ISSN 2220-5438

Moscow Journal of Combinatorics and Number Theory

МФТИ

URSS

Volume 1 • Issue 3 2011

Moscow Journal of Combinatorics and Number Theory. 2011. Vol. 1. Iss. 3. 80 p.

The journal was founded in 2010.

Published by the Moscow Institute of Physics and Technology with the support of Yandex and Microsoft.

The aim of this journal is to publish original, high-quality research articles from a broad range of interests within combinatorics, number theory and allied areas. One volume of four issues is published annually.

Website of our journal
http://mjcnt.phystech.edu

E-mail
mjcnt@phystech.edu

Address of the Editorial Board

Moscow institute of physics
and technology (state university)
Faculty of Innovations
and High Technology,
Laboratorny Korpus, k. 209,
9, Institutskii pereulok,
Dolgoprudny,
Moscow Region,
Russia,
141700

Адрес редакции

Московский физико-технический
институт (государственный университет)
Факультет инноваций
и высоких технологий
Лабораторный корпус, к. 209,
Институтский переулок, д. 9,
г. Долгопрудный,
Московская область,
Российская Федерация,
141700

URSS Publishers

56, Nakhimovsky Prospekt,
Moscow,
Russia,
117335

Издательство «УРСС»

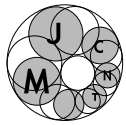
Нахимовский пр-т, 56
Москва,
Российская Федерация,
117335

Журнал зарегистрирован в Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия 3 сентября 2010 г. Свидетельство ПИ № ФС77-41900.

Формат 70×100/16. Печ. л. 5. Зак. № ПЖ-43.
Отпечатано в ООО «ЛЕНАНД».
117312, Москва, пр-т Шестидесятилетия Октября, 11А, стр. 11.

ISSN 2220-5438

Moscow Journal
of Combinatorics
and Number Theory
2011, vol. 1, iss. 3,
pp. 50–68, [pp. 258–276]



Average estimate for additive energy in prime field

Alexey Glibichuk (Haifa)

Abstract: Assume that $A \subseteq \mathbb{F}_p$, $B \subseteq \mathbb{F}_p^*$, $\frac{1}{4} \leqslant \frac{|B|}{|A|}$, $|A| = p^\alpha$, $|B| = p^\beta$. We will prove that for $p \geqslant p_0(\beta)$ one has

$$\sum_{b \in B} E_+(A, bA) \leqslant 15 p^{-(\min\{\beta, 1-\alpha\})/308} |A|^3 |B|.$$

Here $E_+(A, bA)$ is the additive energy of a subset A and its multiplicative shift bA. This improves previously known estimates of this type.

Keywords: finite fields, sum-product sets, exponential sums

AMS Subject classification: 11T23, 11B13

Received: 29.06.2011; **revised:** 02.08.2011

1. Introduction

Let X be a non-empty set endowed with a binary operation $* : X \times X \to X$. Then one can define the operation * on pairs of subsets $A, B \subset X$ by the formula $A*B = \{a*b : a \in A, b \in B\}$. In particular, if A and B are subsets of a ring, we have two such operations: addition $A + B := \{a + b : a \in A, b \in B\}$ and multiplication $AB = A \times B := \{ab : a \in A, b \in B\}$. For a given element b we define the operation $b * A = b \times A$. The sign $*$ may be omitted when there is no danger of confusion. We write $|A|$ for the cardinality of A. We just consider the field $\mathbb{F}_p$ of p elements, where p is an arbitrary prime. All sets are assumed to be subsets of $\mathbb{F}_p$. Given any set $Y \subset \mathbb{F}_p$, we write $Y^* := Y \setminus \{0\}$ for the set of invertible elements of Y.

Definition 1. *For subsets $A, B \subset \mathbb{F}_p$ we denote*

$$E_+(A,B) = \big|\big\{(a_1,a_2,b_1,b_2) \in A\times A\times B\times B : a_1 - a_2 = b_1 - b_2\big\}\big|,$$
$$E_\times(A,B) = \big|\big\{(a_1,a_2,b_1,b_2) \in A\times A\times B\times B : a_1a_2 = b_1b_2\big\}\big|.$$

Numbers $E_+(A,B)$ and $E_\times(A,B)$ are said to be the ***additive energy*** *and the* ***multiplicative energy*** *of sets A and B respectively.*

In the paper [5] J. Bourgain proved the following result.

Theorem 1. *Assume $A \subset \mathbb{F}_p$, $B \subset \mathbb{F}_p$ and $|A| = p^\alpha$, $|B| = p^\beta$ with $\alpha \geqslant \beta$. Then*

$$\sum_{b\in B} E_+(A,bA) < C_1 p^{c_2\gamma}|A|^3|B|$$

where $\gamma = \min(\beta, 1-\alpha)$ and C_1, c_2 are absolute constants (independent of α, β).

In the same paper J. Bourgain deduces from Theorem 1 a sum-product estimate for two different subsets. Later J. Bourgain and the author of this paper in [4] extended Theorem 1 to the case of an arbitrary finite field. More precisely, we proved the following result.

Theorem 2. *Take arbitrary subsets A, B of a finite field $\mathbb{F}_q$ with $q = p^r$ elements, such that $|A| = q^\alpha$, $|B| = q^\beta$, $\alpha \geqslant \beta$ and an arbitrary $0 < \eta \leqslant 1$. Suppose further that for every nontrivial subfield $S \subset \mathbb{F}_q$ and every element $d \in \mathbb{F}_q$ the set B satisfies the restriction*

$$|B \cap dS| \leqslant 4|B|^{1-\eta}.$$

Then

$$\sum_{b\in B} E_+(A,bA) \leqslant 13q^{-\gamma/10430}|A|^3|B| \quad \text{where} \quad \gamma = \min\left(\beta, \frac{5215}{4}\beta\eta,\ 1-\alpha\right).$$

In this paper we also deduced from Theorem 2 a new character sum estimate over a small multiplicative subgroup. J. Bourgain, S. J. Dilworth, K. Ford, S. Konyagin and D. Kutzarova [3] applied Theorem 2 to one of the problems of sparse signal recovery and several other settings in coding theory. Also M. Rudnev and H. Helfgott [9] used a method proposed in the proof of Theorem 1 to obtain a new explicit point-line incidence result in $\mathbb{F}_p$. These examples show that estimates like those from Theorems 1 and 2 have a wide range of applications.

In the current paper a slightly modified version of the method from paper [9] will be used to obtain an improvement of Theorem 2 in the case of prime field $\mathbb{F}_p$. We will establish the following theorem.

