ON ADDITIVE SHIFTS OF MULTIPLICATIVE
ALMOST-SUBGROUPS IN FINITE FIELDS

DMITRII ZHELEZOV

Abstract. We prove that for sets $A, B, C \subset \mathbb{F}_p$ with $|A| = |B| = |C| \leq \sqrt{p}$ and a fixed $0 \neq d \in \mathbb{F}_p$ holds
$$\max(|AB|, |(A + d)C|) \gg |A|^{1+1/26}.$$ 
In particular,
$$|A(A + 1)| \gg |A|^{1+1/26}$$
and
$$\max(|AA|, |(A + 1)(A + 1)|) \gg |A|^{1+1/26}.$$ 
The first estimate improves the bound by Roche-Newton and Jones.

In the general case of a field of order $q = p^m$ we obtain similar estimates with the exponent $1 + 1/559 + o(1)$ under the condition that $AB$ does not have large intersection with any subfield coset, answering a question of Shparlinski.

Finally, we prove the estimate
$$\left| \sum_{x \in \mathbb{F}_q} \psi(x^n) \right| \ll q^{-2\delta_2} n^{2+2\delta_2}$$
for Gauss sums over $\mathbb{F}_q$, where $\psi$ is a non-trivial additive character and $\delta_2 = 1/56 + o(1)$. The estimate gives an improvement over the classical Weil bound when $q^{1/2} < n = o\left(q^{29/57+o(1)}\right)$.

1. Introduction

One of the main open problems in additive combinatorics is the so-called sum-product phenomenon, which broadly speaking asserts that a set cannot be structured both additively and multiplicatively. There are numerous results quantifying this claim, though we mention just the following results which are of the most relevance to the present note. We will use the standard Vinogradov notation $X \ll Y$ and $X \gg Y$ when there is an absolute constant $C$, independent of $X$ and $Y$, such that $|X| \leq C|Y|$ and $|X| \geq C|Y|$, respectively. Little-oh notation $o(1)$ appears only in exponents and should be regarded as implicit logarithmic factors.

Date: July 21, 2015.

2000 Mathematics Subject Classification. 11B25 (primary).

Key words and phrases. product sets.

Department of Mathematical Sciences, Chalmers University Of Technology and University of Gothenburg.
Recall that the multiplicative energy $E^\times(A, B)$ is defined as the number of solutions to
\[ ab = a'b', \quad a, a' \in A, \quad b, b' \in B. \]
If $A = B$ the second argument is usually omitted and the same definition extends to the additive energy $E^+$ in the obvious way. We will usually omit the upper index as only additive energies will appear after (1). We refer the reader to [17] for details.

Shkredov in [14] recently proved that if $\Gamma$ is a multiplicative subgroup of $\mathbb{F}_p$ of order $< \sqrt{p}$, then for an arbitrary non-zero residue $x$
\[ E^\times(\Gamma + x) \ll |\Gamma|^2 \log |\Gamma|. \] (1)
In particular, by Cauchy-Schwartz,
\[ |(\Gamma + x)(\Gamma + x)| \gg \frac{|\Gamma|^2}{\log |\Gamma|}. \]

Garaev and Shen [4] proved that for a set $A \subset \mathbb{F}_p$ with $|A| \leq \sqrt{p}$
\[ |A(A + 1)| \gg |A|^{1+\delta} \]
with $\delta = 1/105 + o(1)$. Roche-Newton and Jones [6] later improved the bound to $\delta = 1/56$. Using an energy estimate from [10] based on a recent incidence result in finite fields by Rudnev [11], we report some progress in a slightly more general setting. Namely we prove the following theorem.

**Theorem 1.** Let $A, B, C \subset \mathbb{F}_p$ with $|A| = |B| = |C| \leq \sqrt{p}$. Then for any fixed $0 \neq d \in \mathbb{F}_p$ holds
\[ \max(|AB|, |(A + d)C|) \gg |A|^{1+1/26}. \]
In particular,
\[ |A(A + 1)| \gg |A|^{1+1/26} \]
and
\[ \max(|AA|, |(A + 1)(A + 1)|) \gg |A|^{1+1/26}. \]

One might think of the theorem above as a generalisation of the aforementioned result of Shkredov to the case of almost-subgroups.

In Section 3 we obtain a similar, though worse, bound for the case of a general finite field $\mathbb{F}_q$, $q = p^m$ thus answering a question of I. Shparlinski.

