Annales Univ. Sci. Budapest., Sect. Comp. 54 (2023) 245–252

SUBSETS OF $\mathbb{F}_p^*$ WITH ONLY SMALL PRODUCTS OR RATIOS

Patrick Letendre (Lévis, Canada)

Communicated by Jean-Marie De Koninck
(Received May 1, 2023; accepted July 2, 2023)

Abstract. Let p be a fixed prime. We estimate the number of elements of a set $A \subseteq \mathbb{F}_p^*$ for which

$$s_1 s_2 \equiv a \pmod p \quad \text{for some} \quad a \in [-X, X] \quad \text{for all} \quad s_1, s_2 \in A.$$

We also consider variations and generalizations.

1. Introduction and notation

Let p be a fixed prime number. For any member α of an equivalence class of $\mathbb{Z}/p\mathbb{Z}$, we write

$$|\alpha|_p := \min_{k \in \mathbb{Z}} |\alpha + kp|$$

and for any finite set A we write $|A| := \#A$ which should not be confused with the norm of a complex number. Inspired by the paper [2], we are interested by the cardinality of a set $A \subseteq \mathbb{F}_p^*$ that satisfies a particular property. Precisely, for each $X \geq 1$ we let $\mathcal{S}(X)$ be the set of all subsets $A \subseteq \mathbb{F}_p^*$ that satisfy

$$\left|\frac{s_1}{s_2}\right|_p \leq X \text{ and/or } \left|\frac{s_2}{s_1}\right|_p \leq X \text{ for each } (s_1, s_2) \in A^2. \tag{1.1}$$

We thus define

$$S(X) := \max_{A \in \mathcal{S}(X)} |A|.$$

Key words and phrases: Congruences, special sets $\pmod p$.
2010 Mathematics Subject Classification: 11A07, 11B75.

Similarly, for each integer $n \geq 2$ and $X \geq 1$ we let $\mathcal{R}_n(X)$ be the set of all subsets $A \subseteq \mathbb{F}_p^*$ that satisfy

$$|s_1 \cdots s_n|_p \leq X \text{ for all pairwise distinct } s_1, \ldots, s_n \in A. \tag{1.2}$$

Then, we consider the quantity

$$R_n(X) := \max_{A \in \mathcal{R}_n(X)} |A|.$$

For any $n \in \mathbb{N}$ and $m \in \mathbb{Z}^*$, we write

$$\tau_n(m) := \#\{(d_1, \ldots, d_n) \in \mathbb{N}^n : \ d_1 \cdots d_n = m\}.$$

We will often use the well known fact that $\tau_n(m) \ll_{n,\epsilon} m^\epsilon$ for each integer $n \geq 2$ and real $\epsilon > 0$. We also write $e_p(z) := \exp\bigl(\frac{2\pi i z}{p}\bigr)$ for any $z \in \mathbb{C}$.

2. Statement of theorems

Theorem 2.1. *Let $t > 0$ be a small fixed real number. For each $1 \leq X \leq \leq \bigl(\frac{1}{4} - t\bigr)p$, we have*

$$S(X) \ll_{\epsilon,t} \min\left(X^\epsilon + \frac{X^{2+\epsilon}}{p}, p^{1/2}\right)$$

for each fixed $\epsilon > 0$.

Theorem 2.2. *Let $t > 0$ be a small fixed real number. For each integer $n \geq 2$ and $1 \leq X \leq \bigl(\frac{1}{2} - t\bigr)p$, we have*

$$R_n(X) \ll_{\epsilon,t,n} \min\left(X^{1/n+\epsilon} + \frac{X^{n/(n-1)+\epsilon}}{p^{1/(n-1)}}, p^{1/n+\epsilon}\right)$$

for each fixed $\epsilon > 0$.

3. Preliminary lemmas

There are a number of interesting results in the literature concerning multilinear exponential sums; see [1], [4], [5] and [6] for example. We will need the following two.