THEOREM 3. *Assume that* $A \subseteq \mathbb{F}_p$, $B \subseteq \mathbb{F}_p^*$, $1/4 \leqslant |B|/|A|$, $|A| = p^\alpha$, $|B| = p^\beta$. *Then for* $p \geqslant p_0(\beta)$ *we have*

$$\sum_{b\in B} E_+(A, bA) \leqslant 15p^{-(\min\{\beta,1-\alpha\})/308}|A|^3|B|.$$

Ideas of M. Rudnev and H. Helfgott in context of this problem work only when $|B| \geqslant K|A|$ for some absolute constant K. The case when $|A|$ is small comparatively to $|B|$ was analyzed by another method. This method is elementary and gives the following estimate.

THEOREM 4. *Assume that* $A \subseteq \mathbb{F}_p$, $B \subseteq \mathbb{F}_p^*$, $|A| = p^\alpha$, $|B| = p^\beta$. *Then for* $p \geqslant p_0(\alpha, \beta)$ *we have*

$$\sum_{b\in B} E_+(A, bA) \leqslant Cp^{-(\min\{\beta,1-\alpha\})/2240}|A|^3|B|,$$

where $C > 0$ *is an absolute constant.*

As we see, Theorem 4 gives a worse estimate than Theorem 3, but it is still better than the one delivered by Theorem 2.

In Section 2 we state preliminary results which will be used in proofs of Theorems 3 and 4. Theorem 3 is proved in Section 3, Theorem 4 is proved in Section 4.

2. Preliminary results

All the subsets in Lemmas below are assumed to be non-empty. The first two lemmas are due to Ruzsa [10, 11]. They are valid for subsets of any abelian group, but here we state them only for subsets of $\mathbb{F}_p$.

LEMMA 1. *For any subsets* X, Y, Z *of* $\mathbb{F}_p$ *we have*

$$|X - Z| \leqslant \frac{|X - Y||Y - Z|}{|Y|}.$$

LEMMA 2. *Let $Y, X_1, X_2, \dots, X_k$ be subsets of $\mathbb{F}_p$. Then*

$$|X_1 + X_2 + \ldots + X_k| \leqslant \frac{\prod_{i=1}^{k} |Y + X_i|}{|Y|^{k-1}}.$$

DEFINITION 2. *For any nonempty subsets $A \subset \mathbb{F}_p$, $B \subset \mathbb{F}_p$, $G \subset A \times B$, we define their* ***partial sum*** *as*

$$|A_G^+ B| = \{a + b : (a, b) \in G\}.$$

Let us recall a modification of Balog—Szemeredi—Gowers result (see the paper of J. Bourgain and M. Garaev [6], Lemma 2.3).

PROPOSITION 1. *Let A and B be subsets of $\mathbb{F}_p$ and $G \subset A \times B$ be such that $|G| \geqslant |A||B|/K$ for some $K > 0$. Then there exist subsets $A' \subset A, B' \subset B$ and a number Q with*

$$|A'| \geqslant \frac{|A|}{4\sqrt{2}K}, \quad \frac{|A|}{8\sqrt{2}K^2 \ln(e|A|)} \leqslant Q \leqslant 2|A'|, \quad |B'| \geqslant \frac{|A||B|}{8\sqrt{2}QK^2 \ln(e|A|)}$$

such that

$$|A_G^+ B|^3 \geqslant |A' + B'| \frac{Q|B|}{256K^3 \ln(e|A|)}.$$

We use the following result from the book of T. Tao and V. Vu [12, Lemma 2.30, p. 80].

LEMMA 3. *If $E_+(A, B) > 1/K \cdot |A|^{3/2}|B|^{3/2}$, $K \geqslant 1$, then there exists $G \subset A \times B$ satisfying*

$$|G| > \frac{1}{2K}|A||B| \quad \textit{and} \quad |A_G^+ B| < 2K|A|^{1/2}|B|^{1/2}.$$

This lemma represents a known technical approach for estimating sum-product sets (see, for example [1], [2]).

LEMMA 4. *For any given subsets $X, Y \subseteq \mathbb{F}_p, G \subset \mathbb{F}_p^*$ there is an element $\xi \in G$ with*

$$|X + \xi Y| \geqslant \frac{|X||Y||G|}{|X||Y| + |G|}.$$

Moreover, the following inequality holds:

$$|X+\xi Y| > \frac{|X|^2|Y|^2}{E_+(X,\xi Y)}.$$

PROOF. Let us take arbitrary elements $\xi \in G$ and $s \in \mathbb{F}_p$ and denote

$$f_\xi^+(s) := |\{(x,y) \in X \times Y : x + y\xi = s\}|.$$

It is obvious that

$$\sum_{s\in\mathbb{F}_p}(f_\xi^+(s))^2 = \left|\left\{(x_1,y_1,x_2,y_2) \in X\times X\times Y\times Y : x_1+y_1\xi = x_2+y_2\xi\right\}\right| =$$
$$= |X||Y| + \left|\left\{(x_1,y_1,x_2,y_2) \in X\times X\times Y\times Y : x_1 \neq x_2, x_1+y_1\xi = x_2+y_2\xi\right\}\right|$$

and

$$\sum_{s\in\mathbb{F}_p} f_\xi^+(s) = |X||Y|. \tag{1}$$

We observe that for every $x_1, x_2 \in X$, $y_1, y_2 \in Y$ such that $x_1 \neq x_2$, there is at most one $\eta \in G$ satisfying the equality $x_1 + y_1\eta = x_2 + y_2\eta$. Therefore,

$$\sum_{\xi\in G}\sum_{s\in\mathbb{F}_p}\left(f_\xi^+(s)\right)^2 \leqslant |X||Y||G| + |X|^2|Y|^2.$$

From the last inequality it directly follows that there is an element $\xi \in G$ such that

$$\sum_{s\in\mathbb{F}_p}\left(f_\xi^+(s)\right)^2 \leqslant |X||Y| + \frac{|X|^2|Y|^2}{|G|}. \tag{2}$$

According to the Cauchy—Schwartz inequality,

$$\left(\sum_{s\in\mathbb{F}_p} f_\xi^+(s)\right)^2 \leqslant |X+\xi Y|\sum_{s\in\mathbb{F}_p}\left(f_\xi^+(s)\right)^2. \tag{3}$$

Observing that

$$\sum_{s\in\mathbb{F}_p^*}\left(f_\xi^+(s)\right)^2 = E_+(X,\xi Y)$$

one can deduce the second assertion of Lemma 4.