**Theorem 2.** Let $A, B, C \subset \mathbb{F}_q$. Suppose that for any proper subfield $F$ and any $c \in \mathbb{F}_q$ holds $|AB \cap cF| \leq |F|^{1/2}$. Then for any fixed $0 \neq d \in \mathbb{F}_q$ holds
\[ \max(|AB|, |(A + d)C|) \geq |A|^{1+1/559+o(1)}. \]

The proof of Theorem 2 is based on a reduction to the sum-product estimate which was proved by Li and Roche-Newton [9] for general finite fields. In this setting one should obviously require that the set in question does not have large intersection with a subfield coset. The precise statement is as follows.
Theorem 3 (Li-Roche-Newton). Let $q = p^n$ and let $A$ be a subset of $\mathbb{F}_q^*$. If $|A \cap cF| \leq |F|^{1/2}$ for any proper subfield $F$ of $\mathbb{F}_q$ and any element $c \in \mathbb{F}_q$, then
\[
\max\{|A + A|, |AA|\} \gg \frac{|A|^{12/11}}{\log^{5/11} |A|}
\]

The exponent in Theorem 2 is sufficiently worse than in the case of $\mathbb{F}_p$ mainly because of the wasteful use of the Balog-Szemerédi-Gowers theorem, so it would be interesting to find a proof which avoids it.

Theorems 1 and 2 can be used in order to estimate the number of solutions to $g - h = d$, $g \in G, h \in H$ for a fixed $d \neq 0$ and $G, H$ multiplicative subgroups. Indeed, let $A$ be the set of all $g \in G$ such that $g - h = d$ for some $h \in H$. Then $|AA| \leq |G|$ and $|(A - d)(A - d)| \leq |H|$. Applying Theorem 1 we obtain the following corollary.

Corollary 1. Let $G, H$ be multiplicative subgroups of $\mathbb{F}_p$ with $|G|, |H| \leq \sqrt{p}$ and $0 \neq d \in \mathbb{F}_p$ be fixed. Then the number of solutions to $g - h = d$, $g \in G, h \in H$ is bounded by
\[
\max\{|G|, |H|\}^{26/27}.
\]

The case of a general field $\mathbb{F}_q$ renders as follows.

Corollary 2. Let $G, H$ be multiplicative subgroups of $\mathbb{F}_q$ and $0 \neq d \in \mathbb{F}_p$ be fixed. Assume that for any proper subfield $F$ and $c \in \mathbb{F}_q$ holds $|G \cap cF| \leq |F|^{1/2}$. Then the number of solutions to $g - h = d$, $g \in G, h \in H$ is bounded by
\[
\max\{|G|, |H|\}^{559/560 + o(1)}.
\]

In Section 4 we prove a sum-product-type estimate for Gauss sums, providing explicit power-saving exponents for the bound of Bourgain and Chang, [1].

Theorem 4. Let $q = p^n$ and $n | q - 1$. Assume also that for any $m \neq \nu | m$ uniformly holds
\[
\gcd\left(n, \frac{p^m - 1}{p^n - 1}\right) \ll n^{\delta} q^{1-\delta} p^{\nu}
\]
with $\delta = 119/605$. Then
\[
\left| \sum_{x \in \mathbb{F}_q} \psi(x^n) \right| \ll q^{\frac{7-2\delta_2}{8}} n^{\frac{2+2\delta_2}{8}}
\]
for any non-trivial additive character $\psi$ and $\delta_2 = 1/56 + o(1)$. 

2. Proof of Theorem \[1\]

Let $K, L$ be such that $|AB| = K|A|$ and $|(A + d)C| = L|A|$. We will show that then in fact either $K$ or $L$ are $\gg |A|^{1/26}$.