Lemma 3.1. *Let $A_1, \ldots, A_n \subseteq \mathbb{F}_p^*$ $(n \geq 2)$ be subsets. Then*

$$\left|\sum_{a_1 \in A_1, \ldots, a_n \in A_n} e_p(a_1 \cdots a_n)\right| \leq p^{1/2}(|A_1| \cdots |A_n|)^{\frac{n-1}{n}}. \tag{3.1}$$

Proof. We assume that $|A_1| \geq |A_2| \geq \cdots \geq |A_n|$. The inequality follows from the well known result

$$\max_{m \in \mathbb{F}_p^*} \left| \sum_{a_1 \in A_1, a_2 \in A_2} e_p(m a_1 a_2) \right| \leq (p|A_1||A_2|)^{1/2},$$

see [5, (1.2)]. ∎

Lemma 3.2. *Let $0 < \delta < 1/4$ and $n \in \mathbb{Z}_+$. There is and effectively computable constant $\delta' = \delta'(\delta) > 0$ such that if p is a sufficiently large prime and $A_1, \ldots, A_n \subset \mathbb{F}_p$ satisfy*
(i) $|A_i| > p^{\delta}$ *for* $1 \leq i \leq n$;
(ii) $\prod_{i=1}^n |A_i| > p^{1+\delta}$;
then there is the exponential sum bound

$$\left| \sum_{a_1 \in A_1, \ldots, a_n \in A_n} e_p(a_1 \cdots a_n) \right| < p^{-\delta'} |A_1| \cdots |A_n|.$$

Proof. It follows from Theorem A of the paper [1]. ∎

The purpose of the following lemma is very similar to Lemma 4.1 of [3].

Lemma 3.3. *Let $\epsilon > 0$ be a real number. Let also $0 \leq \Delta \leq 1 - 2\epsilon$ be a real number. Consider the 1-periodic function defined on $[-\frac{1}{2}, \frac{1}{2})$ by*

$$f(x) := \begin{cases} 0 & -\frac{1}{2} \leq x < -\frac{\Delta}{2} - \epsilon, \\ \frac{x}{\epsilon} + \frac{\Delta}{2\epsilon} + 1 & -\frac{\Delta}{2} - \epsilon \leq x < -\frac{\Delta}{2}, \\ 1 & -\frac{\Delta}{2} \leq x < \frac{\Delta}{2}, \\ -\frac{x}{\epsilon} + \frac{\Delta}{2\epsilon} + 1 & \frac{\Delta}{2} \leq x < \frac{\Delta}{2} + \epsilon, \\ 0 & \frac{\Delta}{2} + \epsilon \leq x < \frac{1}{2}. \end{cases}$$

The function

$$g(x) := \Delta + \epsilon + \sum_{0 < |k| \leq \lceil 1/\epsilon^2 \rceil} (\cos(\pi k \Delta) - \cos(\pi k(\Delta + 2\epsilon))) \frac{e(kx)}{2\epsilon(\pi k)^2}$$

satisfies

$$|f(x) - g(x)| \leq \frac{2\epsilon}{\pi^2}$$

for each $x \in \mathbb{R}$.

Proof. The function $g(x)$ is simply the Fourier series of the function $f(x)$ that has been truncated to keep only the terms with $|k| \leq \lceil 1/\epsilon^2 \rceil$. ∎

4. Proof of Theorem 2.1

We assume throughout the proof that $A \in \mathcal{S}(X)$ and satisfies $S(X) = |A|$. We begin with the first inequality. We choose $s_1 \in A$ that satisfies (1.1) with every element of A by being at least $\frac{|A|}{2}$ times at the denominator. We denote by A_1 the set of values that are thereby at the numerator. Restricting our attention to A_1, we choose $s_2 \in A_1$ that satisfies (1.1) with every element of A_1 by being at least $\frac{|A_1|}{2}$ times at the numerator and we denote by A_2 the set of values that are thereby at the denominator.