Combining inequalities (1), (2) and (3) we see that

$$|X+\xi Y| \geqslant \frac{|X|^2|Y|^2}{|X||Y|+\frac{|X|^2|Y|^2}{|G|}} = \frac{|X||Y||G|}{|X||Y|+|G|}.$$

Lemma 4 now follows. □

Definition 3. *For any given subsets* $X, Y \subset \mathbb{F}_p$, $|Y|>1$ *we denote*

$$Q[X,Y] = \frac{X-X}{(Y-Y)\setminus\{0\}} := \left\{\frac{x_1-x_2}{y_1-y_2} : x_1,\ x_2 \in X,\ y_1, y_2 \in Y,\ y_1 \neq y_2\right\}.$$

If $X=Y$ *then* $Q[X,X]=Q[X]$.

Lemma 5 is a simple extension of Lemma 2.50 from the book by T. Tao and V. Vu [12].

Lemma 5. *Consider two arbitrary subsets* $X, Y \subset \mathbb{F}_p$, $|Y|>1$. *A given element* $\xi \in \mathbb{F}_p$ *is contained in* $Q[X,Y]$ *if and only if* $|X+\xi * Y| < |X||Y|$.

Proof. Consider a mapping $F : X\times Y$ to $X+\xi * Y$ defined by the identity $F(x,y) = x+\xi y$. The mapping F can be non-injective only when $|X+\xi * Y| < |X||Y|$. On the other side, the non-injectivity of F means that there are elements $x_1, x_2 \in X$, $y_1, y_2 \in Y$ such that $(x_1,y_1) \neq (x_2,y_2)$ and $F(x_1,y_1) = F(x_2,y_2)$. It is obvious that $y_1 \neq y_2$ since otherwise $x_1 = x_2$ and we get a contradiction with the condition $(x_1,y_1) \neq (x_2,y_2)$. Hence, $\xi = (x_1-x_2)/(y_2-y_1) \in Q[X,Y]$. Lemma 5 now follows. □

We need the following Lemma due to C.-Y. Shen [7].

Lemma 6. *Let* X_1 *and* X_2 *be two sets. Then for any* $\varepsilon \in (0,1)$ *there exist at most* $\dfrac{\ln 1/\varepsilon}{|X_2|}\min\{|X_1+X_2|, |X_1-X_2|\}$ *additive translates of* X_2 *whose union contains at least* $(1-\varepsilon)|X_1|$ *elements of* X_1.

Proof. For simplicity, we assume that $|X_1+X_2| \leqslant |X_1-X_2|$. The case when $|X_1+X_2| > |X_1-X_2|$ can be considered similarly. Using Lemma 4 we deduce

$$\left|\left\{(x,y,x_1,y_1) \in X_1\times X_2\times X_1\times X_2 : x+y=x_1+y_1\right\}\right| \geqslant \frac{|X_1|^2|X_2|^2}{|X_1+X_2|}.$$

Now we can fix two elements $x_*^1 \in X_1$, $y_*^1 \in X_2$ for which the equation $x_*^1 + y = x + y_*^1$, $x \in X_1$, $y \in X_2$ has at least $|X_1||X_2|/|X_1 + X_2|$ solutions and, therefore, $|(x_*^1 + X_2) \cap (y_*^1 + X_1)| \geqslant |X_1||X_2|/|X_1 + X_2|$. Denoting $N = |X_1 + X_2|/|X_2|$ we can observe that

$$\left|X_1 \cap \left(x_*^1 - y_*^1 + X_2\right)\right| \geqslant \frac{|X_1|}{N}. \tag{4}$$

Obviously, from (4) it follows that

$$\left|X_1^1\right| := \left|X_1 \setminus (x_*^1 - y_*^1 + X_2)\right| \leqslant \left(1 - \frac{1}{N}\right)|X_1|.$$

We can repeat the previous argument for the sets X_1^1 and X_2 and find elements $x_*^2 \in X_1^1$ and $y_*^2 \in X_2$ such that

$$\left|X_1^1 \cap \left(x_*^2 - y_*^2 + X_2\right)\right| \geqslant \frac{\left|X_1^1\right|}{N},$$
$$\left|X_1^2\right| := \left|X_1^1 \setminus \left(x_*^2 - y_*^2 + X_2\right)\right| \leqslant \left(1 - \frac{1}{N}\right)|X_1^1| \leqslant \left(1 - \frac{1}{N}\right)^2 |X_1|.$$

On the i-th iteration we find elements $x_*^i \in X_1^{i-1}$ and $y_*^i \in X_2$ with

$$\left|X_1^{i-1} \cap \left(x_*^i - y_*^i + X_2\right)\right| \geqslant \frac{|X_1^{i-1}|}{N},$$
$$\left|X_1^i\right| := \left|X_1^{i-1} \setminus \left(x_*^i - y_*^i + X_2\right)\right| \leqslant \left(1 - \frac{1}{N}\right)|X_1^{i-1}| \leqslant \left(1 - \frac{1}{N}\right)^i |X_1|.$$

We stop when $|X_1^n| < \varepsilon|X_1|$ for some n. It is easy to see that we will do at most $\ln(1/\varepsilon)K$ steps. The last observation completes the proof of Lemma 6. □

We also need the following sum-product estimate of M. Z. Garaev [8, Theorem 3.1].

THEOREM 5. *Let $A, B \subset \mathbb{F}_p$ be arbitrary subsets. Then*

$$|A - A|^2 \cdot \frac{|A|^2|B|^2}{E_\times(A, B)} \geqslant C|A|^3 L^{1/9}(\log_2 L)^{-1},$$

where $L = \min\left\{|B|, \dfrac{p}{|A|}\right\}$ *and* $C > 0$ *is an absolute constant.*

3. Proof of Theorem 3

Let $A, B \subseteq \mathbb{F}_p$ be as in Theorem 3 and $\delta > 0$, $C > 1$ to be specified. Assume

$$\sum_{b\in B} E_+(A, bA) > C|B|^{1-\delta}|A|^3.$$

Hence there is a subset $B_1 \subseteq B$ such that

$$|B_1| > \frac{C}{2}|B|^{1-\delta} \tag{5}$$

and

$$E_+(A, bA) > \frac{C}{2}|B|^{-\delta}|A|^3 \text{ for } b \in B_1. \tag{6}$$

Fix $b \in B_1$. Applying Lemma 3 to (6), one can deduce that there exists $G^{(b)} \subset A \times bA$, $|G^{(b)}| > C/4 \cdot |B|^{-\delta}|A|^2$ such that $\left|A^+_{G^{(b)}}bA\right| < 4/C \cdot |B|^{\delta}|A|$. Now, by Proposition 1, there are $A_1^{(b)}, A_2^{(b)} \subset A$ and $Q_{(b)}$ such that

$$\left|A_1^{(b)}\right| > \frac{C}{2^4\sqrt{2}}|B|^{-\delta}|A|, \tag{7}$$

$$\frac{C^2}{2^7\sqrt{2}\ln(e|A|)}|A||B|^{-2\delta} \leqslant Q_{(b)} \leqslant 2\left|A_1^{(b)}\right|, \tag{8}$$

$$\left|A_2^{(b)}\right| > \frac{C^2}{2^7\sqrt{2}Q_{(b)}\ln(e|A|)}|B|^{-2\delta}|A|^2, \tag{9}$$

$$\left|A_1^{(b)} + bA_2^{(b)}\right| < \frac{2^{20}}{C^6Q_{(b)}}\ln(e|A|)|B|^{6\delta}|A|^2. \tag{10}$$

