ON RAPID GENERATION OF $SL_2(\mathbb{Z}_q)$

JEREMY CHAPMAN AND ADRIANO MARZULLO

ABSTRACT. We prove that if $A \subset \mathbb{Z}_q \backslash \{0\}$, $A \neq \langle p \rangle$, $q = p^\ell$, $\ell \geq 2$ with $|A| > C\sqrt[3]{\ell^2} q^{\left(1-\frac{1}{4\ell}\right)}$, then $|P(A) \cdot P(A)| \geq C' q^3$ where

$$P(A) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in SL_2(\mathbb{Z}_q) : a_{11} \in A \cap \mathbb{Z}_q^\times,\ a_{12}, a_{21} \in A \right\}.$$

The proof relies on a result in [4] previously established by D. Covert, A. Iosevich and J. Pakianathan which implies that if $|A|$ is much larger than $\sqrt{\ell}\, q^{\left(1-\frac{1}{4\ell}\right)}$, then

$$|\{(a_{11}, a_{12}, a_{21}, a_{22}) \in A \times A \times A \times A : a_{11}a_{22} + a_{12}a_{21} = t\}| = |A|^4 q^{-1} + \mathscr{R}(t)$$

where $|\mathscr{R}(t)| \leq \ell\, |A|^2 q^{\left(1-\frac{1}{2\ell}\right)}$.

1. INTRODUCTION

In this paper we generalize a result found in [3] established by A. Iosevich and the first listed author. In [3], it is proven that if $A \subset \mathbb{F}_q \backslash \{0\}$ with $|A| > Cq^{\frac{5}{6}}$, then the product set $R(A) \cdot R(A)$ contains a positive proportion of all the elements of $SL_2(\mathbb{F}_q)$, where

$$R(A) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in SL_2(\mathbb{F}_q) : a_{11}, a_{12}, a_{21} \in A \right\}.$$

Let $SL_2(\mathbb{Z}_q)$ denote the set of two by two matrices with determinant one over $\mathbb{Z}_q$ where $q = p^\ell$, p prime, and $\ell > 0$. We begin with a definition similar to that of $R(A)$ mentioned above.

Definition 1.1. *Given $A \subset \mathbb{Z}_q$, $A \neq \langle p \rangle$ let*

$$P(A) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in SL_2(\mathbb{Z}_q) : a_{11} \in A \cap \mathbb{Z}_q^\times,\ a_{12}, a_{21} \in A \right\}.$$

Observe that the size of $P(A)$ is less than $|A|^3$. Our goal is to determine how large A needs to be to ensure that the product set $P(A) \cdot P(A) = \{M \cdot M' : M, M' \in P(A)\}$ contains a positive proportion of all the elements of $SL_2(\mathbb{Z}_q)$.

Our work is partly motivated by a result due to H. A. Helfgott who proved in [9] that multiplication by sets in the group $SL_2(\mathbb{Z}_p)$ expands rapidly across the group.

Theorem 1.2. *(Helfgott,* [9]*) Let p be a prime. Let E be a subset of $SL_2(\mathbb{Z}_p)$ not contained in any proper subgroup.*

Date: March 23, 2015.

2010 *Mathematics Subject Classification.* 05A05, 05A15, 11T24.

Key words and phrases. Special Linear Group, Fourier Transform.

Appeared in OJAC 2015. See `analytic-combinatorics.org`.

- *Assume that* $|E| < p^{3-\delta}$ *for some fixed* $\delta > 0$. *Then*
$$|E \cdot E \cdot E| > c|E|^{1+\epsilon},$$
where $c > 0$ *and* $\epsilon > 0$ *depend only on* δ.

- *Assume that* $|E| > p^{\delta}$ *for some fixed* $\delta > 0$. *Then there is an integer* $k > 0$, *depending only on* δ, *such that every element of* $SL_2(\mathbb{Z}_p)$ *can be expressed as a product of at most* k *elements of* $E \cup E^{-1}$.

