathcal{H}_\xi^{(2)}. \tag{5.30}$$

Applying (5.27) with h_1 (resp. ξ) replaced by h_2 (resp. ξ_1), it follows that

$$\frac{\bar{q}}{Q}(x_2[h_2,\xi_1]+Qw_2)\in 2\mathcal{H}_{\xi_1}^{(2)}-2\mathcal{H}_{\xi_1}^{(2)}\quad \text{for } x_2\in B;$$

hence, by (5.30), we have

$$\frac{\bar{q}}{Q}(x_1x_2[h_2,[h_1,\xi]]+Qw)\in 2\mathcal{H}_{\xi_1}^{(2)}-2\mathcal{H}_{\xi_1}^{(2)} \tag{5.31}$$

for some $w\in \mathrm{Mat}_2(\mathbb{Z})$.

Therefore, recalling (5.30), we obtain

$$\left(\frac{\bar{q}}{Q}\right)^2 x_1x_2[h_2,[h_1,\xi]]\in 8\mathcal{H}_\xi^{(4)}-8\mathcal{H}_\xi^{(4)}\left(\mathrm{mod}\,\frac{(\bar{q})^2}{Q}\right) \tag{5.32}$$

for all $x_1,x_2\in B$. The iteration of the process is clear.

Recalling (5.25), in order to be able to apply Proposition 2.1 to the set $\pi_Q(B)\subset\mathbb{Z}_Q$, we need to introduce $r<C$ factors $x_1,\dots,x_r$.

Fix an exponent $\delta_0\gg\varepsilon$ and take $\bar{q}\sim q^{\delta_0/r}$ in the preceding.

Iteration of (5.32) yields

$$\left(\frac{\bar{q}}{Q}\right)^r x_1x_2\dots x_r[h_r,\dots,[h_1,\xi]]\in\mathcal{H}'_\xi\left(\mathrm{mod}\,\frac{(\bar{q})^r}{Q^{r-1}}\right) \tag{5.33}$$

for $x_1,\dots,x_r\in B$, denoting by $\mathcal{H}'_\xi$ a set of the form $m\mathcal{H}_\xi^{(n)}-m\mathcal{H}_\xi^{(n)}$ for some $m,n\in\mathbb{Z}_+$ depending on r.

Apply Proposition 2.1. It follows that for all $x\in Q'\mathbb{Z}_Q$, where $Q'\mid Q$ and $Q'<Q^{1/2}$, we have

$$\left(\frac{\bar{q}}{Q}\right)^r x[h_r,\dots,[h_1,\xi]]\in\mathcal{H}'_\xi\left(\mathrm{mod}\,\frac{(\bar{q})^r}{Q^{r-1}}\right). \tag{5.34}$$

Hence there are $q_1\mid q$ and $q_2\mid q_1$ such that

$$q_1<q^{\delta_0}\quad\text{and}\quad q_1/q_2>q^{c\delta_0}, \tag{5.35}$$

$$q_2x[h_r,\dots,[h_1,\xi]]\in\mathcal{H}'_\xi\,(\mathrm{mod}\,q_1)\quad\text{for all } x\in\mathbb{Z}_{q_1/q_2}. \tag{5.36}$$

It remains to specify the conjugates $h_1, \dots, h_r$ of h'.
Fix $\xi \in \mathrm{Mat}_2(\mathbb{Z})$ such that

$$\pi_p(\xi) \neq 0 \quad \text{and} \quad \pi_p(\mathrm{Tr}\,\xi) = 0. \tag{5.37}$$

Recalling Proposition 4.3, there are $k_1, k_2 \in H.H$ such that

$$\det(1, \xi, k_1\xi k_1^{-1}, k_2\xi k_2^{-1}) \neq 0 \,(\mathrm{mod}\, q_0), \qquad \text{where } q_0 \mid q,\ q_0 < q^{C\varepsilon}. \tag{5.38}$$

Setting $k_0 = 1$, it follows from (5.38) that for some $i \in \{0, 1, 2\}$, we have

$$[h', k_i\xi k_i^{-1}] \neq 0 \,(\mathrm{mod}\, q_0) \tag{5.39}$$

(recall that also $q_1 < q^{C\varepsilon}$) and hence, defining

$$h_1 = k_i^{-1} h' k_i,$$

we also have

$$[h_1, \xi] \neq 0 \,(\mathrm{mod}\, q_0). \tag{5.40}$$

Repeating the argument replacing ξ by $[h_1, \xi]$ (divided by a divisor of q_0), we obtain a conjugate h_2 of h' satisfying

$$[h_2, [h_1, \xi]] \neq 0 \,(\mathrm{mod}\, q_0^2). \tag{5.41}$$

Hence, in (5.36), we may ensure that

$$[h_r, [h_{r-1}, \dots, [h_1, \xi]]] \neq 0 \,(\mathrm{mod}\, q_0^r). \tag{5.42}$$