Let $a_1, a_2, a_3 \in A$, $c \in C$ and $b \in B$. Denote
\[
y_1 = (a_1 + d)c \\
y_2 = (a_2 + d)c \\
y_3 = (a_3 + d)c,
\]
so $y_i \in (A + d)C$. Our starting point is the following identity, motivated by the incidence result of Helfgott and Rudnev \[5\] and the result of Garaev and Shen \[4\].
\[
a_1b - \frac{y_3 - y_1}{y_3 - y_2}a_2b = a_3b - \frac{y_1 - y_2}{y_3 - y_2}.
\]

Here we require that the $y_i$ are pairwise distinct. Note that if we fix $y_1, y_2, y_3$ then still $b$ can be chosen arbitrarily. Also, if two quadruples $(a_1, a_2, a_3, c)$ and $(a_1', a_2', a_3', c')$ both satisfy (3) with the same $y_i$, we have
\[
\frac{y_1}{y_2} = \frac{a_1 + d}{a_2 + d} = \frac{a_1' + d}{a_2' + d},
\]
which guarantees that $(a_1b, a_2b) \neq (a_1'b', a_2'b')$ since $d \neq 0$ and $y_1 \neq y_2$. And of course $(a_1b, a_2b) \neq (a_1'b', a_2'b')$ if $b \neq b'$.

Now we will need some notation in order to estimate the number of triples $(y_1, y_2, y_3)$. Let us reassign $A' = A + d$ and let $A'(), C()$ be the corresponding indicator functions of $A'$ and $C$. Write\[1\]
\[
C_4(y_1, y_2, y_3) = \sum_{c \in C} A'(y_1c^{-1})A'(y_2c^{-1})A'(y_3c^{-1}).
\]

Clearly $C_4$ is supported on $A'C \times A'C \times A'C$.

By the preceding discussion, if the $y_i$’s are pairwise distinct, there are at least $|A|C_4(y_1, y_2, y_3)$ pairs $(p_1, p_2) \in AB \times AB$ such that
\[
p_1 - \frac{y_3 - y_1}{y_3 - y_2}p_2 \in \frac{y_1 - y_2}{y_3 - y_2}AB.
\]

Denoting $\alpha = \frac{y_1 - y_2}{y_3 - y_2}$ and applying the Cauchy-Schwartz inequality, we have
\[
E(AB, \alpha AB) \geq K^{-1}|A|C_4^2(y_1, y_2, y_3). \tag{5}
\]
or
\[
E(AB, \alpha AB)^{1/2} \geq K^{-1/2}|A|^{1/2}C_4(y_1, y_2, y_3). \tag{6}
\]

By Corollary 2.10 in \[17\]
\[
E(AB, \alpha AB) \leq E(AB, AB)^{1/2}E(\alpha AB, \alpha AB)^{1/2} = E(AB, AB),
\]
\[\text{Such functions were studied in \[16\] with numerous applications.}\]
so for we can rewrite \( E(AB, AB) \) and then sum over all pairwise distinct triples \((y_1, y_2, y_3) \in A' C \times A' C \times A' C\). The number of such triples is \( \gg |A'|^3 = L^3 |A|^3 \), so

\[
L^3 |A|^3 E(AB, AB)^{1/2} \gg K^{-1/2} |A|^{1/2} \sum_{(y_1, y_2, y_3) \text{ distinct}} C_4(y_1, y_2, y_3). \tag{7}
\]

It is easy to see that

\[
\sum_{(y_1, y_2, y_3) \in A' C \times A' C \times A' C} C_4(y_1, y_2, y_3) = |C||A|^3 = |A|^4,
\]

and the contribution from the triples with \( y_i = y_j \) is at most \( 3 |C||A|^2 \leq \frac{1}{2} |A|^4 \). Thus, (7) gives

\[
L^3 |A|^3 E(AB, AB)^{1/2} \gg K^{-1/2} |A|^{9/2},
\]

and

\[
E(AB, AB) \gg L^{-6} K^{-1} |A|^3 \tag{8}
\]

Now we apply a powerful energy estimate from [10].

**Theorem 5** (Roche-Newton-Rudnev-Shkredov). Let \( X, Y, Z \subset \mathbb{F}_p \), let \( M = \max(|X|, |YZ|) \). Suppose that \( |X||Y||YZ| \ll p^2 \). Then

\[
E(X, Z) \ll (|X||YZ|)^{3/2}|Y|^{-1/2} + M|X||YZ||Y|^{-1}.
\]

Before using this theorem, recall the following form of the Plünnecke-Ruzsa inequality due to Ruzsa, see [12].

**Lemma 1.** Let \( Y, X_1, \ldots, X_k \) be additive subsets of an abelian group. Then

\[
|X_1 + \ldots + X_k| \leq \prod_{i=1}^k |Y + X_i|/|Y|^{k-1}.
\]

The following corollary is due to Katz and Shen, [7].