See also [6], [10] and [7] for other generalizations and improvements of Helfgott's result. Expansion of finite groups have been studied in recent years and many of the best expanders are linked to the group of invertible matrices of determinant 1. Several papers are devoted to the study of this problem, however among them two breakthrough solutions were obtained in $SL_d(\mathbb{Z}/p^n\mathbb{Z})$ by J. Bourgain and A. Gamburd ([1]) and in $SL_d(\mathbb{Z}/q\mathbb{Z})$ by Bourgain and P. Varjú ([2]) for arbitrary q. Moreover, it is important to mention that sum - product estimates have applications to the incidence problem for lines. On this matter, H.A Helfgott and M. Rudnev prove in [11] an incidence Theorem in $\mathbb{Z}_p$.

What we prove in this paper is slightly different. We provide an estimate for the size of a subset A in $\mathbb{Z}/p^{\ell}\mathbb{Z}$ to get a product estimate in $SL_2(\mathbb{Z}/p^{\ell}\mathbb{Z})$. Our main result is the following.

Theorem 1.3. *Let* $A \subset \mathbb{Z}_q \backslash \{0\}$, $A \neq \langle p \rangle$, $q = p^{\ell}$, *and* $\ell \geq 2$ *with* $|A| \geq C\sqrt[3]{\ell^2}\, q^{\left(1-\frac{1}{4\ell}\right)}$. *Then there exists* $C' > 0$ *such that*

$$|P(A) \cdot P(A)| \geq C'|SL_2(\mathbb{Z}_q)| \geq C'' q^3. \tag{1}$$

Remark 1.4. *If* $\ell = 1$, *that is* $q = p$, *then* $\mathbb{Z}_q \cong \mathbb{F}_q$ *and we obtain the result in* [3]. *Also, observe that if* $A = \langle p \rangle$, *then* $P(A)$ *is the empty set and we see that the threshold assumption on the size of* A *in Theorem 1.3 cannot be improved beyond* $|A| \geq q^{1-\frac{1}{\ell}}$.

We shall make use of the following result due to D. Covert, A. Iosevich and J. Pakianathan ([4]).

Theorem 1.5. *Let* $E \subset \mathbb{Z}_q^d$, *where* $q = p^{\ell}$ *and define*

$$\nu(t) = |\{(x, y) \in E \times E : x \cdot y \equiv x_1 y_1 + \cdots + x_d y_d = t\}|.$$

Then $\nu(t) = |E|^2 q^{-1} + \mathscr{R}(t)$ *where for every* $t \in \mathbb{Z}_q^{\times}$, $|\mathscr{R}(t)| < \ell |E| q^{\frac{d-1}{2}\left(2-\frac{1}{\ell}\right)}$. *In particular, we have that* $\nu(t) > 0$ *whenever* $|E| >> \ell\, q^{\left(\frac{2\ell-1}{2\ell}\right)d+\frac{1}{2\ell}}$.

Remark 1.6. *We shall use Theorem 1.5 with* $E = A \times A$ *and* $d = 2$. *More precisely, we shall use the fact that if* $E = A \times A$ *and the size of* A *is much greater than* $\sqrt{\ell}\; q^{\left(1-\frac{1}{4\ell}\right)}$, *then*

$$|\{(a_{11}, a_{12}, a_{21}, a_{22}) \in A \times A \times A \times A : a_{11}a_{22} + a_{12}a_{21} = t\}| = |A|^4 q^{-1} + \mathscr{R}(t) \tag{2}$$

where $|\mathscr{R}(t)| \leq \ell\, |A|^2\, q^{\left(1-\frac{1}{2\ell}\right)}$.

It is worth mentioning that we have tried to generalize Theorem 1.3 to include a general non-prime q to no avail. The exponential sums get quite complicated and have to be estimated rather than directly evaluated. However, there has been progress in this direction. Recently, D. Covert obtained a distance result for all odd q ([5]). The authors plan to investigate the general q problem more in the near future.

