On the sum–product phenomenon

I. D. Shkredov

Steklov Mathematical Institute

Introduction

Let $\mathrm{R} = \mathrm{R}(+, \cdot)$ be a ring and $A, B \subseteq \mathrm{R}$ be any finite sets.

$$A + B := \{a + b \ : \ a \in A,\ b \in B\} \qquad \text{(sumset)}$$

$$A \cdot B := \{a \cdot b \ : \ a \in A,\ b \in B\} \qquad \text{(product set)}$$

We study both operations simultaniously ($=$ Arithmetic Combinatorics).

$$A+A=\{1,2,\dots,n\}+\{1,2,\dots,n\}=\{2,3,\dots,2n\}\,,$$

$$B\cdot B=\{10,10^2,\dots,10^n\}\cdot\{10,10^2,\dots,10^n\}=\{10^2,10^3,\dots,10^{2n}\}$$

Thus, there are sets $A, B \subset \mathbb{Z}$ s.t. $|A+A| \ll |A|$, $|B \cdot B| \ll |B|$.

On the other hand,

$$|AA| \gg \frac{|A|^2}{\log^c |A|} \qquad \text{and} \qquad |B+B| = \binom{|B|}{2} \gg |B|^2\,.$$

Conjecture (Erdős–Szemerédi, 1983)

Let $A \subset \mathbb{Z}$, $|A| < \infty$. Then

$$\max\{|A+A|, |AA|\} \gg |A|^{2-\varepsilon}, \qquad |A| \to \infty,$$

where $\varepsilon > 0$ is an arbitrary.

The weak sum–product principle:

Theorem (Erdős–Szemerédi, 1983)

Let $A \subset \mathbb{Z}$, $|A| < \infty$. Then

$$\max\{|A+A|, |AA|\} \gg |A|^{1+c}.$$

where $c > 0$ is an absolute constant.

Methods of Number Theory: Erdős–Szemerédi, Nathanson, Ford.
This approach gave weak bounds (= small constant c).

Theorem (Elekes, 1997)

Let $A \subset \mathbb{R}$. Then

$$\max\{|A+A|, |AA|\} \gg |A|^{5/4} .$$

Elekes was the first who realized the connection between the sum–product and geometrical questions, namely, with *incidence geometry*.

The geometrical method works in $\mathbb{R}$ and in $\mathbb{C}$.

Incidence geometry

Let

$$\mathcal{P} \subseteq \mathbb{R}^2 \text{ be a finite number of points}$$

and

$$\mathcal{L} \text{ be a finite number of lines.}$$

Then the number of *incidences* between the points $\mathcal{P}$ and the lines $\mathcal{L}$ is

$$\mathcal{I}(\mathcal{P}, \mathcal{L}) := |\{(p, l) \ : \ p \in \mathcal{P},\, l \in \mathcal{L},\, p \in l\}|\,.$$

Trivial bounds:

$$\mathcal{I}(\mathcal{P}, \mathcal{L}) \le |\mathcal{P}||\mathcal{L}|\,,$$

$$\mathcal{I}(\mathcal{P}, \mathcal{L}) \le \min\{|\mathcal{L}||\mathcal{P}|^{1/2} + |\mathcal{L}|, |\mathcal{P}||\mathcal{L}|^{1/2} + |\mathcal{P}|\}\,.$$

Szemerédi–Trotter

We call a set $\mathcal{L}$ of continuous plane curves a *pseudo-line system* if any two members of $\mathcal{L}$ share at most one point in common (and vice versa).

Theorem (Szemerédi–Trotter, 1983)

Let $\mathcal{P}$ be a set of points and let $\mathcal{L}$ be a pseudo-line system. Then

$$\mathcal{I}(\mathcal{P},\mathcal{L}) = |\{(p,l)\in\mathcal{P}\times\mathcal{L} : p\in l\}| \ll$$
$$\ll (|\mathcal{P}||\mathcal{L}|)^{2/3} + |\mathcal{P}| + |\mathcal{L}|\,.$$

Theorem (Elekes, 1997)

Let $A \subseteq \mathbb{R}$. Then

$$\max\{|A \cdot A|, |A + A|\} \gg |A|^{5/4}\,,$$

$\mathcal{P} = (A + A) \times (A \cdot A)$.
$\mathcal{L} = \{l_{a,b}\}$, $a \in A$, $b \in A$, where

$$l_{a,b} = \{(x, y) \;:\; y = a(x - b)\}\,.$$

Any $l_{a,b} \in \mathcal{L}$ has $|A|$ points from $\mathcal{P}$, namely $(b + c, ac)$, $c \in A$.