Increasing in (5.36) q_2 by a factor dividing q_0^r (hence bounded by $q^{C\varepsilon}$), we obtain $\eta \in \mathrm{Mat}_2(\mathbb{Z})$ satisfying

$$\mathrm{Tr}\,\eta = 0, \tag{5.43}$$

$$\pi_p(\eta) \neq 0, \tag{5.44}$$

$$q_2 x \eta \in \mathcal{H}'_\xi \,(\mathrm{mod}\, q_1) \quad \text{for all } x \in \mathbb{Z}_{q_1/q_2}. \tag{5.45}$$

Finally, applying Proposition 4.3 to η once again, we obtain $k_1, k_2 \in H.H$ such that

$$\det(1, \eta, k_1\eta k_1^{-1}, k_2\eta k_2^{-1}) \neq 0 \,(\mathrm{mod}\, q_0). \tag{5.46}$$

In particular, if $z \in \mathrm{Mat}_2(\mathbb{Z})$ and $\mathrm{Tr}\, z = 0$, then for some $x_0, x_1, x_2 \in \mathbb{Z}_q$,

$$q_0 z = x_0\eta + x_1(k_1\eta k_1^{-1}) + x_2(k_2\eta k_2^{-1}) \,(\mathrm{mod}\, q). \tag{5.47}$$

Since by (5.45) also

$$q_2(x_0\eta + x_1(k_1\eta k_1^{-1}) + x_2(k_2\eta k_2^{-1})) \in \mathcal{H}'_\xi \,(\mathrm{mod}\, q_1) \tag{5.48}$$

we have completed the proof of the following lemma.

Lemma 5.1. *Assume $\varepsilon \ll \delta_0 < 1$. Let $\xi \in \mathrm{Mat}_2(\mathbb{Z})$ be such that $\pi_p(\xi) \neq 0$ and $\pi_p(\mathrm{Tr}\,\xi) = 0$. There are $q_1 \mid q$ and $q_2 \mid q_1$ such that*

$$q_1 < q^{\delta_0} \quad \textit{and} \quad q_1/q_2 > q^{c\delta_0}, \tag{5.49}$$

$$q_2 z \in \mathcal{H}'_\xi \,(\mathrm{mod}\, q_1) \quad \textit{for all } z \in \mathrm{Mat}_2(\mathbb{Z}) \textit{ with } \mathrm{Tr}\, z = 0. \tag{5.50}$$

6. Proof of the upper bound

Take

$$\varepsilon \ll \delta_0 \ll 1 \tag{6.1}$$

(to be specified) and $q_0 \mid q$, $q_0 \sim q^{\delta_0}$. Define

$$H_0 = \{x \in H^{(4)} : x = 1 \,(\mathrm{mod}\, q_0)\}. \tag{6.2}$$

By (3.9), we have

$$\nu^{(2\ell_0)}(H_0) > \frac{1}{(q_0)^3}[\nu^{(\ell_0)}(H)]^2 > q^{-C\varepsilon - 3\delta_0} > q^{-4\delta_0}. \tag{6.3}$$

Hence, taking $\ell_0 \sim \delta_0 \log q$ sufficiently large, we obtain an element $g_0 \in H^{(4)}$ satisfying

$$g_0 \equiv 1 \,(\mathrm{mod}\, q_0), \qquad g_0 \neq 1, \tag{6.4}$$

$$\|g_0\| < C^{\ell_0} < q^{C_1\delta_0}. \tag{6.5}$$

Hence, we may write

$$g_0 = 1 + \tilde{q}\xi_0, \tag{6.6}$$

where

$$\tilde{q} \mid q \quad \text{and} \quad q^{\delta_0} < \tilde{q} < q^{C\delta_0}, \tag{6.7}$$

$$\pi_p(\xi_0) \neq 0, \tag{6.8}$$

$$\mathrm{Tr}\,\xi_0 = 0 \,(\mathrm{mod}\, \tilde{q}). \tag{6.9}$$

Now apply Lemma 5.1 with δ_0 and taking $\xi = \xi_0$. Clearly, if $k \in H^{(s)}$, by (6.6) we have

$$H^{(2s+4)} \ni kg_0k^{-1} = 1 + \tilde{q}k\xi_0k^{-1},$$

and also

$$g_0^{-1} = 1 - \tilde{q}\xi_0 \,(\mathrm{mod}\, (\tilde{q})^2).$$

Hence we obtain

$$(kg_0k^{-1})(k^{-1}g_0^{-1}k) = 1 + \tilde{q}(k\xi_0k^{-1} - k^{-1}\xi_0k) \,(\mathrm{mod}\, (\tilde{q})^2). \tag{6.10}$$

Denote by H' a product set $H^{(s)}$ with s unspecified but suitably bounded.