**Lemma 2.** Let \( Y, X_1, \ldots, X_k \) be additive subsets of an abelian group. Then there exists \( Y' \subset Y \) with \( |Y'| \geq \frac{1}{2} |Y| \) such that

\[
|Y' + X_1 + \ldots + X_k| \ll_k \prod_{i=1}^k |Y + X_i|/|Y|^{k-1}.
\]

We begin with estimating \( |AA| \) by Lemma 1. We have We have

\[
|AA| \leq \frac{|AB||AB|}{|B|} = K^2 |A|.
\]

The next step is to apply multiplicatively Lemma 2 to find \( Y' \subset A \), \( |Y'| \gg |A| \) such that

\[
|Y' AB| \ll \frac{|AA||AB|}{|A|} \leq K^3 |A|.
\]
Now everything is ready to apply Theorem 5 with $X = Z = AB$ and $Y = Y'$. The hypothesis is satisfied since $|A| \leq \sqrt{p}$ implies $|X||Y||YZ| \ll K^4|A|^3 \ll p^2$ unless $K \gg p^{1/8} \gg |A|^{1/4}$ which is better than the estimate we are aiming at.

We then have

$$E(AB, AB) \ll K^6|A|^{5/2} + K^7|A|^2 \ll K^6|A|^{5/2}$$

provided $K \ll \sqrt{|A|}$ which we can safely assume.

Combining with (8) we get

$$K^{14}L^{12} \gg |A|$$

so

$$\max\{K, L\} \gg |A|^{1/26}.$$ 

thus proving Theorem 1.

We now record two quick corollaries of our result as claimed in Theorem 1.

**Corollary 3.** For a subset $A$ of $\mathbb{F}_p$ with $|A| \ll p^{1/2}$ holds

$$|A(A + 1)| \geq |A|^{1+1/26}. $$

**Proof.** Put $B = A + 1$, $C = A$ and $d = 1$. \qed

**Corollary 4.** For a subset $A$ of $\mathbb{F}_p$ with $|A| \ll p^{1/2}$ holds

$$\max(|AA|, |(A + 1)(A + 1)|) \geq |A|^{1+1/26}$$

**Proof.** Put $B = A$, $C = A + 1$ and $d = 1$. \qed

### 3. Finite fields not of prime order

In the case of a field not of prime order the energy estimate (8) still holds since the congruence (4) holds in any field. However, we can no longer use the upper bound of Theorem 5 so we will use the Balog-Szemerédi-Gowers theorem (abbreviates BSG henceforth) instead with the bounds due to Schoen, [15] (see also [17] and [3]).

**Theorem 6** (Balog-Szemerédi-Gowers). If $A$ is a finite subset of an abelian group with the additive energy equal to $\kappa|A|^3$ then there exists $A' \subset A$ with $|A'| \gg \kappa|A|$ such that

$$|A' + A'| \ll \kappa^{-5}|A'|.$$

If we apply the above theorem to (8), we obtain a set $X \subset AB$ with $|X| \gg K^{-4}L^{-6}|AB| = K^{-3}L^{-6}|A|$ such that

$$|X + X| \ll L^{30}K^{20}|X|.$$ 

On the other hand, by the Plünnecke-Ruzsa inequality,

$$|XX| \leq |AABB| \leq \frac{|AA||AA||AB||AB|}{|A|^3} \leq K^6|A| \leq L^6K^9|X|.$$
It is now easy to see that if both $K$ and $L$ are small, then $X$ violates the sum-product inequality of Theorem 3. We then conclude that if $AB$ has small intersection (i.e. less than $|G|^{1/2}$) with any subfield coset $cG$ then
\[
LK = \max\left\{LK, L^6K^5\right\} \gg |X|^{1/11+o(1)} \gg K^{-3/11}L^{-6/11}|A|^{1/11+o(1)},
\]
which implies
\[
\max\{L, K\} \gg |A|^{1/559+o(1)}.
\]

4. Gauss sums

Our proof will be based on the estimate for the number for solutions to
\[
g_1 + g_2 = a
\]
for a fixed $a \in \mathbb{F}_q^*$ and where $g_1, g_2$ are elements of a multiplicative subgroup $G$. One can readily use Corollary 2 but it turns out that a direct application of the Balog-Szemerédi-Gowers with a sum-product estimate gives a better bound.

The central lemma is as follows.