By the Cauchy—Schwartz inequality

$$\frac{C^3}{2^{12}\ln(e|A|)}|B_1||B|^{-3\delta}|A|^2 < \sum_{b\in B_1}|A_1^{(b)} \times A_2^{(b)}| \leqslant$$

$$\leqslant |A|\left[\sum_{b,b'\in B_1}\left|\left(A_1^{(b)} \cap A_1^{(b')}\right) \times \left(A_2^{(b)} \cap A_2^{(b')}\right)\right|\right]^{1/2}.$$

Hence

$$\frac{C^6}{2^{24}\ln^2(e|A|)}|B_1|^2|B|^{-6\delta}|A|^2 < \sum_{b,b'\in B_1}\left|\left(A_1^{(b)}\cap A_1^{(b')}\right)\times\left(A_2^{(b)}\cap A_2^{(b')}\right)\right|$$

and there is some $b_0\in B_1$ such that

$$S=\sum_{b\in B_1}\left|\left(A_1^{(b)}\cap A_1^{(b_0)}\right)\times\left(A_2^{(b)}\cap A_2^{(b_0)}\right)\right| > \frac{C^6}{2^{24}\ln^2(e|A|)}|B_1||B|^{-6\delta}|A|^2.$$

Now we define

$$B_2=\left\{b\in B_1 : \left|A_1^{(b)}\cap A_1^{(b_0)}\right|\cdot\left|A_2^{(b)}\cap A_2^{(b_0)}\right| > \frac{C^6}{2^{25}\ln^2(e|A|)}|B|^{-6\delta}|A|^2\right\}.$$

Obviously,

$$S_1=\sum_{b\in B_1\setminus B_2}\left|\left(A_1^{(b)}\cap A_1^{(b_0)}\right)\times\left(A_2^{(b)}\cap A_2^{(b_0)}\right)\right| \leqslant \frac{C^6}{2^{25}\ln^2(e|A|)}|B_1||B|^{-6\delta}|A|^2,$$

$$S_2=\sum_{b\in B_2}\left|\left(A_1^{(b)}\cap A_1^{(b_0)}\right)\times\left(A_2^{(b)}\cap A_2^{(b_0)}\right)\right| = S-S_1 > \frac{C^6}{2^{25}\ln^2(e|A|)}|B_1||B|^{-6\delta}|A|^2.$$

Observing that $S_2\leqslant|B_2||A|^2$ and using (5) one easily deduces

$$|B_2| > \frac{C^7}{2^{26}\ln^2(e|A|)}|B|^{1-7\delta}, \tag{11}$$

$$\left|A_1^{(b)}\cap A_1^{(b_0)}\right|, \left|A_2^{(b)}\cap A_2^{(b_0)}\right| > \frac{C^6}{2^{25}\ln^2(e|A|)}|B|^{-6\delta}|A| \text{ for } b\in B_2. \tag{12}$$

From (7), (9), (10), (12) and Lemma 1 we see that

$$\left|b_0A_1^{(b_0)}+bA_1^{(b_0)}\right| \leqslant \frac{\left|A_1^{(b_0)}+bA_2^{(b_0)}\right|\left|A_1^{(b_0)}+b_0A_2^{(b_0)}\right|}{\left|A_2^{(b_0)}\right|} \leqslant$$

$$\leqslant \frac{2^{27}\sqrt{2}\ln^2(e|A|)}{C^8}|B|^{8\delta}\left|A_1^{(b_0)}+bA_2^{(b_0)}\right|, \tag{13}$$

$$\left|A_1^{(b_0)}+bA_2^{(b_0)}\right| \leqslant \frac{\left|A_1^{(b_0)}+bA_2^{(b)}\right|\left|A_2^{(b_0)}+A_2^{(b_0)}\right|}{\left|A_2^{(b)}\cap A_2^{(b_0)}\right|} \leqslant$$

$$\leqslant \frac{\left|A_1^{(b_0)}+bA_2^{(b)}\right|\left|A_1^{(b_0)}+b_0A_2^{(b_0)}\right|^2}{|A_2^{(b)}\cap A_2^{(b_0)}|\,|A_1^{(b_0)}|}\leqslant$$

$$\leqslant \frac{2^{69}\sqrt{2}\ln^4(e|A|)}{C^{19}Q_{(b_0)}^2}|A|^2|B|^{19\delta}|A_1^{(b_0)}+bA_2^{(b)}|, \tag{14}$$

$$\left|A_1^{(b_0)}+bA_2^{(b)}\right| \leqslant \frac{\left|A_1^{(b)}+bA_2^{(b)}\right|\left|A_1^{(b_0)}+A_1^{(b_0)}\right|}{\left|A_1^{(b_0)}\cap A_1^{(b)}\right|}\leqslant$$

$$\leqslant \frac{\left|A_1^{(b)}+bA_2^{(b)}\right|\left|A_1^{(b_0)}+b_0A_2^{(b_0)}\right|^2}{\left|A_1^{(b_0)}\cap A_1^{(b)}\right|\left|A_2^{(b_0)}\right|}\leqslant \frac{2^{92}\sqrt{2}\ln^6(e|A|)}{C^{26}Q_{(b)}Q_{(b_0)}}|B|^{26\delta}|A|^3. \tag{15}$$

Hence by (13), (14) and (15) we have

$$\left|b_0A_1^{(b_0)}+bA_1^{(b_0)}\right| \leqslant \frac{2^{189}\sqrt{2}\ln^{12}(e|A|)}{C^{53}Q_{(b_0)}^3Q_{(b)}}|B|^{53\delta}|A|^5.$$

Using (8) we finally obtain

$$\left|b_0A_1^{(b_0)}+bA_1^{(b_0)}\right| \leqslant \frac{2^{219}\sqrt{2}\ln^{16}(e|A|)}{C^{61}}|B|^{61\delta}|A|.$$

Now we redefine $A_1^{(b_0)}$ by A' and B_2/b_0 by B'. One can deduce the following properties (for $\delta<1/440$):

$$|A'+bA'|<\frac{2^{219}\sqrt{2}\ln^{16}(e|A|)}{C^{61}}|B|^{61\delta}|A| \text{ for all } b\in B', \tag{16}$$

$$|B'|>\frac{C^7}{2^{26}\ln^2(e|A|)}|B|^{1-7\delta}, \tag{17}$$

$$|A'|>\frac{C}{2^4\sqrt{2}}|B|^{-\delta}|A|. \tag{18}$$

Our aim is to get a contradiction from (16), (17) and (18).

