

# ON WIENER NORM OF SUBSETS OF $\mathbb{Z}_p$ OF MEDIUM SIZE

S. V. KONYAGIN<sup>1</sup>, I. D. SHKREDOV<sup>2</sup>

Abstract.

*We give a lower bound for Wiener norm of characteristic function of subsets  $A$  from  $\mathbb{Z}_p$ ,  $p$  is a prime number, in the situation when  $\exp((\log p / \log \log p)^{1/3}) \leq |A| \leq p/3$ .*

## 1 Introduction

We consider the abelian group  $G = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ , where  $p$  is a prime number. Denote the Fourier transform of a complex function on  $G$  to be a new function

$$\hat{f}(\gamma) = \frac{1}{p} \sum_{x \in G} f(x) e_p(x\gamma),$$

where  $e_p(u) = \exp(2\pi i u/p)$  (we note that  $e_p$  is correctly defined for  $u \in \mathbb{Z}_p$ ). It is known that the function  $f$  can be reconstructed from  $\hat{f}$  by the inverse Fourier transform

$$f(x) = \sum_{\gamma \in \mathbb{Z}_p} \hat{f}(\gamma) e_p(-x\gamma). \quad (1)$$

We define the Wiener norm of a function  $f$  as

$$\|f\|_{A(G)} = \|f\|_A = \|\hat{f}\|_1 = \sum_{\gamma \in \mathbb{Z}_p} |\hat{f}(\gamma)|.$$

By  $\chi_S$ ,  $S \subset G$  denote the characteristic function of some set  $S$ .

In this note we discuss the problem of estimation from below the Wiener norm of  $\chi_A$  for  $A \subset \mathbb{Z}_p$  in terms of  $p$  and  $|A|$ .

---

<sup>1</sup>The first author is supported by grant RFBR 14-01-00332 and grant Leading Scientific Schools N 3082.2014.1

<sup>2</sup>The second author is supported by grant mol\_a\_ved 12-01-33080.

If  $x \in A$ , then, by (1), we have

$$1 = \left| \sum_{\gamma \in \mathbb{Z}_p} \hat{f}(\gamma) e_p(-x\gamma) \right| \geq \sum_{\gamma \in \mathbb{Z}_p} |\hat{f}(\gamma)|.$$

Thus, we get a trivial estimate for Wiener norm of any nonempty  $A \subset \mathbb{Z}_p$

$$\|\chi_A\|_A \geq 1. \quad (2)$$

Next we observe that because of

$$\|\chi_{\mathbb{Z}_p \setminus A}\|_A = \|\chi_A\|_A + (1 - 2|A|/p)$$

it is sufficient to consider the case  $|A| < p/2$ . It is easy to see that if  $A \subset \mathbb{Z}_p$  is an arithmetic progression with

$$2 \leq |A| < p/2 \quad (3)$$

then

$$\|\chi_A\|_A \asymp \log |A|.$$

It is commonly believed that for any  $A$  satisfying (3) there is the same lower bound

$$\|\chi_A\|_A \gg \log |A|. \quad (4)$$

The first nontrivial lower bound for  $\|\chi_A\|_A$ ,  $|A| < p/2$ , in some range was established in [2]:

$$\|\chi_A\|_A \gg \frac{|A|}{p} \left( \frac{\log p}{\log \log p} \right)^{1/3}.$$

This estimate was improved by T. Sanders [7] for  $|A| < p/2$ ,  $|A| \gg p$ . As was shown in [4], the results of [7] imply the following.