Recalling (3.6), (3.7), we have

$$|H'| < q^{C\varepsilon}|H| < q^{C\varepsilon-\gamma}|\mathrm{SL}_2(q)|. \tag{6.11}$$

It follows from (6.10) that if $z \in \mathcal{H}_{\xi_0}^{(s)} - \mathcal{H}_{\xi_0}^{(s)}$, then

$$1 + \tilde{q}z \in H' \,(\mathrm{mod}\, (\tilde{q})^2).$$

Similarly, for $z \in \mathcal{H}'_{\xi_0}$, we have

$$1 + \tilde{q}z \in H' \,(\mathrm{mod}\,(\tilde{q})^2). \tag{6.12}$$

Let $q_1, q_2 < q^{\delta_0}$ be as in Lemma 5.1. Thus $q_1/q_2 > q^{c\delta_0}$ by (5.49). It follows from (5.50), (6.12), and (6.7) that if $z \in \mathrm{Mat}_2(\mathbb{Z})$ and $\mathrm{Tr}\, z = 0$, then

$$1 + \tilde{q}q_2 z \in H' \,(\mathrm{mod}\,\tilde{q}q_1). \tag{6.13}$$

It follows in particular from (6.13) that if $pq' \mid \tilde{q}q_1$ and $\tilde{q}q_2 \mid q'$, then there is $\xi' \in \mathrm{Mat}_2(\mathbb{Z}_q)$ such that

$$\pi_p(\xi') \neq 0, \tag{6.14}$$

$$\pi_p(\mathrm{Tr}\,\xi') = 0, \tag{6.15}$$

$$1 + q'\xi' \in H'. \tag{6.16}$$

Replacing $\tilde{q}$ (resp. ξ_0) by q' (resp. ξ'), it follows from the preceding that if $z \in \mathrm{Mat}_2(\mathbb{Z})$ and $\mathrm{Tr}\, z = 0$, then

$$1 + q'q_2 z \in H' \,(\mathrm{mod}\, q'q_1). \tag{6.17}$$

Hence, if $q' \mid \tilde{q}(q_1/p)^2$ and $\tilde{q}(q_2)^2 \mid q'$, there is $\xi' \in \mathrm{Mat}_2(\mathbb{Z}_q)$ satisfying (6.14)–(6.16).

Iteration shows that if $q' \mid \tilde{q}(q_1/p)^r$ and $\tilde{q}(q_2)^r \mid \tilde{q}$ (r bounded), the same conclusion holds.

Since $q_2 < q_1^{1-c}$, an appropriate choice of $r < C$ implies that there is ξ' satisfying (6.14)–(6.16) for all $q' \mid q$ such that $\tilde{q}(q_1/p)^r \mid q'$ and $q' \mid \tilde{q}(q_1/p)^{r+1}$ and hence for all $q' \mid q$ such that $\tilde{q}q_1^r \mid q'$. Define

$$q_3 = \tilde{q}q_1^r q_2 < q^{C\delta_0} \quad \text{and} \quad q_4 = q_1/q_2. \tag{6.18}$$

Again by (6.13), we see that if $q' \mid q/q_4$ and $q_3 \mid q'$ and $z \in \mathrm{Mat}_2(\mathbb{Z})$, $\mathrm{Tr}\, z = 0$, then

$$1 + q'z \in H' \,(\mathrm{mod}\, q'q_4). \tag{6.19}$$

Next, we claim that if $q' \mid q$, $q_3 \mid q'$ and $z \in \mathrm{Mat}_2(\mathbb{Z})$ satisfies

$$\det(1 + q_3 z) = 1 \,(\mathrm{mod}\, q') \tag{6.20}$$

then

$$1 + q_3 z \in H' \,(\mathrm{mod}\, q'). \tag{6.21}$$

Notice that (6.20) implies in particular that $\mathrm{Tr}\, z \equiv 0 \,(\mathrm{mod}\, \min(q'/q_3, q_3))$. Hence (6.19) gives the claim for $q' = q_3q_4$.