We will use the symbol

$$M=\max_{b\in B'}|A'+bA'|, \quad \text{so that} \quad M<\frac{2^{219}\sqrt{2}\ln^{16}(e|A|)}{C^{61}}|B|^{61\delta}|A|. \tag{19}$$

Now we use Lemma 4 to establish the bound

$$E_+(A', bA') = \big|\big\{(a_1, a_2, a_3, a_4) \in A' \times A' \times A' \times A' : a_1 + a_2 b = a_3 + a_4 b\big\}\big| \geqslant \\ \geqslant \frac{|A'|^4}{|A' + bA'|} \geqslant \frac{|A'|^4}{M}. \tag{20}$$

By summation over all $b \in B'$ we obviously obtain

$$\big|\big\{(a_1, a_2, a_3, a_4, b) \in A' \times A' \times A' \times A' \times B' : a_1 + a_2 b = a_3 + a_4 b\big\}\big| \geqslant \frac{|A'|^4 |B'|}{M}.$$

There are some elements $\widetilde{a}_2, \widetilde{a}_3 \in A'$ such that

$$\big|\big\{(a_1, a_4, b) \in A' \times A' \times B' : a_1 - \widetilde{a}_3 = (a_4 - \widetilde{a}_2) b\big\}\big| \geqslant \frac{|A'|^2 |B'|}{M}.$$

Let $A'_1 = A' - \widetilde{a}_3$, $A'_2 = A' - \widetilde{a}_2$ be the translates of A' by $\widetilde{a}_3$ and $\widetilde{a}_2$ respectively. Then

$$\big|\big\{(a_1, a_2, b) \in A'_1 \times A'_2 \times B' : a_1 = a_2 b\big\}\big| \geqslant \frac{|A'|^2 |B'|}{M}.$$

There exists some $a_* \in A'_2$ such that

$$\big|\big\{(a_1, b) \in A'_1 \times B' : a_1 = a_* b\big\}\big| \geqslant \frac{|A'||B'|}{M}.$$

Thus, we have a subset $B'_1 \subset (A'_1 \cap a_* B')$ of cardinality

$$\big|B'_1\big| \geqslant \frac{|A'||B'|}{M}.$$

In original notation B'_1 lies in the intersection of $a_*/b_0 B_2$ and some translate of $A_1^{(b_0)}$; moreover, by the bounds (17), (18) and (19) one has

$$\big|B'_1\big| > \frac{C^{69}}{2^{250} \ln^{18}(e|A|)} |B|^{1-69\delta}. \tag{21}$$

We consider three cases.

Case 1. Suppose that $Q\big[B_1'\big] \neq \mathbb{F}_p$. It is clear that $1 + Q\big[B_1'\big] \neq Q\big[B_1'\big]$ since otherwise $Q\big[B_1'\big] = \mathbb{F}_p$. The latter means that there are elements $a, b, c, d \in B_1'$ with $1 + \dfrac{a-b}{c-d} \notin Q\big[B_1'\big]$. Now we recall that B_1' is a subset of $a_*/b_0 \cdot B_2$ so we can regard a, b, c, d as elements of B_2. Observe that for an arbitrary subset $B_1'' \subset B_1'$ we have $1 + \dfrac{a-b}{c-d} \notin Q[B_1'']$ since $Q[B_1''] \subset Q[B_1']$. Therefore, by Lemma 5, for these elements $a, b, c, d \in B_2$ we have

$$\big|B_1''\big|^2 = \left|B_1'' + \left(B_1'' + \frac{a-b}{c-d}B_1''\right)\right| \leqslant \left|B_1'' + B_1'' + \frac{a-b}{c-d}B_1''\right|. \qquad (22)$$

We now use Lemma 6. First of all we will show that for any $b_1 \in B_2$ we can cover 99 % of the elements of the set b_1B_1' (a subset of the translation of $b_1A_1^{(b_0)}$) or $-b_1B_1'$ by at most $\dfrac{2^{109}\ln(100)\ln^8(e|A|)}{C^{28}}|B|^{28\delta}$ additive translates of the set $b_0A_1^{(b_0)}$. Indeed $b_0A_1^{(b_1)} \cap A_1^{(b_0)}$ is a subset of $b_0A_1^{(b_0)}$, and by Lemma 6 and Lemma 1 we can cover 99 % of the elements of either b_1B_1' or $-b_1B_1'$ by at most

$$\frac{\ln(100)}{\big|b_0A_1^{(b_1)} \cap A_1^{(b_0)}\big|} \min\Big\{\big|b_0A_1^{(b_1)} \cap A_1^{(b_0)} + b_1B_1'\big|, \big|b_0A_1^{(b_1)} \cap A_1^{(b_0)} - b_1B_1'\big|\Big\} \leqslant$$

$$\leqslant \frac{\ln(100)}{\big|A_1^{(b_1)} \cap A_1^{(b_0)}\big|} \min\Big\{\big|b_0A_1^{(b_1)} \cap A_1^{(b_0)} + b_1A_1^{(b_0)}\big|, \big|b_0A_1^{(b_1)} \cap A_1^{(b_0)} - b_1A_1^{(b_0)}\big|\Big\} \leqslant$$

$$\leqslant \frac{\ln(100)\big|A_1^{(b_1)} \cap A_1^{(b_0)} + b_1A_2^{(b_0)} \cap A_2^{(b_1)}\big|\big|A_1^{(b_0)} + b_0A_2^{(b_0)} \cap A_2^{(b_1)}\big|}{\big|A_1^{(b_1)} \cap A_1^{(b_0)}\big|\big|b_0b_1A_2^{(b_1)} \cap A_2^{(b_0)}\big|} \leqslant$$

$$\leqslant \frac{\ln(100)\big|A_1^{(b_1)} + b_1A_2^{(b_1)}\big|\big|A_1^{(b_0)} + b_0A_2^{(b_0)}\big|}{\big|A_1^{(b_1)} \cap A_1^{(b_0)}\big|\big|A_2^{(b_1)} \cap A_2^{(b_0)}\big|} \leqslant \frac{2^{105}\ln(100)\ln^8(e|A|)}{C^{28}}|B|^{28\delta}$$

additive translates of $b_0A_1^{(b_1)} \cap A_1^{(b_0)}$ and whence of $b_0A_1^{(b_0)}$. In the last estimate we have used (8), (10) and (12).