**Theorem 1** *Let  $p$  be a prime number,  $A \subset \mathbb{Z}_p$ ,  $0 < \eta = |A|/p < 1/2$ . If  $\eta \geq (\log p)^{-1/4} (\log \log p)^{1/2}$  then*

$$\|\chi_A\|_A \gg (\log p)^{1/2} (\log \log p)^{-1} \eta^{3/2} \left( 1 + \log \left( \eta^2 (\log p)^{1/2} (\log \log p)^{-1} \right) \right)^{-1/2},$$

and if  $\eta < (\log p)^{-1/4} (\log \log p)^{1/2}$  then

$$\|\chi_A\|_A \gg \eta^{1/2} (\log p)^{1/4} (\log \log p)^{-1/2}.$$

Our interest to study Wiener norm of large subsets of  $\mathbb{Z}_p$  was inspired by the paper of V.V. Lebedev [5] on quantitative variants of Beurling–Helson theorem.

Theorem 1 is nontrivial if our subset  $A$  is large, that is

$$|A|p^{-1}(\log p)^{1/2}(\log \log p)^{-1} \rightarrow \infty$$

(and of course  $|A| < p/2$ ). For small  $A$  we proved in [4] a sharp estimate.

**Theorem 2** *Let  $p$  be a prime number,  $A \subset \mathbb{Z}_p$ , and*

$$2 \leq |A| \leq \exp((\log p / \log \log p)^{1/3}).$$

*Then*

$$\|\chi_A\|_A \gg \log |A|.$$

In this note we study the subsets  $A \subset \mathbb{Z}_p$  of medium size. Our main result is the following assertion.

**Theorem 3** *Let  $p$  be a prime number,  $A \subset \mathbb{Z}_p$ ,*

$$\exp((\log p / \log \log p)^{1/3}) \leq |A| \leq p/3.$$

*Then*

$$\|\chi_A\|_A \gg (\log(p/|A|))^{1/3}(\log \log(p/|A|))^{-1+o(1)}.$$

We observe that using arguments of Theorem 2 one can get analogous estimates for sets  $A$  slightly exceeding the bound indicated in the statement. However, the improvement is marginal. Moreover, it seems that by that way one cannot get a nontrivial estimate for rather large subsets, namely, such that  $\log |A| \gg \log p$ .

## 2 Comparison with the continuous case

We denote  $e(u) = \exp(2\pi iu)$ . For sets  $B \subset \mathbb{Z}$  a continuous analog of (4) is a well-known fact. Namely, it was proved in [3] and [6] that if  $B \subset \mathbb{Z}$ ,  $2 \leq |B| < \infty$  then

$$\int_0^1 \left| \sum_{b \in B} e(bu) \right| du \gg \log |B|.$$

Moreover, in [6] the following stronger result was proved: if  $b_1 < \dots < b_l$  are real numbers and  $c_j$  are arbitrary complex numbers then

$$\int_0^1 \left| \sum_{j=1}^l c_j e(b_j u) \right| du \gg \sum_{j=1}^l \frac{|c_j|}{j}. \quad (5)$$

This inequality implies the following lemma.

**Lemma 4** *Let  $n \in \mathbb{N}$ ,  $B \subset [-2n, 2n] \subset \mathbb{Z}$ ,  $|B| \geq 2$ ,  $0 < \eta < 1/2$ ,  $|B \cap [-n, n]| \geq (1 - \eta)|B|$ ,  $c(b)$  ( $b \in B$ ) are complex numbers with  $c(b) = 1$  for  $b \in B \cap [-n, n]$ . Then*

$$\int_0^1 \left| \sum_{b \in B} c(b) e(bu) \right| du \gg \min \left( \log \frac{1}{\eta}, \log |B| \right).$$