1.1. **Fourier analysis used in this paper.** We shall make use of the following basic formulas of Fourier analysis on $\mathbb{Z}_q^d$. Let $f : \mathbb{Z}_q^d \to \mathbb{C}$ and let χ denote a non-trivial additive character on $\mathbb{Z}_q$. Define

$$\widehat{f}(m) = q^{-d} \sum_{x \in \mathbb{Z}_q^d} \chi(-x \cdot m) f(x).$$

It is not difficult to check that

$$(Inversion)\ f(x) = \sum_{m \in \mathbb{Z}_q^d} \chi(x \cdot m) \widehat{f}(m)$$

and

$$(Plancherel)\ \sum_{m \in \mathbb{Z}_q^d} |\widehat{f}(m)|^2 = q^{-d} \sum_{x \in \mathbb{Z}_q^d} |f(x)|^2.$$

2. Proof of Theorem 1.3 (estimate 1)

We are looking to solve the equation

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & \frac{1+a_{12}a_{21}}{a_{11}} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{21} \\ b_{12} & \frac{1+b_{12}b_{21}}{b_{11}} \end{pmatrix} = \begin{pmatrix} t & \alpha \\ \beta & \frac{1+\alpha\beta}{t} \end{pmatrix},$$

which leads to equations

$$a_{11}b_{11} + a_{12}b_{12} = t, \quad \frac{b_{21}}{b_{11}} t + \frac{a_{12}}{b_{11}} = \alpha, \quad \text{and} \quad \frac{a_{21}}{a_{11}} t + \frac{b_{12}}{a_{11}} = \beta. \tag{3}$$

Let $D_t(a_{11}, b_{11}, a_{12}, b_{12})$ denote the characteristic function of the set

$$D_t = \{(a_{11}, b_{11}, a_{12}, b_{12}) \in A \times A \times A \times A : a_{11}b_{11} + a_{12}b_{12} = t\}$$

and let $E = A \times A$. Then the number of six-tuplets satisfying the equations (3) is given by

$$\begin{aligned} \nu(t, \alpha, \beta) &= \frac{1}{q^2} \sum_{u,v \in \mathbb{Z}_q} \sum_{\substack{a_{11}, b_{11}, a_{12} \in \mathbb{Z}_q \\ b_{12}, a_{21}, b_{21} \in \mathbb{Z}_q}} D_t(a_{11}, b_{11}, a_{12}, b_{12}) E(a_{21}, b_{21}) \chi(u(b_{21}t + a_{12} - \alpha b_{11})) \chi(v(a_{21}t + b_{12} - \beta a_{11}) \\ &= q^{-2}|D_t||E| + q^4 \sum_{\mathbb{Z}_q^2 \setminus \{(0,0)\}} \widehat{D}_t(\beta v, \alpha u, -u, -v) \widehat{E}(tv, tu) \\ &= \nu_0(t, \alpha, \beta) + \nu_{main}(t, \alpha, \beta). \end{aligned}$$

So we have $\nu_0(t, \alpha, \beta) = \dfrac{|D_t||A|^2}{q^2}$.

Let $t \in \mathbb{Z}_q^\times$. We will now estimate $|D_t|$ using Theorem 1.5 and Remark 1.6 . By (2) we have

$$|D_t| = |A|^4 q^{-1} + \mathscr{R}(t) \leq \frac{|A|^4}{q} + \ell |A|^2 q^{\left(1 - \frac{1}{2\ell}\right)}. \tag{4}$$

It follows that

$$\begin{aligned}\nu_0(t,\alpha,\beta) &\leq \frac{|A|^4}{q^2}\left(\frac{|A|^2}{q}+\ell q^{\left(1-\frac{1}{2\ell}\right)}\right)\\ &= \frac{|A|^6}{q^3}+\frac{|A|^4}{q}\frac{\ell}{q^{\frac{1}{2\ell}}}.\end{aligned}$$

Thus, $\sum_{\substack{t\in\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}} \nu_0^2(t,\alpha,\beta) \leq q^3\left(\frac{|A|^6}{q^3}+\frac{|A|^4}{q}\frac{\ell}{q^{\frac{1}{2\ell}}}\right)^2$ which implies that

$$\sum_{\substack{t\in\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}} \nu_0^2(t,\alpha,\beta) \leq \frac{|A|^{12}}{q^3}+\frac{2\ell\,|A|^{10}}{q^{\left(1+\frac{1}{2\ell}\right)}}+\frac{q\ell^2\,|A|^8}{q^{\frac{1}{\ell}}}. \tag{5}$$