Proceeding by induction, assume the claim holds for $q' \leq q/q_4$. Let $z \in \mathrm{Mat}_2(\mathbb{Z})$ satisfy

$$\det(1 + q_3 z) = 1 \,(\mathrm{mod}\, q'q_4). \tag{6.22}$$

There is $g \in H'$ such that

$$g = 1 + q_3 z \,(\mathrm{mod}\, q'),$$

and hence

$$(1 + q_3 z)g^{-1} = 1 + q'w, \tag{6.23}$$

where by (6.22) we have

$$\det(1 + q'w) \equiv 1 \,(\mathrm{mod}\, q'q_4) \quad \text{and} \quad \mathrm{Tr}\, w = 0 \,(\mathrm{mod}\, q_4).$$

Again by (6.19)

$$1 + q'w \in H' \,(\mathrm{mod}\, q'q_4)$$

and hence

$$1 + q_3 z \in H' \,(\mathrm{mod}\, q'q_4). \tag{6.24}$$

This proves the claim.

It follows that

$$H' \supset \{z \in \mathrm{SL}_2(q) : z = 1 \,(\mathrm{mod}\, q_3)\}.$$

Recalling (6.11), (6.18) we have

$$q^{C\varepsilon - \gamma} |\mathrm{SL}_2(q)| > \frac{1}{(q_3)^3} |\mathrm{SL}_2(q)|$$

and

$$q^{3C\delta_0 + C\varepsilon} > q^{\gamma}, \tag{6.25}$$

which is a contradiction for an appropriate choice of δ_0.

We have therefore proven the following.

Proposition 6.1. *Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a symmetric set, $|\Gamma| = 2k$, generating a free group and consider the probability measure on $\mathrm{SL}_2(\mathbb{Z})$*

$$\nu = \frac{1}{2k} \sum_{g \in \Gamma} \delta_g.$$

Fix a prime $p \neq 2$. For all $\gamma > 0$, there is $C(\gamma)$ such that if $q \in \mathbb{Z}_+$ is of the form $q = p^n$ and $\ell > C(\gamma) \log q$, then

$$\|\pi_q[\nu^{(\ell)}]\|_\infty < q^{\gamma} |\mathrm{SL}_2(q)|^{-1}. \tag{6.26}$$

It follows indeed that taking $\ell > C(\gamma) \log q$, we may ensure that

$$\|\pi_q[\nu^{(\ell)}]\|_2 < q^{\gamma} |\mathrm{SL}_2(q)|^{-1/2}. \tag{6.27}$$

Otherwise Lemma 3.1 would clearly apply, taking $\mu = \pi_q[\nu^{(\ell')}]$ for some $\ell' \sim \log q$, and produce an approximate group $H \subset \mathrm{SL}_2(q)$ satisfying (3.4)–(3.6) with $\varepsilon = \varepsilon(\gamma) > 0$ small enough. But we showed in Sections 4–6 that this leads to a contradiction.

7. Multiplicity bound

Let p be a fixed odd prime. We have

$$|\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})| = p^{3n-2}(p-1)(p+1). \tag{7.1}$$

For $n \geq r$ let $\pi_{n,r}$ denote the surjective homomorphism

$$\pi_{n,r} : \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}),$$

and let $G_{n,r}$ denote the kernel of this homomorphism. The group $G_{n,r}$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ of order $p^{3(n-r)}$.

Lemma 7.1. *Let p be an odd prime and let $n \geq 2$. The dimension of a faithful irreducible representation of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ is at least*

$$\frac{1}{2}p^{n-2}(p-1)(p+1).$$

Proof. Let ρ be a faithful irreducible representation of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ and denote by χ the corresponding character. Assume $n = 2k$ (the proof is similar for n odd) and consider the restriction $\rho_{G_{n,k}}$.

A typical element in $G_{n,k}$ has the form $I + p^k\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ with $a, b, c \in \mathbb{Z}/p^k\mathbb{Z}$, and we have

$$\left(I + p^k\begin{pmatrix} a_1 & b_1 \\ c_1 & -a_1 \end{pmatrix}\right)\left(I + p^k\begin{pmatrix} a_2 & b_2 \\ c_2 & -a_2 \end{pmatrix}\right) = I + p^k\begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & -a_1 - a_2 \end{pmatrix},$$

so $G_{n,k}$ is a direct product of cyclic groups generated by

$$I + p^k\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad I + p^k\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad I + p^k\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

In particular, $G_{n,k}$ is an abelian group. More generally, it is easy to see that for $r \geq n/2$ the group $G_{n,r}$ is abelian.