**Proof** Let  $B = \{b_1 < \dots < b_l\}$  where  $l = |B|$ , and let  $B \cap [-n, n] = \{b_{l_1} < \dots < b_{l_2}\}$ . The polynomial  $\sum_{b \in B} c(b) e(bu)$  can be rewritten as  $\sum_{j=1}^l c_j e(b_j u)$  where  $c_j = 1$  for  $l_1 \leq j \leq l_2$ . We denote

$$S = \int_0^1 \left| \sum_{b \in B} c(b) e(bu) \right| du.$$

By (5),

$$S \gg \sum_{j=l_1}^{l_2} \frac{1}{j} \gg \log((l_2 + 1)/l_1).$$

We have  $l_2 - l_1 + 1 \geq (1 - \eta)l$ . If  $\eta < 1/l$ , then  $l_1 = 1$ ,  $l_2 = l$ ,  $S \gg \log((l_2 + 1)/l_1) = \log l$  as required. If  $\eta \geq 1/l$ , then we have

$$l_1 \leq \eta l + 1 < 2\eta l.$$

Hence,

$$\log((l_2 + 1)/l_1) \geq \log((l_1 + (1 - \eta)l)/l_1) \geq \log((1 + \eta)/2\eta) \gg \log(1/\eta),$$

and we again get the assertion of the lemma.  $\square$

The discrete and continuous  $L^1$ -norms of trigonometric polynomials can be compared by the following lemma.

**Lemma 5** *We have*

$$\frac{1}{p} \sum_{\gamma \in \mathbb{Z}_p} \left| \sum_{|x| \leq p/3} c_x e_p(x\gamma) \right| \gg \int_0^1 \left| \sum_{|x| \leq p/3} c_x e(xu) \right| du.$$

See [11], chapter 10, Theorem 7.28.

One can deduce (4) from Lemma 5 provided that  $A \subset [-p/3, p/3]$  (this inclusion means that any residue  $a \in A$  has an integer representative from  $[-p/3, p/3]$ ) or if some non-degenerate affine image of  $A$  in  $\mathbb{Z}_p$  is contained in  $[-p/3, p/3]$ . This argument was used in the proof of Theorem 2.

Now let us define the de la Vallée-Poussin polynomials and means. For functions

$$F(\gamma) = \sum_{x \in \mathbb{Z}_p} c_x e_p(x\gamma), \quad G(\gamma) = \sum_{x \in \mathbb{Z}_p} d_x e_p(x\gamma)$$

we define their convolution

$$F * G(\gamma) = \sum_{x \in \mathbb{Z}_p} c_x d_x e_p(x\gamma).$$

It is easy to see that

$$F * G(\gamma) = \frac{1}{p} \sum_{\xi_1 + \xi_2 = \gamma} F(\xi_1) G(\xi_2).$$

Therefore,

$$\sum_{\gamma \in \mathbb{Z}_p} |F * G(\gamma)| \leq \frac{1}{p} \sum_{\gamma \in \mathbb{Z}_p} |F(\gamma)| \sum_{\gamma \in \mathbb{Z}_p} |G(\gamma)|. \quad (6)$$

Study of arbitrary trigonometric polynomials in  $\mathbb{Z}_p$  can be reduced to polynomials of small degree using de la Vallée-Poussin means. Define the de la Vallée-Poussin polynomial of order  $n \leq p/4$  as

$$V_n(\gamma) = \sum_{|x| \leq n} e_p(x\gamma) + \sum_{n < |x| \leq 2n} \frac{2n - |x| + 1}{n + 1} e_p(x\gamma)$$

and the de la Vallée-Poussin mean for  $F$  of order  $n \leq p/4$  as  $F * V_n$ .

We need in the lemma.

**Lemma 6** For  $n \leq p/4$  the following inequality holds

$$\sum_{\gamma \in \mathbb{Z}_p} |V_n(\gamma)| \leq 3p.$$

The proof is contained in the proof of Theorem 7.28 of chapter 10 in [11].

Using Lemma 6 and (6) we obtain the following lemma.

**Lemma 7** For  $n \leq p/4$  the following inequality holds

$$\sum_{\gamma \in \mathbb{Z}_p} \left| \sum_{|x| \leq n} c_x e_p(x\gamma) + \sum_{n < |x| \leq 2n} \frac{2n - |x| + 1}{n + 1} c_x e_p(x\gamma) \right| \leq 3 \sum_{\gamma \in \mathbb{Z}_p} \left| \sum_{|x| \leq p/2} c_x e_p(x\gamma) \right|.$$

Combining Lemmas 7, 5, and 4 we get the following.