We now estimate $\sum_{\substack{t\in\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}} \nu_{main}^2(t,\alpha,\beta)$. By Cauchy-Schwartz and Plancherel we have

$$\begin{aligned}\nu_{main}^2(t,\alpha,\beta) &\leq q^8 \sum_{u,v\in\mathbb{Z}_q}\left|\widehat{D}_t(\beta v,\alpha u,-u,-v)\right|^2\cdot\sum_{u,v\in\mathbb{Z}_q}\left|\widehat{E}(tv,tu)\right|^2\\ &\leq |E|q^6\sum_{u,v\in\mathbb{Z}_q}\left|\widehat{D}_t(\beta v,\alpha u,-u,-v)\right|^2\\ &= |A|^2q^6\sum_{u,v\in\mathbb{Z}_q}\left|\widehat{D}_t(\beta v,\alpha u,-u,-v)\right|^2.\end{aligned}$$

It follows that

$$\sum_{\alpha,\beta\in\mathbb{Z}_q}\nu_{main}^2(t,\alpha,\beta) \leq |A|^2q^6\sum_{\substack{\alpha,\beta,\\ u,v\in\mathbb{Z}_q}}\left|\widehat{D}_t(\beta v,\alpha u,-u,-v)\right|^2. \tag{6}$$

In order to apply Plancherel we need to perform a change of variables. Write

$$\alpha=p^{\gamma_1}\alpha_0,\ \ \beta=p^{\gamma_2}\beta_0,\ \ u=p^{\gamma_3}u_0,\ \ v=p^{\gamma_4}v_0$$

where $\gamma_i\in\{0,1,2,\dots,\ell\}$, $i\in\{1,\dots,4\}$, and $u_0,v_0,\alpha_0,\beta_0\in\mathbb{Z}_q^\times$.

Let $D_t^p\left(y_1,y_2,y_3,y_4\right)$ denote the characteristic function of the set

$$D_t^p=\{(p^{\gamma_2+\gamma_4}x_1,\ p^{\gamma_1+\gamma_3}x_2,\ p^{\gamma_3}x_3,\ p^{\gamma_4}x_4)\,:\,\mathbf{x}=(x_1,x_2,x_3,x_4)\in D_t\}.$$

Note that if $\mathbf{m}=(m_1,m_2,m_3,m_4)$ and $\mathbf{y}=(y_1,y_2,y_3,y_4)$, then

$$\begin{aligned}\widehat{D}_t^p(\mathbf{m}) &= q^{-4}\sum_{\mathbf{y}\in\mathbb{Z}_q^4}\chi\left(-\mathbf{y}\cdot\mathbf{m}\right)D_t^p(\mathbf{y})\\ &= q^{-4}\sum_{\mathbf{y}\in D_t^p}\chi\left(-\mathbf{y}\cdot\mathbf{m}\right).\end{aligned}$$

Now, observe that $\mathbf{y} \in D_t^p$ means that $\mathbf{y} = (p^{\gamma_2+\gamma_4}x_1,\ p^{\gamma_1+\gamma_3}x_2,\ p^{\gamma_3}x_3,\ p^{\gamma_4}x_4)$ with $\mathbf{x} \in D_t$. Thus,

$$\begin{aligned}
\widehat{D}_t^p(\mathbf{m}) &= q^{-4}\sum_{\mathbf{y}\in D_t^p}\chi\left(-\mathbf{y}\cdot\mathbf{m}\right)\\
&= q^{-4}\sum_{\mathbf{x}\in D_t}\chi\left(-p^{\gamma_2+\gamma_4}x_1m_1 - p^{\gamma_1+\gamma_3}x_2m_2 - p^{\gamma_3}x_3m_3 - p^{\gamma_4}x_4m_4\right)\\
&= q^{-4}\sum_{\mathbf{x}\in\mathbb{Z}_q^4}\chi\left(-p^{\gamma_2+\gamma_4}x_1m_1 - p^{\gamma_1+\gamma_3}x_2m_2 - p^{\gamma_3}x_3m_3 - p^{\gamma_4}x_4m_4\right)D_t(\mathbf{x})\\
&= \widehat{D}_t\left(p^{\gamma_2+\gamma_4}m_1,\ p^{\gamma_1+\gamma_3}m_2,\ p^{\gamma_3}m_3,\ p^{\gamma_4}m_4\right).
\end{aligned}$$