We consider all these estimates together. This enables us to choose B_1'' as a subset containing at least 98 % of the elements from B_1' such that $(a-b)B_1''$ gets covered by at most $\dfrac{2^{210}\ln^2(100)\ln^{16}(e|A|)}{C^{56}}|B|^{56\delta}$ translates of $b_0A_1^{(b_0)} + b_0A_1^{(b_0)}$.

Similarly, we can find a subset $\widetilde{A}_1^{(b_0)}$ containing at least 98 % of the elements of $A_1^{(b_0)}$ such that $(c-d)\widetilde{A}_1^{(b_0)}$ gets covered by at most $\dfrac{2^{210}\ln^2(100)\ln^{16}(e|A|)}{C^{56}}|B|^{56\delta}$ translates of $b_0A_1^{(b_0)}+b_0A_1^{(b_0)}$. Now we apply Lemma 2 to (22) as follows:

$$\begin{aligned}\left|B_1''+B_1''+\frac{a-b}{c-d}B_1''\right| &\leqslant \frac{\left|\widetilde{A}_1^{(b_0)}+B_1''+B_1''\right|\left|\widetilde{A}_1^{(b_0)}+\frac{a-b}{c-d}B_1''\right|}{\left|\widetilde{A}_1^{(b_0)}\right|}\leqslant\\ &\leqslant \frac{2^4\sqrt{2}|B|^{\delta}}{C|A|}\left|A_1^{(b_0)}+A_1^{(b_0)}+A_1^{(b_0)}\right|\left|\widetilde{A}_1^{(b_0)}+\frac{a-b}{c-d}B_1''\right|\leqslant\\ &\leqslant \frac{2^{87}\ln^6(e|A|)}{C^{25}}|B|^{25\delta}\left|\widetilde{A}_1^{(b_0)}+\frac{a-b}{c-d}B_1''\right|. \qquad (23)\end{aligned}$$

The covering argument above implies that

$$\begin{aligned}\left|\widetilde{A}_1^{(b_0)}+\frac{a-b}{c-d}B_1''\right| &\leqslant \frac{2^{420}\ln^4(100)\ln^{32}(e|A|)}{C^{112}}|B|^{112\delta}\left|A_1^{(b_0)}+A_1^{(b_0)}+A_1^{(b_0)}+A_1^{(b_0)}\right|\leqslant\\ &\leqslant \frac{2^{530}\ln^4(100)\ln^{40}(e|A|)}{C^{144}}|B|^{144\delta}|A|.\end{aligned}$$

Comparing this with (21), (22) and using the conditions $|B|/|A|\geqslant 1/4$, $\left|B_1''\right|\geqslant 0.98\left|B_1'\right|$, for large p we deduce that

$$\begin{aligned}&\frac{(0.98)^2C^{138}}{2^{500}\ln^{36}(e|A|)}|B|^{2-138\delta}<\frac{2^{613}\ln^4(100)\ln^{46}(e|A|)}{C^{169}}|B|^{169\delta}|A|\Leftrightarrow\\ &\Leftrightarrow\frac{|B|^{2-307\delta}}{|A|\ln^{82}(e|A|)}<\frac{2^{1113}\ln^4(100)}{(0.98)^2C^{307}}\Rightarrow|B|^{1-308\delta}<\frac{2^{1115}\ln^4(100)}{(0.98)^2C^{307}}. \qquad (24)\end{aligned}$$

Now we define $C=\dfrac{2^{1115/307}\ln^{4/307}(100)}{(0.98)^{2/307}}$ and from (24) deduce the inequality

$$|B|<|B|^{308\delta}$$

which is false when $\delta\leqslant 1/308$. This finishes the proof of Theorem 3 in the case 1.

Case 2. Suppose that $\left|B_1'\right|>\sqrt{p}$. It is clear that $Q\left[B_1'\right]=\mathbb{F}_p$ since for an arbitrary $\xi\in\mathbb{F}_p$ the equality $\left|B_1'+\xi B_1'\right|=\left|B_1'\right|^2$ is impossible (simply because $\left|B_1'\right|^2>p$).

Let us take arbitrary elements $\xi \in \mathbb{F}_p^*$, $s \in \mathbb{F}_p$, an arbitrary subset $|B_1''| \geqslant 0.96|B_1'|$ and denote

$$f_\xi(s) := \big|\{(b_1, b_2) \in B_1' \times B_1' : b_1 + \xi b_2 = s\}\big|,$$
$$f_\xi'(s) := \big|\{(b_1, b_2) \in B_1'' \times B_1'' : b_1 + \xi b_2 = s\}\big|$$

It is obvious that

$$\sum_{s\in\mathbb{F}_p}(f_\xi(s))^2 = \big|\{(b_1, b_2, b_3, b_4) \in B_1' \times B_1' \times B_1' \times B_1' : b_1 + \xi b_2 = b_3 + \xi b_4\}\big| =$$
$$= |B_1'|^2 + \big|\{(b_1, b_2, b_3, b_4) \in B_1' \times B_1' \times B_1' \times B_1' : b_1 \neq b_3, b_1 + \xi b_2 = b_3 + \xi b_4\}\big|$$

and

$$\sum_{s\in\mathbb{F}_p} f_\xi(s) = |B_1'|^2, \quad \sum_{s\in\mathbb{F}_p} f_\xi'(s) = |B_1''|^2.$$

Let us observe that for every $b_1, b_2, b_3, b_4 \in B_1'$ such that $b_1 \neq b_3$, there is at most one $\eta \in \mathbb{F}_p^*$ satisfying the equality $b_1 + \eta b_2 = b_3 + \eta b_4$. Therefore,

$$\sum_{\xi\in\mathbb{F}_p^*}\sum_{s\in\mathbb{F}_p}(f_\xi(s))^2 \leqslant |B_1'|^2(p-1) + |B_1'|^4.$$

From the last inequality it directly follows that there exists an element $\xi \in \mathbb{F}_p^*$ such that

$$\sum_{s\in\mathbb{F}_p}(f_\xi'(s))^2 \leqslant \sum_{s\in\mathbb{F}_p}(f_\xi(s))^2 \leqslant |B_1'|^2 + \frac{|B_1'|^4}{p-1}.$$

Note that this ξ is independent of B_1''. According to the Cauchy—Schwartz inequality,

$$\Big(\sum_{s\in\mathbb{F}_p} f_\xi'(s)\Big)^2 \leqslant |B_1'' + \xi B_1''| \sum_{s\in\mathbb{F}_p}(f_\xi'(s))^2.$$