**Lemma 8** Let  $B \subset \mathbb{Z}_p$ ,  $n \leq p/6$ ,  $0 < \eta < 1/2$ . Assume that  $|B \cap [-2n, 2n]| \geq 2$  and

$$|B \cap [-n, n]| \geq (1 - \eta)|B \cap [-2n, 2n]|.$$

Then

$$\|\hat{\chi}_B\|_1 \gg \min \left( \log \frac{1}{\eta}, \log |B \cap [-2n, 2n]| \right).$$

### 3 Balog–Szemerédi–Gowers theorem, Freiman’s theorem, and structure of sets with small Wiener norm

Given an arbitrary set  $Q \subset \mathbb{Z}_p$  and  $k \in \mathbb{N}$ , denote the quantity  $\mathbf{T}_k(Q)$  as the number of solutions to the equation

$$x_1 + \cdots + x_k = x'_1 + \cdots + x'_k$$

with  $x_1, \dots, x_k, x'_1, \dots, x'_k \in Q$ . Note that for  $\mathbf{T}_2(Q)$  is commonly called the additive energy of  $Q$  (see, e.g. [10]). We have

$$\mathbf{T}_k(Q) = p^{2k-1} \sum_{\gamma} |\hat{\chi}_Q(\gamma)|^{2k}.$$

The following lemma is a particular case of Lemma 4 from [4].

**Lemma 9** *Let  $Q \subset A \subset \mathbb{Z}_p$ ,  $\|\chi_A\|_A \leq K$ ,  $k \in \mathbb{N}$ . Then*

$$\mathbf{T}_k(Q) \geq \frac{|Q|^{2k}}{|A|K^{2k-2}}.$$

In particular,

$$\mathbf{T}_2(A) \geq \frac{|A|^3}{\|\chi_A\|_A^2}. \quad (7)$$

For subsets  $A, B$  of an ambient additive abelian group their sum and difference are defined in a natural way:

$$A \pm B = \{a \pm b : a \in A, b \in B\}.$$

The following result is the current version of the Balog–Szemerédi–Gowers theorem [9] (see also [1]).

**Lemma 10** *If  $G$  is an additive abelian group,  $A$  is a nonempty finite subset of  $G$ ,  $\mathbf{T}_2(A) \geq |A|^3/L$ , then there exists  $A' \subset A$  such that  $|A'| \gg |A|/L$  and*

$$|A' - A'| \ll L^4|A'|. \quad (8)$$

Next, it is known that

$$|A'| |A' + A'| \leq |A' - A'|^2$$

(see Corollary 6.29 from [10]). Hence, (8) implies the inequality

$$|A' + A'| \ll L^8|A'|. \quad (9)$$

Another important ingredient from Additive Combinatorics is Freiman's theorem. Define a generalized arithmetic progression (GAP) as a subset of  $\mathbb{Z}_p$  of the form

$$P = P(x_0; \mathbf{x}; \mathbf{w}) = \left\{ x_0 + \sum_{i=1}^d v_i x_i : 0 \leq v_i < w_i (i = 1, \dots, d) \right\}$$

where  $\mathbf{x} = (x_1, \dots, x_d) \in \mathbb{Z}_p^d$ ,  $\mathbf{w} = (w_1, \dots, w_d) \in \mathbb{N}^d$ . We will assume that all  $x_i$  are not equal to zero. The dimension of  $P$  is  $d$  and the size of  $P$  is  $\prod_{i=1}^d w_i$ . The following result is the current version of the Freiman's theorem [7].