$$|A|^3 \ll (|\mathcal{P}||\mathcal{L}|)^{2/3} \leq |A + A|^{2/3}|A \cdot A|^{2/3}|A|^{4/3}\,.$$

Modern sum–product results in $\mathbb{R}$

Theorem (Solymosi, 2008)

Let $A \subset \mathbb{R}$. Then

$$\max\{|A \cdot A|, |A + A|\} \gg |A|^{4/3-\varepsilon}.$$

Theorem (Konyagin–Shkredov, Rudnev–Stevens–Shkredov, 2016–2017)

Let $A \subset \mathbb{R}$. Then

$$\max\{|A + A|, |AA|\} \gg |A|^{4/3+c}, \qquad |A| \to \infty,$$

where $c > 0$ is an absolute constant.

General sum–products

General principle

If A belongs to a ring $\mathcal{R}(+,*)$ and

$$|A+A|, |A*A| \ll |A|^{1+\varepsilon},$$

then A has "large" intersection with a subring.

Exm. 1. Let $\mathcal{R} = \mathbb{F}_p$. Then $\mathbb{F}_p + \mathbb{F}_p = \mathbb{F}_p$, $\mathbb{F}_p * \mathbb{F}_p = \mathbb{F}_p$.
Exm. 2. Let $\mathcal{R} = \mathbb{F}_{p^2}$. Then the subring $\mathbb{F}_p \subseteq \mathcal{R}$ does not grow.
Exm. 3. Let $\mathcal{R} = \mathbb{Z}/m\mathbb{Z}$. Then for any divisor $d|m$ the subring $\{0, d, 2d, \dots, m-d\}$ does not grow.

Additive/multiplicative shifts of subrings do not grow as well.

Finite fields

Bourgain–Katz–Tao, 2004 / Bourgain–Glibichuk–Konyagin, 2006

Let $A \subseteq \mathbb{F}_p$, $|A| < p^{1-\varepsilon}$. Then there is $\delta = \delta(\varepsilon) > 0$ s.t.

$$\max\{|A \cdot A|, |A + A|\} \gg_\varepsilon |A|^{1+\delta} .$$

Large A:

Theorem (Garaev, 2007–2008)

Let $A \subseteq \mathbb{F}_p$, $|A| \gg p^{2/3}$. Then

$$\max\{|A \cdot A|, |A + A|\} \gg p^{1/2}|A|^{1/2}$$

and this is sharp.

Further works for small subsets A:
Garaev $(\frac{1}{14})$, Katz–Shen $(\frac{1}{13})$, Bourgain–Garaev $(\frac{1}{12}-\varepsilon)$, Li $(\frac{1}{12})$.

Theorem 1/11 (Rudnev, 2011)

Let $A \subseteq \mathbb{F}_p$, $|A| < p^{1/2}$. Then

$$\max\{|A \cdot A|, |A+A|\} \gg |A|^{12/11-\varepsilon} .$$

Combinatorial rather geometrical methods.

Conjecture (Erdős–Szemerédi in $\mathbb{F}_p$)

Let $A \subseteq \mathbb{F}_p$, $|A| < p^{1/3}$. Then

$$\max\{|A \cdot A|, |A+A|\} \gg |A|^{2-\varepsilon} .$$

Sum–product

Let $A \subseteq \mathbb{F}_p$, $|A| > p^\delta$. Then there is $k = k(\delta)$ such that

$$kA^k - kA^k = \mathbb{F}_p \,.$$

Sum–product but not *product–sum*.

Conjecture

Let $A \subseteq \mathbb{F}_p$, $|A| > p^\delta$. Then there is $k = k(\delta)$ such that

$$(kA)^k/(kA)^k = \mathbb{F}_p^* \,?$$

Modern sum–product results in $\mathbb{F}_p$

Theorem (Roche-Newton–Rudnev–Shkredov, 2016 Askoy-Yazici–Murphy–Rudnev–Shkredov, 2017)

Let $A \subset \mathbb{F}_p$, $|A| < p^{5/8}$. Then

$$\max\{|A+A|, |AA|\} \gg |A|^{1+1/5} .$$

Theorem (Rudnev, 2017)