Now consider the decomposition of $\rho_{G_{n,k}}$ into irreducible representations θ_i of the abelian group $G_{n,k}$. Since the representation ρ is faithful, there is at least one θ which does not contain in its kernel $G_{n,n-1}$, the abelian normal subgroup of order p^3. Since $G_{n,k}$ is normal, by Clifford's theorem [10] we have

$$\rho_{G_{n,k}} = \langle \chi_{G_{n,k}}, \theta \rangle \sum_{i=1}^{t} \theta_i, \tag{7.2}$$

where θ_i are distinct conjugates of θ in $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Thus the dimension of ρ is bounded from below by t, the size of the orbit of θ under conjugation by $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

Since $G_{n,k}$ is an abelian group, $\widehat{G}_{n,k}$ is isomorphic to $G_{n,k}$. Under this isomorphism the character $\theta \in \widehat{G}_{n,k}$ which does not vanish on $G_{n,n-1}$ corresponds to an element g in $G_{n,k} \setminus G_{n,k+1}$, the set-theoretic difference of $G_{n,k}$ and $G_{n,k+1}$, and the size t of the orbit is equal to the size of the orbit of g under conjugation by $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$.

Claim 7.1. *Let $g \in G_{n,k} \setminus G_{n,k+1}$. Then the centralizer of g in $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ has size at most $2p^{2n}$.*

Now since t, the size of the orbit of g under conjugation, is equal to the size of the group divided by the size of the centralizer, Claim 7.1 implies

$$t \geq \frac{|\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})|}{2p^{2n}} = \frac{1}{2}p^{n-2}(p-1)(p+1),$$

completing the proof of Lemma 7.1. □

Proof of Claim 7.1. An element g in $G_{n,k} \setminus G_{n,k+1}$ has the form $I + p^k\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ with a, b, c in $\mathbb{Z}/p^k\mathbb{Z}$ and at least one of a, b, c not divisible by p. Our aim is to bound the number of solutions to $hg = gh$ where $h = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ is a matrix in $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 1+p^k a & p^k b \\ p^k c & 1-p^k a \end{pmatrix} \equiv \begin{pmatrix} 1+p^k a & p^k b \\ p^k c & 1-p^k a \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \pmod{p^{2k}}.$$

This amounts to solving the following system of congruences for $\alpha, \beta, \gamma, \delta$:

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{p^{2k}}, \tag{7.3}$$

$$\beta c \equiv \gamma b \pmod{p^k}, \tag{7.4}$$

$$b(\alpha - \delta) \equiv 2a\beta \pmod{p^k}, \tag{7.5}$$

$$c(\alpha - \delta) \equiv 2\gamma a \pmod{p^k}, \tag{7.6}$$

$$\gamma b \equiv \beta c \pmod{p^k}. \tag{7.7}$$

If we replace (7.3) by

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{p^k}, \tag{7.8}$$

then it is clear that any solution of (7.4)–(7.8) will determine a matrix in $\mathrm{SL}_2(\mathbb{Z}/p^k\mathbb{Z})$, any of whose inverse images under $\pi_{n,k}$ will be in the centralizer of g in $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Consequently, the size of the centralizer of g is equal to the number of solutions to the system (7.4)–(7.8), multiplied by the size of $G_{n,k}$, which is equal to p^{3k}.

It remains to show that the system (7.4)–(7.8) has at most $2p^k$ solutions. If $b \not\equiv 0 \pmod{p}$, then the system (7.4)–(7.8) is easily seen to reduce to the following quadratic equation for β, δ:

$$b\delta^2 + 2a\beta\delta - \beta^2 c \equiv b \pmod{p^k}, \tag{7.9}$$

and with γ and α determined by

$$\gamma \equiv \beta c/b \pmod{p^k}, \qquad \alpha \equiv \delta + 2a\beta/b \pmod{p^k}$$

(with a similar set of equations in the case $c \not\equiv 0 \pmod{p}$).

If $a \not\equiv 0 \pmod{p}$ then the system (7.4)–(7.8) is easily seen to reduce to the following quadratic equation for α, δ:

$$-bc\alpha^2 + 4(a^2 + bc)\alpha\delta - bc\delta^2 \equiv 4a^2 \pmod{p^k}, \tag{7.10}$$

with β and γ determined by

$$\beta \equiv \frac{b(\alpha-\delta)}{2a} \pmod{p^k}, \qquad \gamma \equiv \frac{c(\alpha-\delta)}{2a} \pmod{p^k}.$$

Both equations (7.9) and (7.10) are of the form

$$Ax^2 + Bxy + Cy^2 \equiv D \pmod{p^k}, \tag{7.11}$$

with $D \not\equiv 0 \pmod{p}$. Denoting the number of solutions of (7.11) by $s(k)$ we clearly have $s(k) = p^{k-1}s(1)$. Now since $s(1) \leq 2p$ (see, for example, [9]), the proof of Claim 7.1 is complete. □