Hence, for any $\mathbf{m} \in \mathbb{Z}_q^4$ we get the following relation:

$$\widehat{D}_t^p(m_1,m_2,m_3,m_4) = \widehat{D}_t\left(p^{\gamma_2+\gamma_4}m_1,\ p^{\gamma_1+\gamma_3}m_2,\ p^{\gamma_3}m_3,\ p^{\gamma_4}m_4\right).$$

Using this relation with the change of variables

$$\begin{aligned}
\alpha' &= \alpha_0u_0, \quad u' = -u_0\\
\beta' &= \beta_0v_0, \quad v = -v_0
\end{aligned}$$

we have

$$\begin{aligned}
\sum_{\substack{\alpha,\beta,\\ u,v\in\mathbb{Z}_q}}\left|\widehat{D}_t\left(\beta v,\alpha u,-u,-v\right)\right|^2 &= \sum_{\substack{\gamma_1,\gamma_2,\\ \gamma_3,\gamma_4\in\{0,\ldots,\ell-1\}}}\ \sum_{\substack{\alpha_0,\beta_0,\\ u_0,v_0\in\mathbb{Z}_q^\times}}\left|\widehat{D}_t\left(p^{\gamma_2+\gamma_4}\beta_0v_0,\ p^{\gamma_1+\gamma_3}\alpha_0u_0,\ -p^{\gamma_3}u_0,\ -p^{\gamma_4}v_0\right)\right|^2\\
&= \sum_{\substack{\gamma_1,\gamma_2,\\ \gamma_3,\gamma_4\in\{0,\ldots,\ell-1\}}}\ \sum_{\substack{\alpha',\beta',\\ u',v'\in\mathbb{Z}_q^\times}}\left|\widehat{D}_t\left(p^{\gamma_2+\gamma_4}\beta',\ p^{\gamma_1+\gamma_3}\alpha',\ p^{\gamma_3}u',\ p^{\gamma_4}v'\right)\right|^2\\
&\le \sum_{\substack{\gamma_1,\gamma_2,\\ \gamma_3,\gamma_4\in\{0,\ldots,\ell-1\}}}\ \sum_{\substack{\alpha',\beta',\\ u',v'\in\mathbb{Z}_q^\times}}\left|\widehat{D}_t^p\left(\beta',\alpha',u',v'\right)\right|^2\\
&\le \ell^4\sum_{\substack{\alpha',\beta',\\ u',v'\in\mathbb{Z}_q}}\left|\widehat{D}_t^p\left(\beta',\alpha',u',v'\right)\right|^2\\
&= q^{-4}\ell^4\sum_{\substack{x_1,x_2,\\ x_3,x_4\in\mathbb{Z}_q}}\left|D_t^p(x_1,x_2,x_3,x_4)\right|^2\\
&= q^{-4}\ell^4\left|D_t^p\right|\\
&\le q^{-4}\ell^4|D_t|
\end{aligned}$$

since $\left|D_t^p\right| \le |D_t|$. By (4) it follows that

$$\sum_{\substack{\alpha,\beta,\\ u,v\in\mathbb{Z}_q}}\left|\widehat{D}_t\left(\beta v,\alpha u,-u,-v\right)\right|^2 \le \ell^4q^{-4}\left(\frac{|A|^4}{q} + \ell|A|^2q^{\left(1-\frac{1}{2\ell}\right)}\right). \tag{7}$$

Now, using (6) and (7) we have that

$$\sum_{\substack{t\in\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}} \nu_{main}^2(t,\alpha,\beta) \leq \ell^4|A|^2q^6qq^{-4}\left(\frac{|A|^4}{q}+\ell\,|A|^2\,q^{\left(1-\frac{1}{2\ell}\right)}\right)$$

That is,

$$\sum_{\substack{t\in\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}} \nu_{main}^2(t,\alpha,\beta) \leq \ell^4\,|A|^6\,q^2+\ell^5\,|A|^4\,q^{\left(4-\frac{1}{2\ell}\right)}. \tag{8}$$

Hence, in view of (8) and (5) we have that

$$\sum_{\substack{t\in\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}} \nu^2(t,\alpha,\beta) \leq C\left(\frac{|A|^{12}}{q^3}+\frac{2\ell\,|A|^{10}}{q^{\left(1+\frac{1}{2\ell}\right)}}+\frac{q\ell^2\,|A|^8}{q^{\frac{1}{\ell}}}+\ell^4\,|A|^6\,q^2+\ell^5\,|A|^4\,q^{\left(4-\frac{1}{2\ell}\right)}\right). \tag{9}$$