Let $\mathcal{P}, \Pi$ be finite sets of points and planes in $\mathbb{F}_p^3$, $|\mathcal{P}| \le |\Pi|$ and $|\mathcal{P}| = O(p^2)$. Also, let k be the maximal number of collinear points in $\mathcal{P}$. Then

$$|\mathcal{I}(\mathcal{P}, \Pi)| := |\{(q, \pi) \in \mathcal{P} \times \Pi : \, q \in \pi\}| \ll |\Pi|\sqrt{|\mathcal{P}|} + k|\Pi| .$$

Applications: exponential sums

Theorem (Bourgain–Glibichuk–Konyagin, 2006)

Let $\delta \in (0,1]$, p be a prime number and $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| \ge p^\delta$. Then there is $\varepsilon = \varepsilon(\delta) > 0$ such that $\xi \neq 0$ one has

$$|\sum_{x\in\Gamma} e^{2\pi i x\xi/p}| \ll |\Gamma| p^{-\varepsilon} \,.$$

Thus, any multiplicative subgroup Γ, $|\Gamma| \ge p^\delta$ is uniformly distributed or, in other words, for any $a, b \in \{1, 2, \dots, p\}$ one has

$$|\Gamma \cap [a,b]| = \frac{|\Gamma|}{p} \cdot (b-a) + O(|\Gamma|^{1-\varepsilon'}) \,.$$

Another consequence is the uniform distribution of Diffie–Hellman sequence (Bourgain, 2004)

$$(g^x, g^y, g^{xy}) \in \mathbb{F}_p^3 ,$$

where $1 \le x, y \le p^\delta$.

Bourgain's expander map. If

$$x * y := x^2 + xy , \qquad x, y \in \mathbb{F}_p ,$$

then for any $A, B \subseteq \mathbb{F}_p$, $|A| = |B|$

$$|A * B| = |\{a * b \;:\; a \in A,\ b \in B\}| \gg \min\{|A|^{1+\varepsilon}, p\} .$$

Bourgain (2005), Shkredov (2010).

Multilinear exponential sums

Classical (Vinogradov, Erdős, ...) bound:
for any two sets $X_1, X_2 \subseteq \mathbb{F}_p$ one has

$$\left| \sum_{x_1 \in X_1} \sum_{x_2 \in X_2} e^{\frac{2\pi i x_1 x_2}{p}} \right| \le \sqrt{p|X_1||X_2|}\,.$$

Nontrivial if

$$|X_1||X_2| > p^{1+\delta}\,.$$

Many sets.

Theorem (Bourgain, 2009)

For any sets $X_1, \dots, X_n \subseteq \mathbb{F}_p$ with

$$|X_j| > p^\delta \qquad \text{and} \qquad |X_1||X_2| \dots |X_n| > p^{1+\delta} \,.$$

Then there is $\varepsilon = \varepsilon(\delta) > 0$ such that

$$\left| \sum_{x_1 \in X_1} \dots \sum_{x_n \in X_n} e^{\frac{2\pi i x_1 \dots x_n}{p}} \right| \ll \Big(\prod_{j=1}^{n} |X_j|\Big)^{1-\varepsilon} \,.$$

Applications to Theoretical Computer Science (explicit constructions of 2–source extractors).

Sums with multiplicative characters

Theorem (Hanson, 2015)

Let $A, B, C \subseteq \mathbb{F}_p$, $\delta > 0$ and

$$|A|, |B|, |C| > \delta \sqrt{p}\,.$$

Then

$$\left| \sum_{a \in A,\, b \in B,\, c \in C} \chi(a+b+c) \right| = o_\delta(|A||B||C|)\,.$$

Improvements: Shkredov–Volostnov (2017). An analog with two sets instead of three is *Karatsuba's conjecture*.

Theorem (Shkredov–Shparlinski, 2016)

Let χ be a nontrivial multiplicative character. Then for any sets $A, B, C, D \subseteq \mathbb{F}_p$, $|A| > p^{\varepsilon}$ one has

$$\sum_{a\in A,\, b\in B,\, c\in C,\, d\in D} \chi(a+b+cd)\,, \quad \sum_{a\in A,\, b\in B,\, c\in C,\, d\in D} \chi(a+b(c+d))$$

$$\ll |A||B||C||D| \left(\frac{p}{|B||C||D|} \right)^{\varepsilon/16} .$$

Nontrivial if $|B||C||D| > p^{1+\varepsilon}$.

Applications: Dynamical systems

Let $a, b > 1$ be integers $\log a/\log b \notin \mathbb{Q}$ (exm. $a = 2$, $b = 3$).