**Lemma 11** *If  $B$  is a nonempty subset of  $\mathbb{Z}_p$ ,  $|B+B| \leq M|B|$ ,  $M \geq 2$ , then there is a GAP  $P$  of dimension at most  $\log^{3+o(1)} M$  and size at most  $|B|$  such that*

$$|B \cap P| \geq |B| \exp\left(-\log^{3+o(1)} M\right).$$

Applying subsequently (7), Lemma 8 with (9), and Lemma 11 we get

**Lemma 12** *For any  $\varepsilon > 0$  and  $K \geq K(\varepsilon)$  if  $A$  is a nonempty subset of  $\mathbb{Z}_p$  with  $\|\chi_A\|_A \leq K$  and*

$$d_\varepsilon = d_\varepsilon(K) = \log^{3+\varepsilon} K \tag{10}$$

*then there exists a GAP  $P$  of dimension at most  $d_\varepsilon$  and size at most  $|A|$  such that*

$$|A \cap P| \geq |A|e^{-d_\varepsilon}.$$

Our immediate purpose is to put some multiplicative translate of a set with small Wiener norm into a small segment of  $\mathbb{Z}_p$ . To do it, recall Blichfeld's lemma ([10], Lemma 3.27).

**Lemma 13** *Let  $\Gamma \subset \mathbb{R}^d$  be a lattice of full rank, and let  $V$  be an open set in  $\mathbb{R}^d$  such that  $\text{mes}(V) > \text{mes}(\mathbb{R}^d/\Gamma)$ . Then there exist distinct  $x, y \in V$  such that  $x - y \in \Gamma$ .*

Let  $P = P(x_0; \mathbf{x}; \mathbf{w})$  be the GAP from Lemma 12, let

$$\alpha_i = \frac{(|A|/p)^{1/d}}{w_i}$$

for  $i = 1, \dots, d$ ,  $\delta > 0$  be a small number,

$$V_\delta = \prod_{i=1}^d (-\delta, \alpha_i + \delta) \subset \mathbb{R}^d.$$

We observe that

$$\text{mes}(V_\delta) > \prod_{i=1}^d \alpha_i = \frac{|A|}{p} \prod_{i=1}^d w_i^{-1} \geq \frac{1}{p}.$$

Let  $\Gamma$  be the lattice

$$\Gamma = \mathbb{Z}^d + \frac{\mathbf{x}}{p}\mathbb{Z}.$$



Then  $\Gamma$  is a union of  $p$  translates of  $\mathbb{Z}^d$ . Consequently,  $\text{mes}(\mathbb{R}^d/\Gamma) = 1/p$ . Now we can apply Lemma 13 and conclude that there exist distinct  $x, y \in V_\delta$  such that  $x - y \in \Gamma$ . Tending  $\delta$  to 0 we see that there are distinct points

$$x, y \in V_0 = \prod_{i=1}^d [0, \alpha_i]$$

with  $x - y \in \Gamma$ . Equivalently, putting

$$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$$

and denoting by  $|z|$ ,  $z \in \mathbb{Z}_p$  the minimal absolute value of a representative of  $z$  in  $\mathbb{Z}$ , we see that there exists  $q \in \mathbb{Z}_p^*$ ,  $q < p$  such that for  $i = 1, \dots, d$  the following holds  $|qx_i| \leq p\alpha_i$ .

For any  $x \in P$  we have

$$|q(x - x_0)| = \left| q \sum_{i=1}^d v_i x_i \right| < \sum_{i=1}^d w_i |qx_i| \leq \sum_{i=1}^d w_i \alpha_i = dp(|A|/p)^{1/d}.$$

So, we get the following structural property of sets with small Wiener norm.