8. Proof of Theorem 1.1

For a Cayley graph $\mathcal{G}(G, S)$ with $S = \{g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}\}$ the adjacency matrix can be written as

$$A(\mathcal{G}(G,S)) = \Pi_R(g_1) + \Pi_R(g_1^{-1}) + \cdots + \Pi_R(g_k) + \Pi_R(g_k^{-1}), \tag{8.1}$$

where Π_R is a regular representation of G given by the permutation action of G on itself. Every irreducible representation $\rho \in \hat{G}$ appears in Π_R with the multiplicity equal to its dimension:

$$\Pi_R = \rho_0 \oplus \bigoplus_{\substack{\rho\in\hat{G}\\ \rho\neq\rho_0}} \underbrace{\rho \oplus \cdots \oplus \rho}_{d_\rho}, \tag{8.2}$$

where ρ_0 denotes the trivial representation and $d_\rho = \dim(\rho)$ is the dimension of the irreducible representation ρ.

Let $N = |G|$. The adjacency matrix $A(\mathcal{G}(G, S))$ is a symmetric matrix having N real eigenvalues which we can list in decreasing order:

$$2k = \lambda_0 > \lambda_1 \geq \cdots \geq \lambda_{N-1} \geq -2k;$$

the eigenvalue $2k$ corresponds to the trivial representation in the decomposition (8.2). The strict inequality

$$2k = \lambda_0 > \lambda_1$$

follows from connectivity of our graphs (since we have chosen p sufficiently large).

Denoting by W_{2m} the number of closed walks from identity to itself of length $2m$, the trace formula takes the form

$$\sum_{j=0}^{N-1} \lambda_j^{2m} = N W_{2m}. \tag{8.3}$$

We now fix $S = \{g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}\}$ such that $\langle S\rangle$ is a free subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and consider, for fixed p, the Cayley graphs $\mathcal{G}(n) = \mathcal{G}(\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}), S_n)$, where S_n is the projection of S modulo p^n.

Let $N(n) = |\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})| \sim p^{3n}$. Let $\Omega(n)$ denote the nontrivial spectrum of the adjacency matrix $A(\mathcal{G}(n))$ of $\mathcal{G}(n)$ (that is, all the eigenvalues of $A(\mathcal{G}(n))$ except for $\pm 2k$) and let $\lambda(n)$ be the eigenvalue of maximum modulus in $\Omega(n)$.

Nontrivial irreducible representations of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ can be split into faithful and nonfaithful ones. Since the set $\{G_{n,r}\}$ gives all normal subgroups of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$, nonfaithful irreducible representations of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ arise as faithful irreducible representations of $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ for some $r < n$. Corresponding to this split we have the decomposition

$$\Omega(n) = \Omega_{\mathrm{old}}(n) \cup \Omega_{\mathrm{new}}(n), \quad \text{where} \quad \Omega_{\mathrm{old}}(n) = \bigcup_{r<n} \Omega_{\mathrm{new}}(r).$$

Thus the "old" eigenvalues of $\mathcal{G}(n)$, corresponding to nonfaithful irreducible representations of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$, appear as "new" eigenvalues of $\mathcal{G}(r)$ for some $r < n$. Consequently, to establish the desired expansion property it suffices to establish a uniform bound on the "new" eigenvalues.

Proposition 6.1 implies that for

$$l > C(\varepsilon) \log_{2k} p^n$$

we have

$$W_{2l} < \frac{(2k)^{2l} p^{n\varepsilon}}{|\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})|}. \tag{8.4}$$

Now combining (8.4) with the bound on the dimension of nontrivial faithful irreducible representations of $\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ given in Lemma 7.1 we obtain, using (8.3),

$$\frac{1}{2} p^{n-2}(p-1)(p+1)\lambda_{\mathrm{new}}(n)^{2l} < |\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})| \frac{(2k)^{2l} p^{n\varepsilon}}{|\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})|}; \tag{8.5}$$

consequently,

$$|\lambda_{\mathrm{new}}(n)| < (2k)^{1-(1-\varepsilon)/2C(\varepsilon)} = \beta(S) < 2k,$$

completing the proof of Theorem 1.1. □

9. Further comments

Our aim is to sketch an alternative approach to the results from Section 4, mainly in view of an extension to the higher rank case (details will appear in [5]).