Theorem (Furstenberg)

The sequence

$$\{2^n 3^m \alpha\}_{n,m \in \mathbb{N}}$$

is dense in $[0, 1]$, provided α is irrational.

How dense are sets

$$\{a^n b^m \alpha \ : \ n, m \le N\}, \qquad \text{and}$$

$$\{a^n b^m s \ : \ n, m \le M, s \in S\}, \qquad S \subseteq \mathbb{Z}/N\mathbb{Z}.$$

If the subgroup $\langle a, b \rangle$ in $\mathbb{Z}/N\mathbb{Z}$ has size N^{ε} and S is a, b invariant then just S itself has no gaps of size N^{-c}.

Theorem (Bourgain, Lindenstrauss, Michel, Venkatesh, 2009)

Let $\alpha \in \mathbb{R}/\mathbb{Z}$ such that for some k one has $\left|\alpha - \frac{p}{q}\right| \ge \frac{1}{q^k}$, $\quad q \ge 2$. Then the set

$$\{a^n b^m \alpha \; : \; n, m \le N\}$$

is $(\log\log N)^{-\kappa\varepsilon/100}$–dense in $\mathbb{R}/\mathbb{Z}$ with $\kappa = \kappa(a, b, k)$.

Theorem (Bourgain, Lindenstrauss, Michel, Venkatesh, 2009)

Let $S \subseteq \mathbb{Z}/N\mathbb{Z}$, $|S| > N^{\varepsilon}$. Then the set

$$\{k \cdot s \; : \; k = a^n b^m < N\,, s \in S\}$$

is $(\log N)^{-\kappa\varepsilon/100}$–dense.

Applications: structure of sumsets

General question

What can we say about the structure of sets S equal

$$A + A \quad \text{or} \quad A - A \quad \text{or} \quad A + B\ ?$$

Always $S = S + \{0\}$ or $S = (S + x) - \{x\}$,
so we consider $|A|, |B| > 1$.

It is natural to suppose that sumsets have rich additive structure.
But only a few things are known.

A hypothesis of Ostmann

Let $\mathcal{P}$ be the primes numbers and by $\mathcal{P}'$ denote a set that differs from $\mathcal{P}$ in only finitely many elements.

Conjecture (Ostmann, 1968 and Erdős, 1976)

Do there exist sets A, B with $|A|, |B| > 1$ such that

$$\mathcal{P}' = A + B?$$

Erdős : out of reach (because $\mathcal{P}'$ is too close to $\mathbb{N}$).
On the other hand, $\mathcal{P}'$ enjoes the "subgroup" property: $\forall k$

$$|(\mathcal{P}')^k \cap \{1, \ldots, N\}| = o_k(N) \,.$$

Theorem (Elsholtz, 2001)

For any A, B, C with $|A|, |B|, |C| > 1$ the following holds

$$\mathcal{P}' \neq A + B + C$$

and moreover

$$\frac{x^{1/2}}{(\log x)^5} \ll A(x) \ll x^{1/2} (\log x)^4 \,.$$

Sieve methods + intersections of shifts of sumsets.

"Random" sumsets = sumsets of random sets.

Can a sumset be a multiplicative subgroup?

If we believe that sumsets have some *additive* structure then can we prove that any *multiplicatively* rich set, say, a multiplicative subgroup (or the primes), is not a sumset?

Answer: not yet, this is complicated.

Conjecture (Sárközy, 2012)

Let $\mathcal{R} \subset \mathbb{F}_p$ be the set of all quadratic residues. Is it true that

$$\mathcal{R} \neq A + B \qquad \forall A, B, \quad |A|, |B| > 1?$$

Shkredov (2014) : yes, for $A = B$.

Theorem (Shkredov, 2014)

Let $\mathcal{R} \subset \mathbb{F}_p$ be the set of all quadratic residues. Then

$$\mathcal{R} = A + A \ \Rightarrow \ p = 3, A = \{2\},$$

and

$$\mathcal{R} = A \dot{+} A := \{a_1 + a_2 \ : \ a_1, a_2 \in A, a_1 \neq a_2\} \ \Rightarrow$$

$$\Rightarrow p = 3, 7, 13, \quad \exists \text{ four sets } A.$$

Some results when $|\mathcal{R} \triangle (A + A)|$ is small.