Let $\text{Support}\big(\nu(t,\alpha,\beta)\big)$ be the characteristic function of the set

$$\text{Support}\,(\nu)=\Big\{(t,\alpha,\beta)\in\mathbb{Z}_q^3\,:\,\nu(t,\alpha,\beta)\neq 0\Big\}.$$

Now,

$$\left(|P\,(A)|^2-\sum_{\substack{t\in\mathbb{Z}_q\setminus\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}}\nu(t,\alpha,\beta)\right)^2=\left(\sum_{\substack{t\in\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}}\nu(t,\alpha,\beta)\,\text{Support}\big(\nu(t,\alpha,\beta)\big)\right)^2.$$

In view of (9) and applying the Cauchy-Schwarz Inequality, we have

$$\begin{aligned}\left(\sum_{\substack{t\in\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}}\nu(t,\alpha,\beta)\,\text{Support}\big(\nu(t,\alpha,\beta)\big)\right)^2 &\leq \left(\sum_{\substack{t\in\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}}\nu^2(t,\alpha,\beta)\right)\left(\sum_{\substack{t\in\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}}\text{Support}\big(\nu(t,\alpha,\beta)\big)\right)\\ &=\big|\text{Support}\,(\nu)\big|\sum_{\substack{t\in\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}}\nu^2(t,\alpha,\beta)\\ &\leq\big|\text{Support}\,(\nu)\big|\,C\left(\frac{|A|^{12}}{q^3}+\frac{2\ell\,|A|^{10}}{q^{\left(1+\frac{1}{2\ell}\right)}}+\frac{q\ell^2\,|A|^8}{q^{\frac{1}{\ell}}}+\ell^4\,|A|^6\,q^2+\ell^5\,|A|^4\,q^{\left(4-\frac{1}{2\ell}\right)}\right).\end{aligned}$$

Thus,

$$\left(|P\,(A)|^2-\sum_{\substack{t\in\mathbb{Z}_q\setminus\mathbb{Z}_q^\times\\ \alpha,\beta\in\mathbb{Z}_q}}\nu(t,\alpha,\beta)\right)^2\leq C\big|\text{Support}\,(\nu)\big|\left(\frac{|A|^{12}}{q^3}+\frac{2\ell\,|A|^{10}}{q^{\left(1+\frac{1}{2\ell}\right)}}+\frac{q\ell^2\,|A|^8}{q^{\frac{1}{\ell}}}+\ell^4\,|A|^6\,q^2+\ell^5\,|A|^4\,q^{\left(4-\frac{1}{2\ell}\right)}\right). \tag{10}$$

We now turn our attention to $\sum_{\substack{t\in\mathbb{Z}_q\setminus\mathbb{Z}_q^\times \\ \alpha,\beta\in\mathbb{Z}_q}} \nu(t,\alpha,\beta)$. Fixing a_{21} and b_{21} in A we have that

$$\sum_{\substack{t\in\mathbb{Z}_q\setminus\mathbb{Z}_q^\times \\ \alpha,\beta\in\mathbb{Z}_q}} \nu(t,\alpha,\beta) \le |A|^2 \,|\{(a_{11},b_{11},a_{12},b_{12}) \,:\, a_{11}b_{11}+a_{12}b_{12}=t\}|$$
$$\le |A|^2\,|A|^3\,|\{a_{11} \,:\, a_{11}b_{11}=t-a_{12}b_{12}\}|\,.$$

By a known result in Congruence Theory, $|\{a_{11} \,:\, a_{11}b_{11}=t-a_{12}b_{12}\}| < p^{\ell-1}$.

Thus, $\sum_{\substack{t\in\mathbb{Z}_q\setminus\mathbb{Z}_q^\times \\ \alpha,\beta\in\mathbb{Z}_q}} \nu(t,\alpha,\beta) \le |A|^2\,|A|^3\,p^{\ell-1} \le C\,|A|^6$ if $|A| \ge C\sqrt{\ell}\,q^{\left(1-\frac{1}{4\ell}\right)}$, as desired.