The main issue is the (handy) use in Section 4 of the expander property of $\pi_P[\nu]$ for P prime. The result is obtained in [3] and uses Helfgott's work [14] on the "product theorem" in $\mathrm{SL}_2(P)$, P prime. At present, those results are not available for $\mathrm{SL}_d(P)$, $d > 2$. One may follow however a different route which makes use of the theory of random matrix products over $\mathbb{R}$ (see [1] for instance). The considerations easily generalize to higher ranks, provided we assume that $\Gamma = \operatorname{supp} \nu$, $\nu = (1/|\Gamma|) \sum_{g\in\Gamma} \delta_g$ as in §3, generates a group $\langle\Gamma\rangle$ which is Zariski dense in $\mathrm{SL}_d(\mathbb{R})$ (for $d = 2$, this is automatically satisfied if $\langle\Gamma\rangle$ is nonelementary).

Consider the following representation of $\mathrm{SL}_2(\mathbb{R})$. Denote by V the subspace of $\mathrm{Mat}_2(\mathbb{R})$ consisting of the traceless matrices and let $\rho : \mathrm{SL}_2(\mathbb{R}) \to \mathrm{GL}(V)$ be defined by

$$\rho(g)\xi = g\xi g^{-1} \quad \text{for } \xi \in V,\ g \in \mathrm{SL}_2(\mathbb{R}). \tag{9.1}$$

We follow the terminology from [1].

When restricted to $\langle\Gamma\rangle$, the representation ρ is strongly irreducible (no finite union of hyperplanes of V is invariant under a finite index subgroup of $\langle\Gamma\rangle$). This follows indeed from the strong irreducibility of ρ and the fact that the Zariski closure $\overline{\langle\Gamma\rangle}$ equals $\mathrm{SL}_2(\mathbb{R})$.

Next, using the simplicity of the Lyapunov exponents, clearly $\rho[\nu]$ is contractive (see [1, Ch. III]).

At this point a set of results becomes available on the behavior of the random walk in the projective space $P(V)$ (in what follows, our notations differ from [1]). First, there is a unique $\rho[\nu]$-invariant distribution η on $P(V)$, satisfying in particular

$$\sup_{\|y\|=1} \int \left(\frac{\|x\|}{|\langle x, y\rangle|} \right)^{\alpha} d\eta(\bar{x}) < \infty \tag{9.2}$$

and hence

$$\sup_{\bar{y}\in P(V)} \int \delta(\bar{x}, \bar{y})^{-\alpha}\, d\eta(\bar{x}) < \infty \tag{9.3}$$

for some $\alpha > 0$ (depending on ν). (See [1, Theorem 2.1, p. 155 and Proposition 4.1, p. 161].) Here $\delta(\bar{x}, \bar{y})$ denotes the usual distance on $P(V)$.

Given $\beta > 0$, denote by $\mathcal{L}(\beta)$ the space of β-Hölder continuous functions on $P(V)$ with norm

$$\|f\|_\beta = \sup_{\bar{x}\in P(V)} |f(\bar{x})| + \sup_{\substack{\bar{x},\bar{y}\in P(V)\\ \bar{x}\neq\bar{y}}} \frac{|f(\bar{x}) - f(\bar{y})|}{\delta(\bar{x}, \bar{y})^{\beta}}. \tag{9.4}$$

According to [1, Theorem 2.5, p. 106], $\rho[\nu]^{(n)}$ converges exponentially fast to η, in the following weak* sense: For $0 < \alpha < \alpha_0$ and $f \in \mathcal{L}_\alpha$, we have

$$\left\| \sum_g f(\rho(g)\bar{x})\nu^{(\ell)}(g) - \int f(\bar{y})\eta(d\bar{y}) \right\|_\alpha < Ce^{-c\ell}\|f\|_\alpha, \tag{9.5}$$

where the constants $c, C > 0$ depend on α and $\rho[\nu]$ only.

Combining (9.2), (9.5) one easily deduces that

$$\max_{\|x\|=\|y\|=1} \nu^{(\ell)}\{g : \langle\rho(g)x, y\rangle = 0\} < Ce^{-c\ell}. \tag{9.6}$$

Hence

$$\max_{\xi,\xi'\in V\setminus\{0\}} \nu^{(\ell)}\{g : \mathrm{Tr}\,\xi' g\xi g^{-1} = 0\} < Ce^{-c\ell}. \tag{9.7}$$

This result suffices for our needs. In particular, one may recover Corollary 4.3 and Proposition 4.1 from (9.7).

Acknowledgments. It is a pleasure to thank Bob Guralnick for inspiring discussions and penetrating remarks.

The first author was supported in part by the NSF grant DMS-0808042. The second author was supported in part by DARPA, NSF and Sloan Foundation.