General multiplicative subgroups

Theorem (Shparlinski, 2013)

Let $\Gamma \subseteq \mathbb{F}_p$ be a multiplicative subgroup and for some $A, B \subseteq \mathbb{F}_p$ one has

$$A + B \subseteq \Gamma\,,$$

where $|A|, |B| \gg 1$. Then

$$|A|,\, |B| \le |\Gamma|^{1/2+o(1)}$$

as $|\Gamma| \to \infty$. In particular, if $A + B = \Gamma$ then

$$|A|,\, |B| = |\Gamma|^{1/2+o(1)}\,.$$

Sárközy: $\Gamma = \mathcal{R}$.

Theorem (Shkredov, 2016)

Let Γ be a subgroup, $|\Gamma| < p^{6/7-\varepsilon}$. Then

$$\Gamma \neq A - A\,,$$

where A is an arbitrary set.

Theorem (Shkredov, 2017)

Let Γ be a subgroup, $|\Gamma| < p^{2/3-\varepsilon}$. Then

$$\Gamma \neq A + B\,,$$

where $|A|, |B| > 1$ are arbitrary sets.

The necessary condition: real case

Put $D = A - A$.

Theorem (Roche–Newton—Zhelezov, 2015)

Let $A \subset \mathbb{R}$ be a finite set, and $\varepsilon > 0$ be a real number. Then for some constant $C'(\varepsilon) > 0$ one has

$$|DD|, |D/D| \gg_\varepsilon |D| \cdot \exp(C'(\varepsilon) \log^{1/3-o(1)} |D|) .$$

Actually, they proved

$$\mathrm{E}^\times(D) \ll |A|^6 \exp(-C'(\varepsilon) \log^{1/3-o(1)} |A|) ,$$

where $\mathrm{E}^\times(D)$ is the *multiplicative energy* of a set D, namely,

$$\mathrm{E}^\times(D) := |\{(d_1, d_2, d_3, d_4) \in D^4 \ : \ d_1 d_2 = d_3 d_4\}| .$$

Theorem (Shkredov, 2016)

Let $A \subset \mathbb{R}$ be a finite set. Put $D = A - A$. Then

$$|DD| \gg |D|^{1+\frac{1}{12}} \log^{-\frac{1}{4}} |D| \,.$$

and

$$|D/D| \gg |D|^{1+\frac{1}{8}} \log^{-\frac{5}{8}} |D| \,.$$

Thus, say, $\{1, 2, 2^2, 2^3, \ldots, 2^n\}$ is not a difference set.

Similar holds in $\mathbb{F}_p$.

Theorem (Murphy–Petridis–Roche-Newton–Rudnev–Shkredov, 2017)

Let $A \subset \mathbb{F}_p$ be a set. Put $D = A - A$, $|A| < p^{125/384}$. Then

$$|DD|,\, |D/D| \gg |D|^{1+c}\,,$$

where $c < \frac{1}{250}$ is an arbitrary.

Again, the product set and the quotient set of D are large.

Corollary

Let Γ be a subgroup, $|\Gamma| < p^{6/7-\varepsilon}$. Then

$$\Gamma \neq A - A\,,$$

where A is an arbitrary set.

Decomposition of sets with small product set in $\mathbb{R}$

Theorem (Shkredov–Zhelezov, 2016)

There is an $\epsilon > 0$ s.t. for all sufficiently large $A \subset \mathbb{R}$ with

$$|AA| \le |A|^{1+\epsilon}$$

one has

$$A \neq B + C \,, \qquad |B|, |C| > 1 \,.$$

Corollary (Shkredov–Zhelezov, 2016)

There is an absolute constant $c > 0$ s.t. for any real sets B, C with $|B|, |C| > 1$

$$|(B+C)(B+C)| \gg |B+C|^{1+c} \,.$$

Corollary (Shkredov–Zhelezov, 2016)

For any real set A one has

$$\mathrm{E}^{\times}(A \pm A) \ll |A|^{6-c},$$

where $c > 0$ is an absolute constant.

It improves the result of Roche–Newton and Zhelezov:

$$\mathrm{E}^{\times}(A \pm A) \ll |A|^{6} \exp(-\log^{1/3-o(1)} |A|).$$

Theorem (Murphy–Petridis–Roche-Newton–Rudnev–Shkredov, 2017)

Let $A \subset \mathbb{F}_p$ be a set. Then the number of collinear tuples is

$$Q[A] = \frac{|A|^8}{p^2} + O(|A|^5 \log |A|) \,.$$

Theorem (Shkredov, 2013)

Let $\varepsilon > 0$ be a positive real and $\Gamma \subseteq \mathbb{F}_p$ be a multiplicative subgroup, $|\Gamma| \le p^{2/3-\varepsilon}$. Then for some $\delta(\varepsilon) > 0$ one has

$$\mathrm{E}^{+}(\Gamma) \ll |\Gamma|^{5/2-\delta(\varepsilon)} \,.$$

We combine these two results and further sum–product observations.