**Lemma 3.** Let $G \subset \mathbb{F}_q$ be a multiplicative subgroup and $\delta_1 = 486/605$. Assume that for any proper subfield $F$ holds
\[
|G \cap F| \ll |G|^\delta_1.
\]
Then
\[
E(G) \ll |G|^{3-\delta_2},
\]
with $\delta_2 = 1/56 + o(1)$.

**Proof.** Let $E(G) = |G|^{3-\delta'}$ and assume $\delta' < \delta_2 = 1/56 + o(1)$ for contradiction. Let $A$ be the set given by the BSG theorem applied additively to $G$, so $|A| \gg |G|^{1-\delta'}$ and
\[
|A + A| \ll |A|^{1+5\delta'/1-\delta'}.
\]
The product set $AA$ is clearly contained in $G$, so $|AA| \ll |A|^{1/(1-\delta')}$. It remains to check the necessary conditions and apply the sum-product estimate. In fact, we will use a different condition than the hypothesis of Theorem 3. Namely, one can rule out the case of $A$ having large intersection with a subfield coset (Case 4 in the proof of Theorem 5 in [9]) if for any proper subfield coset $cF$ holds
\[
|cF \cap A| \ll |A|^{1-2/11+o(1)}.
\]
Since $|cF \cap A| \leq |F \cap G| \leq |G|^{\delta_1} \leq |A|^{\delta_1/(1-\delta')}$, the condition (10) holds if $\delta' < \delta_2$. Thus, we can apply the sum-product estimate of Theorem 3 which gives
\[
\max\{ |A|^{1+5\delta'/1-\delta'}, |A|^{1/(1-\delta')} \} \gg |A|^{1+1/11+o(1)},
\]

More concretely, using the notation of the original paper, one should use (7) of [9] together with the trivial $|\mathbb{F}_{\tilde{A}_{x_0}} \cap A| \geq \tilde{A}_{x_0}$.
so \(1 + 5\delta^\prime/(1 - \delta^\prime) = \max\{1 + 5\delta^\prime/(1 - \delta^\prime), 1/(1 - \delta^\prime)\} \geq 1 + 1/11 + o(1)\), contradicting the original assumption \(\delta^\prime < \delta_2 = 1/56 + o(1)\).

\[\Box\]

**Remark 1.** In the above lemma one can take \(\delta_1\) arbitrarily close to 1 at the expense of worsening \(\delta_2\).

A Gauss sum is a sum of the form

\[S_n(a) = \sum_{x \in \mathbb{F}_q} \psi_a(x^n),\]

where \(\psi_a := e_p(\text{Tr}(ax))\) with the standard definitions \(e_p(x) := \exp(\frac{2\pi ix}{p})\) and \(\text{Tr}(x) = x + x^p + \ldots + x^{p^{m-1}}\). If \(a \neq 0\) the character \(\psi_a\) is non-trivial and we will assume that henceforth.

The classical Weil bound gives the estimate

\[|S_n(a)| \leq (n - 1)q^{1/2},\]

which becomes trivial if \(n \gg q^{1/2}\), so it is interesting to extend the range of \(n\) where a non-trivial bound holds. The first result of this kind for fields not of prime order was obtained by Shparlinski [13] with the values of \(n\) up to \(p^{1/6}q^{1/2}\). It was later extended by Bourgain and Chang [1], who proved

\[|S_n(a)| \ll q^{1-\delta},\]

with some unspecified \(\delta\) depending only on a fixed parameter \(\epsilon\) which controls the interaction with subfields (in particular, \(n \leq q^{1-\epsilon}\)), similarly to the condition (2) of Theorem 4. We invite the interested reader to consult [1] and [2] for further details. Here our goal is to give an explicit power-saving exponent for \(n \gg q^{1/2}\).

We will use the following adaptation of an estimate appeared in [8] (Lemma 3 with \(m = l = 2\)).

**Lemma 4.** Let \(G\) be a multiplicative subgroup of \(\mathbb{F}_q^*\). Then

\[|S(a, G)| := \left| \sum_{g \in G} \psi_a(g) \right| \leq q^{1/8} E(G)^{1/4}.\]

Let \(G\) be the group of \(n\)th powers, which is of order \((q - 1)/n\). Combining Lemma 3 with (11) one gets

\[|S_n(a)| \ll n|S(a, G)| \ll q^{7-2\delta_2} n^{2+2\delta_2},\]

provided the subfield intersection hypothesis of Lemma 3 is satisfied. The bound (12) is non-trivial if \(n = o(q^{(1+2\delta_2)/(2+2\delta_2)}) = o(q^{29/57+o(1)})\).