References

[1] Bougerol, P., Lacroix, J.: Products of Random Matrices with Applications to Schrödinger Operators. Progr. Probab. Statist. 8, Birkhäuser (1985) Zbl 0572.60001 MR 0886674

[2] Bourgain, J.: The sum-product theorem in $\mathbb{Z}_q$ with q arbitrary. Preprint (2007)

[3] Bourgain, J., Gamburd, A.: Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. Ann. of Math. **167**, 625–642 (2008) MR 2415383

[4] Bourgain, J., Gamburd, A.: On the spectral gap for finitely-generated subgroups of SU(2). Invent. Math. **171**, 83–121 (2008) Zbl 1135.22010 MR 2358056

[5] Bourgain, J., Gamburd, A.: Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$: II. Preprint

[6] Bourgain, J., Gamburd, A., Sarnak, P.: Affine linear sieve, expanders, and sum-product. Preprint

[7] Bourgain, J., Glibichuk, A., Konyagin, S.: Estimate for the number of sums and products and for exponential sums in fields of prime order. J. London Math. Soc. **73**, 380–398 (2006) Zbl 1093.11057 MR 2225493

[8] Bourgain, J., Katz, N., Tao, T.: A sum-product estimate in finite fields and applications. Geom. Funct. Anal. **14**, 27–57 (2004) Zbl pre02121750 MR 2053599

[9] Cassels, J. W. S.: Rational Quadratic Forms. Academic Press (1978) Zbl 0395.10029 MR 0522835

[10] Clifford, A. H.: Representations induced in an invariant subgroup. Ann. of Math. **38**, 533–550 (1937) Zbl 0017.29705 MR 1503352

[11] Dawson, C. M., Nielsen, M. A.: The Solovay–Kitaev algorithm. Quantum Information Comput. **6**, 81–95 (2006) MR 2212257

[12] Gamburd, A.: Spectral gap for infinite index "congruence" subgroups of $\mathrm{SL}_2(\mathbb{Z})$. Israel J. Math. **127**, 157–200 (2002) Zbl 1028.11031 MR 1900698

[13] Gamburd, A., Shahshahani, M.: Uniform diameter bounds for some families of Cayley graphs. Int. Math. Res. Notices **2004**, no. 71, 3813–3824 Zbl 1066.05072 MR 2104475

[14] Helfgott, H.: Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Ann. of Math. **167**, 601–623 (2008) MR 2415382

[15] Hoory, S., Linial, N., Wigderson, A.: Expander graphs and their applications. Bull. Amer. Math. Soc. **43**, 439–561 (2006) MR 2247919

[16] Kesten, H.: Symmetric random walks on groups. Trans. Amer. Math. Soc. **92**, 336–354 (1959) Zbl 0092.33503 MR 0109367

[17] Lubotzky, A.: Discrete Groups, Expanding Graphs and Invariant Measures. Progr. Math. 125, Birkhäuser (1994) Zbl 0826.22012 MR 1308046

[18] Lubotzky, A.: Cayley graphs: eigenvalues, expanders and random walks. In: Surveys in Combinatorics, P. Rowlinson (ed.), London Math. Soc. Lecture Note Ser. 218, Cambridge Univ. Press, 155–189 (1995) Zbl 0835.05033 MR 1358635

[19] Lubotzky, A., Weiss, B.: Groups and expanders. In: Expanding Graphs (Princeton, NJ, 1992), DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 10, J. Friedman (ed.), Amer. Math. Soc., 95–109 (1993) Zbl 0787.05049 MR 1235570

[20] Sarnak, P.: What is an expander? Notices Amer. Math. Soc. **51**, 762–763 (2004) Zbl pre02115090 MR 2072849

[21] Sarnak, P., Xue, X.: Bounds for multiplicities of automorphic representations. Duke Math. J. **64**, 207–227 (1991) Zbl 0741.22010 MR 1131400

[22] Selberg, A.: On the estimation of Fourier coefficients of modular forms. In: Proc. Sympos. Pure Math. 8, Amer. Math. Soc., 1–15 (1965) Zbl 0142.33903 MR 0182610

[23] Shalom, Y.: Expanding graphs and invariant means. Combinatorica **17**, 555–575 (1997) Zbl 0906.05027 MR 1645694

[24] Shalom, Y.: The algebraization of Kazhdan's property (T). In: Int. Congress of Math. Vol. II, Eur. Math. Soc., 1283–1310 (2006) Zbl 1109.22003 MR 2275645

[25] Tao, T.: Product sets estimates for non-commutative groups. Preprint (2005)

[26] Tao, T., Vu, V.: Additive Combinatorics. Cambridge Univ. Press (2006) Zbl 1127.11002 MR 2289012