Now, for each value $s \in A_2$ we have two representations. Indeed,

$$\frac{s}{s_1} \equiv a \pmod{p} \quad \text{and} \quad \frac{s_2}{s} \equiv b \pmod{p} \quad \text{with} \quad 0 < |a|, |b| \leq X.$$

We deduce that

$$s_1 a \equiv \frac{s_2}{b} \pmod{p} \ \Rightarrow\ ab \equiv \frac{s_2}{s_1} \equiv: \alpha \pmod{p} \quad \text{with} \quad 0 < |a|, |b|, |\alpha| \leq X.$$

We thus have $ab = \alpha + Kp$ with $0 \leq |K| \leq \left\lfloor \frac{2X^2}{p} \right\rfloor$. For each fixed value of K, the number of solutions (a, b) is at most $2\tau_2(\alpha + Kp) \ll X^{\epsilon}$. Indeed, we either have X so small that K is only 0 and thus the inequality follows from the inequality for the divisors function for an $\alpha \leq X$, otherwise, we have X large and the inequality remains true. We deduce that

$$|A| \leq 4|A_2| \ll X^{\epsilon}\left(1 + \frac{X^2}{p}\right).$$

We now turn to the second inequality. We can assume that $|A|$ and p are large enough. We will apply Lemma 3.3 with $\Delta := \frac{2X}{p}$ and $\epsilon < \frac{t}{100}$ small enough. We get

$$\begin{aligned}
\frac{|A|^2 + |A|}{2} &\leq \sum_{s_1, s_2 \in A} f\Big(\frac{s_1 s_2^{-1}}{p}\Big) = \\
&= \sum_{s_1, s_2 \in A} g\Big(\frac{s_1 s_2^{-1}}{p}\Big) + O(\epsilon |A|^2) \leq \\
&\leq \Delta |A|^2 + C \log(1/\epsilon) \max_{0 < |k| \leq \lceil 1/\epsilon^2 \rceil} \Big| \sum_{s_1, s_2 \in A} e_p(k s_1 s_2^{-1}) \Big| + O(\epsilon |A|^2)
\end{aligned}$$

for some constant C large enough. We deduce that there is a value of k, with $0 < |k| \leq \lceil 1/\epsilon^2 \rceil < p$, such that

$$\frac{t|A|^2}{\log(1/\epsilon)} \ll \Big| \sum_{s_1, s_2 \in A} e_p(k s_1 s_2^{-1}) \Big| \leq p^{1/2} |A|.$$

The second inequality follows from Lemma 3.1. The proof is complete. ■

5. Proof of Theorem 2.2

We assume throughout the proof that $A \in \mathcal{R}_n(X)$ and satisfies $R_n(X) = |A|$. Also, for any $k \geq 1$, we say that $(s_1, \ldots, s_k)$ is an *admissible* k-tuple if the s_j are pairwise distinct ($j = 1, \ldots, k$). There are exactly $|A| \cdot (|A| - 1) \cdots (|A| - k + 1)$ admissible k-tuples. We can assume that $|A|$ is large enough since otherwise there is nothing to prove.

We begin with the second inequality. Proceeding as previously, we write

$$\begin{aligned} |A|^n &\leq \sum_{\substack{s_1,\ldots,s_n \in A \\ (s_1,\ldots,s_n) \text{ admissible}}} f\Big(\frac{s_1 \cdots s_n}{p}\Big) + O(|A|^{n-1}) = \\ &= \sum_{s_1,\ldots,s_n \in A} g\Big(\frac{s_1 \cdots s_n}{p}\Big) + O(\epsilon|A|^n + |A|^{n-1}) \leq \\ &\leq \Delta|A|^n + C\log(1/\epsilon) \max_{0<|k|\leq\lceil 1/\epsilon^2\rceil} \Big| \sum_{s_1,\ldots,s_n \in A} e_p(ks_1 \cdots s_n)\Big| + \\ &\quad + O(\epsilon|A|^n + |A|^{n-1}). \end{aligned}$$

Now, assuming that $|A| > p^{1/n+\delta}$ for some fixed $0 < \delta < 1/4n$, we get to

$$\frac{t|A|^n}{\log(1/\epsilon)} \ll \Big| \sum_{s_1,\ldots,s_n \in A} e_p(ks_1 \cdots s_n)\Big| \leq p^{-\delta'}|A|^n$$

for some $\delta' > 0$, from Lemma 3.2. This is a contradiction for p large enough and we deduce that $|A| \ll p^{1/n+\epsilon}$ for each $\epsilon > 0$. Also, in the case $n = 2$, we can take $\epsilon = 0$ by using Lemma 3.1 instead.