Now we see that

$$|B_1'' + \xi B_1''| \geqslant \frac{|B_1''|^4(p-1)}{|B_1'|^2(p-1) + |B_1'|^4} \geqslant \frac{(0.96)^4|B_1'|^4(p-1)}{|B_1'|^2(p-1) + |B_1'|^4} \geqslant (0.96)^4\frac{p-1}{2}. \qquad (25)$$

Recall that $Q[B_1'] = \mathbb{F}_p$. So we can find elements $a, b, c, d \in B_1'$, such that $\xi = \dfrac{a-b}{c-d}$ (again, we can regard them as elements of B_2). Using a covering

argument as in the proof of the case 1 we can choose B_1'' as a subset containing at least 96 % of the elements from B_1' such that $(a-b)B_1'' + (c-d)B_1''$ gets covered by at most $\frac{2^{420}\ln^4(100)\ln^{32}(e|A|)}{C^{112}}|B|^{112\delta}$ translates of $b_0A_1^{(b_0)} + b_0A_1^{(b_0)} + b_0A_1^{(b_0)} + b_0A_1^{(b_0)}$. Now we see that

$$\left|B_1'' + \frac{a-b}{c-d}B_1''\right| \leqslant \frac{2^{420}\ln^4(100)\ln^{32}(e|A|)}{C^{112}}|B|^{112\delta}\left|A_1^{(b_0)} + A_1^{(b_0)} + A_1^{(b_0)} + A_1^{(b_0)}\right| \leqslant$$
$$\leqslant \frac{2^{530}\ln^4(100)\ln^{40}(e|A|)}{C^{144}}|B|^{144\delta}|A|.$$

Again, comparing this with (25) and using the condition $|B|/|A| \geqslant 1/4$, we deduce that

$$(0.96)^4\frac{p}{4} \leqslant (0.96)^4\frac{p-1}{2} < \frac{2^{530}\ln^4(100)\ln^{40}(e|A|)}{C^{144}}|B|^{144\delta}|A| \Rightarrow$$
$$\Rightarrow \frac{p}{4} < \frac{2^{530}\ln^4(100)}{C^{144}(0.96)^4}p^{145\beta\delta+\alpha}. \tag{26}$$

Now we define $C = \frac{2^{265/72}\ln^{1/36}(100)}{(0.96)^{1/36}}$ and from (3) deduce the inequality

$$p < p^{145\beta\delta+\alpha}$$

which is false when $\delta \leqslant \frac{1-\alpha}{145\beta}$. This concludes the proof of the theorem in the case 2.

Case 3. Suppose that $Q[B_1'] = \mathbb{F}_p$ and $|B_1''| \leqslant \sqrt{p}$. Repeating the argument from the proof of case 2 for an arbitrary subset $B_1'' \subset B_1'$, $|B_1''| \geqslant 0.96|B_1'|$ we find elements $a, b, c, d \in B_2$ independent of the subset B_1'' with

$$\left|B_1'' + \frac{a-b}{c-d}B_1''\right| \geqslant (0.96)^4\frac{|B_1'|^2}{2}.$$

Using a covering argument as in the proof of the case 1 we can choose B_1'' as a subset containing at least 96 % of the elements from B_1' such that $(a-b)B_1'' + (c-d)B_1''$ gets covered by at most $\frac{2^{420}\ln^4(100)\ln^{32}(e|A|)}{C^{112}}|B|^{112\delta}$ translates

of $b_0A_1^{(b_0)}+b_0A_1^{(b_0)}+b_0A_1^{(b_0)}+b_0A_1^{(b_0)}$. Now we see that

$$\left|B_1'+\frac{a-b}{c-d}B_1'\right|\leqslant\frac{2^{420}\ln^4(100)\ln^{32}(e|A|)}{C^{112}}|B|^{112\delta}\left|A_1^{(b_0)}+A_1^{(b_0)}+A_1^{(b_0)}+A_1^{(b_0)}\right|\leqslant$$
$$\leqslant\frac{2^{530}\ln^4(100)\ln^{40}(e|A|)}{C^{144}}|B|^{144\delta}|A|.$$

Comparing this with (21) and using the condition $|B|/|A|\geqslant 1/4$, we deduce that

$$\frac{(0.96)^4C^{138}}{2^{500}\ln^{36}(e|A|)}|B|^{2-138\delta}<\frac{2^{530}\ln^4(100)\ln^{40}(e|A|)}{C^{144}}|B|^{144\delta}|A|\Leftrightarrow$$
$$\Leftrightarrow\frac{|B|^{2-282\delta}}{|A|\ln^{76}(e|A|)}<\frac{2^{1030}\ln^4(100)}{(0.96)^4C^{282}}\Rightarrow|B|^{1-283\delta}<\frac{2^{1032}\ln^4(100)}{(0.96)^4C^{282}}. \qquad (27)$$

Now we define $C=\dfrac{2^{516/141}\ln^{2/141}(100)}{(0.96)^{2/141}}$ and from (3) deduce the inequality

$$|B|<|B|^{283\delta}$$

which is false when $\delta\leqslant 1/283$. Note that in all the cases the value of the constant C is strictly less than 15. Theorem 3 is proved. □

4. Proof of Theorem 4

As in the proof of Theorem 3 we assume contrary, i. e. $\sum\limits_{b\in B}E_+(A,bA)>C|B|^{1-\delta}|A|^3$ for some $C>0$, $\delta>0$. Following the argument from the beginning of the proof of Theorem 3, we find $A'\subset A$ and $B'\subset\mathbb{F}_p^*$, $1\in B'$ (which is in fact a subset of a multiplicative shift of B) such that

$$|A'+bA'|<\frac{2^{219}\sqrt{2}\ln^{16}(e|A|)}{C^{61}}|B|^{61\delta}|A|=L\ \text{ for all }\ b\in B', \qquad (28)$$

$$|B'|>\frac{C^7}{2^{26}\ln^2(e|A|)}|B|^{1-7\delta}, \qquad (29)$$

$$|A'|>\frac{C}{2^4\sqrt{2}}|B|^{-\delta}|A|. \qquad (30)$$

Using Lemma 4 we obtain

$$\left|\left\{(a_1,a_2,a_3,a_4)\in A'\times A'\times A'\times A' : a_1+ba_2=a_3+ba_4\right\}\right| > \frac{|A'|^4}{L} \quad \text{for all} \quad b\in B'.$$