Multiplicative decompositions

Let $\mathcal{S}$ be a set and $0 \in \mathcal{S}$. Then $\mathcal{S} = \{0, 1\}\mathcal{S}$. On the other hand, if $\mathcal{S} \setminus \{0\} = AB$, then $\mathcal{S} \cup \{0\} = (A \cup \{0\})B$. So, we delete zero from $\mathcal{S}$.

What can we say about multiplicative decomposition of an interval?

This question was posed by Shparlinski.

If $\mathcal{S} = -\mathcal{S}$, then $\mathcal{S} = \{-1, 1\}\mathcal{S}$. Finally, if $p \geq 5$, then

$$\{3^*-1, 3^*, 3^*+1\} \pmod p = \{-1, 2\} \cdot \{-3^*, 1-3^*\} \pmod p\,.$$

Theorem (Garaev–Konyagin, 2013)

There exists an absolute $c > 0$ such that if an interval $\mathcal{I} \subset \mathbb{F}_p^*$, $|\mathcal{I}| < cp$ is $\mathcal{I} = AB$, then either

$$\mathcal{I} = \pm\{3^* - 1, 3^*, 3^* + 1\}$$

or $\mathcal{I} = -\mathcal{I}$.
In the latter case any nontrivial decomposition $\mathcal{I} = AB$ implies that one of the sets A or B coincides with $\{-r, r\}$, $r \in \mathbb{F}_p$.

The constant c cannot be taken greater than $1/2$.

Theorem (Shkredov, 2017)

Let Γ be a subgroup, $|\Gamma| < p^{6/7-\varepsilon}$ and $\xi \neq 0$. Then

$$\xi\Gamma + 1 \neq A/A\,.$$

where A is an arbitrary set.

Theorem (Shkredov, 2017)

1) $\exists \varepsilon > 0$ s.t. for all sufficiently large $A \subset \mathbb{R}$ with $|AA| \le |A|^{1+\varepsilon}$ there is no decomposition $A + 1 = B/B$ with $|B \setminus \{0\}| > 1$.
2) In a similar way, let $B \subset \mathbb{R}$ be a set such that $|B \setminus \{0\}| > 1$. Then the following holds

$$|(B/B - 1)(B/B - 1)| \gg |B/B|^{1+c}\,.$$

Problems

Problem 1. It is known that for $D = A - A$ one has

$$|D|^{3/2} \gg |D/D| \gg |D|^{1+c},$$

where $c = 1/8 - o(1)$. What is the right exponent?

Problem 2. Recall

$$R[A] = \left\{ \frac{a_1 - a}{a_2 - a} \ : \ a, a_1, a_2 \in A,\ a_2 \neq a \right\} \subseteq D/D\,.$$

Is it true $|R[A]| \gg |A - A|$, $|R[A]| \gg |A/A|$?

Problem 3. $S \subset \mathbb{F}_p$, $|S| \le p/2$ is a *perfect difference set* iff the number of solutions of the equation $x = s_1 - s_2$, $s_1, s_2 \in S$, $x \neq 0$ does not depend on x.

Is it true that $S \neq A - A$ for any set A?

Problem 4. We know that for $D = A - A$ one has

$$|DD|, \;\; |D/D| \gg |D|^{1+c} .$$

Is it true that for any $n \in \mathbb{N}$ there is $m \in \mathbb{N}$ such that for some $a, b \in \mathbb{N}$, $a + b \le m$ the following holds

$$|D^m|, \;\; |D^a D^{-b}| \ge |D|^n \quad ?$$

The square root barrier

Problem 6. Is it true that for any $A \subseteq \mathbb{F}_p$, $|A| > p^{1/2-\varepsilon}$ one has

$$(A - A)^n = \mathbb{F}_p \,,$$

where $n = n(\varepsilon)$?

Problem 7. Let $\Gamma \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup, $|\Gamma| > p^{\varepsilon}$. Is it true that for some $n = n(\varepsilon)$ one has

$$(\Gamma - \Gamma)^n = \mathbb{F}_p \,.$$

Gaps in quadratic residues and so on.

Thank you for your attention!