Thus, it remains to check that the condition (2) of Theorem 4 implies (9). Let \(F\) be a proper subfield of order \(p^r\). By considering a generator of \(\mathbb{F}_q^*\) we can easily
calculate

$$|G \cap F| = \frac{\gcd(n, \frac{q - 1}{p - 1})(p^\nu - 1)}{n} \ll \gcd(n, \frac{q - 1}{p - 1})p^\nu |G|.$$ 

Thus, if (2) holds with $\delta = 119/605$ then for any proper subfield $F$

$$|G \cap F| \leq |G|^\delta_1$$

with $\delta_1 = 1 - \delta = 486/605$.

**Remark 2.** Like Lemma 3, it is possible to prove Theorem 4 with $\delta$ arbitrarily close to zero at the expense of worsening $\delta_2$.

5. **Acknowledgements**

The author is indebted to Igor Shparlinski for essentially showing how Lemma 3 applies to Gauss sums. The author would like to thank Alisa Sedunova for bringing the problem (originally due to Igor Shparlinski) to the author’s attention. The author is also grateful to Ilya Shkredov, Oliver Roche-Newton and Peter Hegarty for feedback and careful proofreading.

**References**

[1] J. Bourgain and M.-C. Chang, A Gauss sum estimate in arbitrary finite fields, C. R. Acad. Sci. Paris, Ser. I 342 (2006) 643–646.
[2] J. Bourgain and M.-C. Chang, Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_q$, where $Q$ is composite with few prime factors. Geom. Funct. Anal. 16 (2006), no. 2, 327–366.
[3] J. Fox and B. Sudakov, Dependent Random Choice, arXiv:math/0909.3271 (2009), 31pp.
[4] M. Garaev, C.-Y. Shen, On the size of the set $A(A + 1)$, Math. Z. 265 (2010), 125–132.
[5] H. Helfgott and M. Rudnev, An explicit incidence theorem in $\mathbb{F}_p$, Mathematika 57 (2011), no. 11, 35–145.
[6] T. Jones and O. Roche-Newton, Improved bounds on the set $A(A + 1)$, J. Combin. Theory Ser. A 120 (2013), no. 3, 515–526.
[7] N. H. Katz and C.-Y. Shen, A slight improvement of Garaev’s sum-product estimate, Proc. Amer. Math. Soc. 136(7), 2499–2504.
[8] S. V. Konyagin, Estimates of trigonometric sums over subgroups and of Gauss sums, Proceedings of the 4th International Conference ”Current problems of number theory and its applications”, Tula 2001, Moscow State University Publishing House, Moscow, 2002, 86–114 (in Russian).
[9] L. Li and O. Roche-Newton, An improved sum-product estimate for general finite fields, SIAM J. Discrete Math. 25 (2011), no. 3, 1285–1296.
[10] O. Roche-Newton, M. Rudnev and I. D. Shkredov, New sum-product type estimates over finite fields, arXiv:1408.0542.
[11] M. Rudnev, On the number of incidences between planes and points in three dimensions, arXiv:1407.0426.
[12] M. Ruzsa, An application of graph theory to additive number theory, Scientia, Ser. A 3 (1989), 97–109.
[13] I. Shparlinski, Bounds of Gauss sums in finite fields, Proc. Amer. Math. Soc. 132 (2004), no. 10, 2817–2824.
[14] I. D. Shkredov, On tripling constant of multiplicative subgroups, arXiv:1504.04522.
[15] T. Schoen, New bounds in Balog-Szemerédi-Gowers theorem, Combinatorica, DOI: 10.1007/s00493-014-3077-4, (2014), 1–7
[16] T. Schoen and I. D. Shkredov, Higher moments of convolutions, J. Number Theory 133 (2013), no. 5, 1693–1737.
[17] T. Tao and V. Vu, Additive combinatorics, Cambridge Studies in Mathematics, Cambridge Univ. Press, 2006.

Department of Mathematical Sciences, Chalmers University Of Technology and University of Gothenburg, 41296 Gothenburg, Sweden
E-mail address: zhelezov@chalmers.se