By summation over all $b\in B'$ one gets

$$\left|\left\{(a_1,a_2,a_3,a_4,b)\in A'\times A'\times A'\times A'\times B' : a_1+ba_2=a_3+ba_4\right\}\right| > \\ > \frac{|A'|^4|B'|}{L} \quad \text{for all} \quad b\in B'.$$

Now we can fix elements $a_3^0, a_2^0\in A'$ such that

$$\left|\left\{(a_1,a_4,b)\in A'\times A'\times B' : a_1-a_3^0=b(a_4-a_2^0)\right\}\right| > \frac{|A'|^2|B'|}{L}. \tag{31}$$

We denote

$$f(s)=\left|\left\{(a,b)\in A'\times B' : b(a-a_2^0)=s\right\}\right|, \quad g(s)=\begin{cases}1, & \text{if } s\in A'-a_3^0;\\ 0, & \text{otherwise.}\end{cases}$$

Clearly,

$$\left|\left\{(a_1,a_4,b)\in A'\times A'\times B' : a_1-a_3^0=b(a_4-a_2^0)\right\}\right| = \sum_{s\in\mathbb{F}_p} f(s)g(s), \tag{32}$$

$$\sum_{s\in\mathbb{F}_p} f^2(s) = E_\times\left(A'-a_2^0, B'\right). \tag{33}$$

Now, by the Cauchy—Schwartz inequality,

$$\left(\sum_{s\in\mathbb{F}_p} f(s)g(s)\right)^2 \leqslant \sum_{s\in\mathbb{F}_p} f^2(s)\sum_{s\in\mathbb{F}_p} g^2(s)$$

and, by (32) and (33), one can deduce that

$$E_\times\left(A'-a_2^0, B'\right) > \frac{|A'|^3|B'|}{L^2}.$$

Consider two cases.

Case 1. Assume that $|A'||B'| \leqslant p$. Applying Theorem 5 one obtains

$$\frac{L^4}{|A'|} > |A' - A'|^2 \cdot \frac{|A'|^2|B'|^2}{E_\times\left(A' - a_2^0, B'\right)} \geqslant C_1 \frac{|A'|^3|B'|^{1/9}}{\log_2(|B'|)}.$$

Using (28), (29) and (30) we deduce

$$\frac{C_1 C^{43/9}|B|^{1/9-43/9\delta}|A|^4}{2^{188/9}\ln^{2/9}(e|A|)\log_2(|B|)} < \frac{2^{878}\ln^{64}(e|A|)}{C^{244}}|B|^{244\delta}|A|^4 \Rightarrow$$

$$\Rightarrow |B|^{1/9} < \frac{2^{8090/9}\ln^{578/9}(e|A|)\log_2(|B|)}{C_1 C^{2239/9}}|B|^{2239/9\delta}. \tag{34}$$

Defining $C = \dfrac{2^{8090/2239}}{C_1^{9/2239}}$, we observe that for sufficiently large p from (4) it follows that

$$|B|^{1/9} < |B|^{2240/9\delta}.$$

This gives a contradiction when $\delta = 1/2240$. The proof of Theorem 4 in this case is completed.

Case 2. Assume that $|A'||B'| > p$. Again, applying Theorem 5 we obtain

$$\frac{L^4}{|A'|} > |A' - A'|^2 \cdot \frac{|A'|^2|B'|^2}{E_\times\left(A' - a_2^0, B'\right)} \geqslant C_1 \frac{|A'|^{26/9}p^{1/9}}{\log_2 p}.$$

Using (28) and (30) we deduce

$$\frac{C_1 C^{35/9}|A|^{35/9}p^{1/9}}{2^{35/2}|B|^{35/9}\log_2 p} < \frac{2^{878}\ln^{64}(e|A|)}{C^{244}}|B|^{244\delta}|A|^4 \Rightarrow$$

$$\Rightarrow \frac{2^{1791/2}\ln^{64}(e|A|)\log_2 p}{C^{2231/9}C_1}|A|^{1/9}|B|^{2231/9\delta} > p^{1/9}. \tag{35}$$

Defining $C = \dfrac{2^{19119/4462}}{C_1^{9/2231}}$, we observe that for sufficiently large p from (4) it follows that

$$p^{1/9} < |B|^{2232/9\delta}|A|^{1/9}.$$

This gives a contradiction when $\delta = \dfrac{1-\alpha}{2232}$. Theorem 4 is proved. □

Acknowledgements. The author thanks Professors S. Konyagin and M. Rudnev for useful discussions which helped him to improve the final result. The research is supported by RFBR grant № 11-01-00759-a.

Bibliography

1. ***J. Bourgain, N. Katz, T. Tao,*** *A sum-product estimate in finite fields and their applications*, Geom and Funct. Anal. **14** (2004), 27–57.
2. ***J. Bourgain, S. Konyagin,*** *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, C. R. Acad. Sci. Paris **I 337** (2003), 75–80.
3. ***J. Bourgain, S. J. Dilworth, K. Ford, S. Konyagin, D. Kutzarova,*** *Explicit constructions of RIP matrices*, Proc. 43rd ACM Symposium of the Theory of Computing (STOC) (2011), 637–644.
4. ***J. Bourgain, A. Glibichuk,*** *Exponential sum estimate over subgroup in an arbitrary finite field*, accepted for publication in Journal de Analyze Mathématiques.
5. ***J. Bourgain,*** *Multilinear exponential sums in prime fields under optimal entropy condition on the sources*, Geometric and Functional Analysis **18**, № 5 (2009), 1477–1502.
6. ***J. Bourgain, M. Z. Garaev,*** *On a variant of sum-product estimates and explicit exponential sums bounds in prime fields*, Mathematical proceedings of the Cambridge Philosophical Society, **146** (2009), part 1, 1–21.
7. ***Chun-Yen Shen,*** *Quantitative sum product estimates on different sets*, Electron. J. Combin. **15**, № 1 (2008).
8. ***M. Z. Garaev,*** *Sums and products of sets and estimates of rational trigonometric sums in fields of prime order*, Russian Mathematical Surveys **65**, № 4 (2010), 599–658.
9. ***H. Helfgott, M. Rudnev,*** *An explicit incidence theorem in* $\mathbb{F}_p$, preprint, arXiv:1001.1980v2.
10. ***I. Z. Ruzsa,*** *An application of graph theory to additive number theory*, Scientia **A 3** (1989), 97–109.
11. ***I. Z. Ruzsa,*** *Sums of finite sets*, Number theory (New York, 1991–1995), 281–293, Springer, New York, 1996.
12. ***T. Tao, V. Vu,*** *Additive combinatorics*, Cambridge University Press, Cambridge, 2006.

Alexey Glibichuk

Technion, Israel Institute of Technology,
Amato Building,
32000 Haifa, Israel
aanatol@mail.ru