For the first inequality, we define α by

$$\pm\alpha := \max_{\substack{r_1,\ldots,r_n \in A \\ (r_1,\ldots,r_n) \text{ admissible}}} |r_1 \cdots r_n|_p,$$

and we assume that $\alpha \equiv s_1 \cdots s_n \pmod p$ (with $(s_1, \ldots, s_n)$ admissible). We now define a change of variables according to this choice. In the set $A' := A \setminus \{s_1, \ldots, s_n\}$, we can write an element r as $r \equiv a_j \frac{s_j}{\alpha} \pmod p$ for some $0 < |a_j| \leq X$ ($j = 1, \ldots, n$).

Any of the $|A'| \cdot (|A'| - 1) \cdots (|A'| - n + 1)$ admissible n-tuples $(r_1, \ldots, r_n)$ gives rise to

$$r_1 \cdots r_n \equiv c \pmod p \;\Rightarrow\; a_1\frac{s_1}{\alpha} \cdots a_n\frac{s_n}{\alpha} \equiv c \pmod p \tag{5.1}$$

$$\Rightarrow\; a_1 \cdots a_n \equiv c\alpha^{n-1} \pmod p$$

$$\Rightarrow\; a_1 \cdots a_n = c\alpha^{n-1} + Kp \tag{5.2}$$

where $0 < |c|, |a_1|, \ldots, |a_n| \le X$ and $0 \le |K| \le \lfloor \frac{2X^n}{p} \rfloor$. From there, we distinguish two cases.

Case 1: $K = 0$ for more than half of the admissible n-tuples. In this case, we have

$$\begin{aligned} |A'|^n &\ll |\{(a_1, \ldots, a_n) \in \mathbb{Z}^n : \ a_1 \cdots a_n = c\alpha^{n-1}, \ 0 < |\alpha|, |c| \le X\}| = \\ &= 2^{n-1} \sum_{0<|c|\le X} \tau_n(c\alpha^{n-1}) \ll X^{1+\epsilon} \end{aligned}$$

for each fixed $\epsilon > 0$.

Case 2: $K \neq 0$ for at least half of the admissible n-tuples. In this case, we fix a value of $r = r_1 \equiv a^{\frac{s_1}{\alpha}} (\not\equiv 0) \pmod p$ that is in $\gg |A'|^{n-1}$ admissible n-tuples $(r, r_2, \ldots, r_n)$ in (5.1) that lead to (5.2) with $K \neq 0$. Then, we consider the congruence

$$\begin{aligned} rr_2 \cdots r_n \equiv c \pmod p \quad &\Rightarrow \quad aa_2 \cdots a_n \equiv c\alpha^{n-1} \pmod p \\ &\Rightarrow \quad aa_2 \cdots a_n = c\alpha^{n-1} + Kp \end{aligned}$$

with $0 < |c|, |a_2|, \ldots, |a_n| \le X$ and $0 < |K| \le \lfloor \frac{2X^n}{p} \rfloor$. Now, we write $d :=$ $:= gcd(a, \alpha^{n-1})$ and $a' := \frac{a}{d}$, $\beta := \frac{\alpha^{n-1}}{d}$ and $K' := \frac{K}{d}$. We find that

$$aa_2 \cdots a_n = c\alpha^{n-1} + Kp \ \Rightarrow \ a'a_2 \cdots a_n \equiv K'p \pmod \beta$$

so that a fixed value of K' gives at most d values of $a_2 \cdots a_n \pmod{\alpha^{n-1}}$. There are $\ll \frac{X^n}{dp}$ possible values for K' and since $0 < |a_2 \cdots a_n| \le |\alpha|^{n-1}$, we have in fact at most $2d$ values of $a_2 \cdots a_n$. That is, we have at most $\ll \frac{X^n}{p}$ possible values of (c, K). We get

$$|A'|^{n-1} \ll \sum_{\substack{(c,K) \\ c\alpha^{n-1}+Kp\neq 0}} \tau_{n-1}\left(\frac{c\alpha^{n-1} + Kp}{a}\right) \ll \frac{X^{n+\epsilon}}{p}$$

for each fixed $\epsilon > 0$. For $n = 2$ we have in fact $\epsilon = 0$ in this last inequality. The result follows.