That is,

$$\sum_{\substack{t\in\mathbb{Z}_q\setminus\mathbb{Z}_q^\times \\ \alpha,\beta\in\mathbb{Z}_q}} \nu(t,\alpha,\beta) \le C\,|A|^6\,. \tag{11}$$

On the other hand,

$$\begin{aligned}
|P(A)| &\ge \left(p^\ell - p^{\ell-1}\right)^3 \\
&= p^{3\ell} - 3p^{3\ell-1} + 3p^{3\ell-2} - p^{3\ell-3} \\
&= q^3\left(\frac{p^3-3p^2+3p-1}{p^3}\right) \\
&= q^3\left(\frac{p-1}{p}\right)^3 \\
&\ge C\,|A|^3 \ \text{ where } \ C\in(0,1) \ \text{ if } \ |A| \ge C\sqrt{\ell}\,q^{\left(1-\frac{1}{4\ell}\right)} \ \text{ as desired.}
\end{aligned}$$

That is,

$$|P(A)| \gtrsim |A|^3\,. \tag{12}$$

So, (11) and (12) imply that

$$|P(A)|^2 - \sum_{\substack{t\in\mathbb{Z}_q\setminus\mathbb{Z}_q^\times \\ \alpha,\beta\in\mathbb{Z}_q}} \nu(t,\alpha,\beta) \ge (1-C)\,|A|^6\,.$$

That is,

$$\left(|P(A)|^2 - \sum_{\substack{t\in\mathbb{Z}_q\setminus\mathbb{Z}_q^\times \\ \alpha,\beta\in\mathbb{Z}_q}} \nu(t,\alpha,\beta)\right)^2 \ge (1-C)^2\,|A|^{12}\,. \tag{13}$$

By (10) and (13) we have

$$\big|\text{Support}\,(\nu)\big|\left(\frac{|A|^{12}}{q^3}+\frac{2\ell\,|A|^{10}}{q^{\left(1+\frac{1}{2\ell}\right)}}+\frac{q\ell^2\,|A|^8}{q^{\frac{1}{\ell}}}+\ell^4\,|A|^6\,q^2+\ell^5\,|A|^4\,q^{\left(4-\frac{1}{2\ell}\right)}\right)\geq(1-C)^2\,|A|^{12}.$$

This implies

$$\big|\text{Support}\,(\nu)\big|\geq\frac{(1-C)^2\,|A|^{12}}{\frac{|A|^{12}}{q^3}+\frac{2\ell|A|^{10}}{q^{\left(1+\frac{1}{2\ell}\right)}}+\frac{q\ell^2|A|^8}{q^{\frac{1}{\ell}}}+\ell^4\,|A|^6\,q^2+\ell^5\,|A|^4\,q^{\left(4-\frac{1}{2\ell}\right)}}.\tag{14}$$

To conclude the proof, we need to find the size of $|A|$ such that the term $\frac{|A|^{12}}{q^3}$ in (14) dominates all of the other terms in the denominator.

- $\frac{|A|^{12}}{q^3}\gtrsim\frac{2\ell|A|^{10}}{q^{\left(1+\frac{1}{2\ell}\right)}}\iff|A|^2\gtrsim 2\ell\,q^{\left(2-\frac{1}{2\ell}\right)}\iff|A|\gtrsim\sqrt{\ell}\,q^{\left(1-\frac{1}{4\ell}\right)}$
- $\frac{|A|^{12}}{q^3}\gtrsim\frac{q\ell^2|A|^8}{q^{\frac{1}{\ell}}}\iff|A|^4\gtrsim\ell^2 q^{\left(4-\frac{1}{\ell}\right)}\iff|A|\gtrsim\sqrt{\ell}\,q^{\left(1-\frac{1}{4\ell}\right)}$
- $\frac{|A|^{12}}{q^3}\gtrsim\ell^4\,|A|^6\,q^2\iff|A|^6\gtrsim\ell^4 q^5\iff|A|\gtrsim\sqrt[3]{\ell^2}\,q^{\frac{5}{6}}$
- $\frac{|A|^{12}}{q^3}\gtrsim\ell^5\,|A|^4\,q^{\left(4-\frac{1}{2\ell}\right)}\iff|A|^8\gtrsim\ell^5 q^{\left(7-\frac{1}{2\ell}\right)}\iff|A|\gtrsim\sqrt[8]{\ell^5}\,q^{\left(\frac{7}{8}-\frac{1}{16\ell}\right)}$