Remark 5.1. There are various inequalities more effective for some medium size of the parameter X in Theorem 2.2. Using the same notation as previously, we write

$$r_k(a) := |\{(r_1, \ldots, r_k) \in A'^k \text{ admissible} : \ r_1 \cdots r_k \equiv a \pmod p\}|$$

for each $k = 1, \ldots, n-1$. For a fixed value of k we can split each admissible n-tuple $(r_1, \ldots, r_n) \in A'^n$ into $r_1 \cdots r_n \equiv bc \equiv a \pmod p$, i.e. respectively

$r_1 \cdots r_{n-k} \equiv b \pmod p$ and $r_{n-k+1} \cdots r_n \equiv c \pmod p$. This leads to

$$\begin{aligned}
|A'| \cdots (|A'| - n + 1) &\le \sum_{0<|a|\le X} \sum_{b=1}^{p-1} r_{n-k}(b) r_k(ab^{-1}) \le \\
&\le \max_{m\in\mathbb{F}_p^*} r_k(m) \sum_{0<|a|\le X} \sum_{b=1}^{p-1} r_{n-k}(b) = \\
&= 2X|A'| \cdots (|A'| - n + k + 1) \max_{m\in\mathbb{F}_p^*} r_k(m).
\end{aligned}$$

Now, for any fixed $m \in \mathbb{F}_p^*$ we use the change of variables from the proof of the first inequality to write

$$\begin{aligned}
r_1 \cdots r_k \equiv m \pmod p \quad &\Rightarrow \quad a_1 \cdots a_k \equiv \ell \pmod p \quad (\text{for some } \ell = \pm|\ell|_p) \\
&\Rightarrow \quad a_1 \cdots a_k = \ell + Kp \quad \left(\text{with } 0 \le |K| \le \left\lfloor \frac{2X^k}{p} \right\rfloor\right).
\end{aligned}$$

As previously, we deduce that

$$r_k(m) \le 2^{k-1} \sum_K \tau_k(\ell + Kp) \ll X^\epsilon \left(1 + \frac{X^k}{p}\right).$$

Overall, we get to

$$|A| \ll |A'| \ll \left(X^{1/k} + \frac{X^{1+1/k}}{p^{1/k}}\right) X^\epsilon$$

for any $k = 1, \ldots, n-1$.

6. Concluding remarks

The set

$$A := \{\pm 2^k : k = 0, \ldots, \lfloor \log(X)/\log(2) \rfloor\}$$

shows that $S(X) \gg \log(2X)$. Also, the set

$$A := \{\pm 1, \ldots, \pm \lfloor X^{1/n} \rfloor\}$$

shows that $R_n(X) \gg X^{1/n}$. We conjecture that both $S(X) \ll_{\epsilon,t} X^\epsilon$ and $R_n(X) \ll_{\epsilon,t,n} X^{1/n+\epsilon}$ hold for each $\epsilon > 0$ when $X \le \left(\frac{1}{2} - t\right) p$ for a fixed $t > 0$ as $p \to \infty$.

References

[1] **Bourgain, J.,** Multilinear exponential sums in prime fields under optimal entropy condition on the sources, *Geom. Funct. Anal.*, **18** (2009), no. 5, 1477–1502.

[2] **Cilleruelo, J. and M. Z. Garaev,** Concentration of points on two and three dimensional modular hyperbolas and applications, *Geom. Funct. Anal.*, **21** (2011), no. 4, 892–904.

[3] **Green, B. and A. Harper,** Inverse questions for the large sieve, *Geom. Funct. Anal.*, **24** (2014), no. 4, 1167–1203.

[4] **Macourt, S.,** Incidence results and bounds of trilinear and quadrilinear exponential sums, *SIAM J. Discrete Math.*, **32** (2018), no. 2, 815–825.

[5] **Petridis, G. and I. E. Shparlinski,** Bounds of trilinear and quadrilinear exponential sums, *J. Anal. Math.*, **138** (2019), no. 2, 613–641.

[6] **Shkredov, I.D.,** On asymptotic formulae in some sum-product questions, *Trans. Moscow Math. Soc.*, **79** (2018), 231–281.

P. Letendre
Lévis
Canada
Patrick.Letendre.1@ulaval.ca