Hence, $\big|\text{Support}\,(\nu)\big|\gtrsim q^3$ if $|A|\gtrsim\sqrt[3]{\ell^2}\,q^{\max\left\{1-\frac{1}{4\ell},\,\frac{5}{6},\,\frac{7}{8}-\frac{1}{16\ell}\right\}}$. Now, noticing that $\max\left\{1-\frac{1}{4\ell},\,\frac{5}{6},\,\frac{7}{8}-\frac{1}{16\ell}\right\}=1-\frac{1}{4\ell}$ if $\ell\geq 2$, the proof is complete.

ACKNOWLEDGEMENTS

The authors sincerely thank Professor Alex Iosevich for the many helpful discussions concerning this paper. We would also like to thank the referees for their comments which added to the value of the paper.

REFERENCES

[1] Bourgain, J. (1-IASP-SM); Gamburd, A. (1-UCSC) *Random walks and expansion in $SL_d(\mathbb{Z}/p^n\mathbb{Z})$. II.* (English summary) With an appendix by Bourgain. J. Eur. Math. Soc. (JEMS) 11 (2009), no. 5, 1057-1103. https://www.math.ias.edu/files/bourgain/random.pdf

[2] Bourgain, J. (1-IASP-SM); Varjú, P. (1-PRIN) *Expansion in $SL_d(\mathbb{Z}/q\mathbb{Z})$; q arbitrary.* (English summary) Invent. Math. 188 (2012), no. 1, 151-173. http://arxiv.org/pdf/1006.3365.pdf

[3] Chapman, J. Iosevich, A. *On rapid Generation of $SL_2(\mathbb{F}_q)$* , Integers Electronic Journal of Combinatorial Number Theory, Volume 9 (2009), 47-52. http://www.emis.de/journals/INTEGERS/papers/j4/j4.Abstract.html

[4] Covert, D. Iosevich, A. Pakianathan, J. *Geometric configurations in the ring of integers modulo p^l*, (2011). http://arxiv.org/pdf/1105.5373.pdf

[5] Covert, D. *Results on the Erdős-Falconer distance problem in $\mathbb{Z}_q^d$ for odd q*, preprint. http://arxiv.org/pdf/1309.1495v2.pdf

[6] Dinai, O. *Growth in SL_2 over finite fields, J. Group Theory* **14**, No. 2, 273–297 (2011). http://www.degruyter.com/view/j/jgth.2011.14.issue-2/jgt.2010.056/jgt.2010.056.xml

[7] Gill, N. (4-BRST-SM); Helfgott, H.A. (4-BRST-SM) *Growth of small generating sets in* $SL_n(\mathbb{Z}/p\mathbb{Z})$, Int. Math. Res. Not. IMRN 2011, no. 18, 4226- 4251. http://arxiv.org/pdf/1002.1605v2.pdf

[8] Hart, D. Iosevich, A. *Sums and products in finite fields: an integral geometric viewpoint*, Contemporary Mathematics, (2007). http://arxiv.org/pdf/0705.4256.pdf

[9] Helfgott, H. A. *Growth and generation in* $SL_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. **167** (2008), 601-623. http://arxiv.org/pdf/math/0509024.pdf

[10] Helfgott, H. A. (4-BRST-SM) *Growth in* $SL_3(\mathbb{Z}/p\mathbb{Z})$. (English summary) J. Eur. Math. Soc. (JEMS) 13 (2011), no **3**, 761- 851. http://arxiv.org/pdf/0807.2027.pdf

[11] Helfgott, H.A. (4-BRST); Rudnev, M. (4-BRST) *An explicit incidence theorem in* $\mathbb{F}_p$ (English summary) Mathematika 57 (2011), no. 1, 135 - 145. http://arxiv.org/pdf/1001.1980v2.pdf

DEPARTMENT OF MATHEMATICS, LYON COLLEGE, 2300 HIGHLAND ROAD, BATESVILLE, AR, USA
E-mail address: jeremy.chapman@lyon.edu

DEPARTMENT OF MATHEMATICS, BECKER COLLEGE, 61 SEVER STREET, WORCESTER, MA, USA
E-mail address: adriano.marzullo@becker.edu