**Lemma 14** *For any  $\varepsilon > 0$  and  $K \geq K(\varepsilon)$  if  $A$  is a nonempty subset of  $\mathbb{Z}_p$  with  $\|\chi_A\|_A \leq K$ ,  $d_\varepsilon$  is defined by (10),*

$$m = \left[ d_\varepsilon p \left( \frac{|A|}{p} \right)^{1/d_\varepsilon} \right],$$

*then there exist  $x_0 \in \mathbb{Z}_p$  and  $q \in \mathbb{Z}_p^*$  such that for the set*

$$B = q(A - x_0) = \{q(x - x_0) : x \in A\}$$

*we have*

$$|B \cap [-m, m]| \geq |A|e^{-d_\varepsilon}.$$

## 4 Upper estimates of $T_k(Q)$ for scattered $Q$

Let us formulate the main result of the section.

**Lemma 15** *Let  $I, k, m, M$  be positive integers. Let also  $Q = \bigsqcup_{i=1}^I Q_i \subseteq \mathbb{Z}$  be a set such that  $Q_i \subseteq [-4^i m, -\frac{4^i}{2} m) \cup (\frac{4^i}{2} m, 4^i m]$ ,  $i$  runs over a subset of  $\mathbb{N}$  of cardinality  $I$ , and  $|Q_i| = M$ . Then*

$$\mathbf{T}_k(Q) \leq 2^{8k} k^k I^k M^{2k-1}. \quad (11)$$

**Proof of Lemma 15.** First of all, put  $Q^+ = Q \cap \{x : x \geq 0\}$  and  $Q^- = Q \setminus Q^+$ . Using Hölder inequality, one can easily obtain

$$\mathbf{T}_k(Q) \leq 4^k \max\{\mathbf{T}_k(Q^+), \mathbf{T}_k(Q^-)\}$$

and, thus, we need in an appropriate upper bound for  $\mathbf{T}_k(Q^+), \mathbf{T}_k(Q^-)$ . Without losing of generality, we bound just  $\mathbf{T}_k(Q^+)$ , and, moreover, we write  $Q$  instead of  $Q^+$ .

Further, put  $N_k(x) = |\{q_1 + \dots + q_k = x : q_j \in Q\}|$ . Clearly,  $\sum_x N_k^2(x) = \mathbf{T}_k(Q)$  and

$$\sum_x N_k(x) = |Q|^k = I^k M^k.$$

In view of the last identity it is sufficient to prove the following uniform estimate for  $N_k(x)$ .

**Lemma 16** *For any  $x$ , we have*

$$N_k(x) \leq 2^{6k} k^k M^{k-1}.$$

**Proof of the lemma.** Take a vector  $\vec{s} = (s_1, \dots, s_b)$ ,  $s_1 + \dots + s_b = k$ , and put

$$N_k^{\vec{s}}(x) = |\{q_1 + \dots + q_k = x : \exists s_1 \text{ elements from } A_{i_1}, \dots, \exists s_b \text{ elements from } A_{i_b}\}|,$$

where  $i_1 < i_2 < \dots < i_l$ . Then

$$N_k(x) = \sum_{\vec{s}} N_k^{\vec{s}}(x) \cdot \frac{k!}{s_1! \dots s_b!}. \quad (12)$$

Thus, we need to estimate  $N_k^{\vec{s}}(x)$  for any  $\vec{s}$ . Because of

$$N_k^{\vec{s}}(x) \leq \sum_{q_1 \in A_{i_1}} \cdots \sum_{q_b \in A_{i_{b-1}}} \delta_0(q_1 + \cdots + q_b - x) \leq \Delta_1(\vec{s}) \cdots \Delta_{b-1}(\vec{s}) M^{k-1}, \quad (13)$$

where  $\Delta_l(\vec{s})$  is the number of choices for indices of sets  $A_{i_l}$ , and  $\delta_0(z)$  is the function such that  $\delta_0(z) = 1$  iff  $z = 0$ . We need to estimate the quantities  $\Delta_l(\vec{s})$ . Suppose that the sets  $A_{i_1}, \dots, A_{i_{l-1}}$  are fixed and let us find an upper bound for the number of sets  $A_{i_l}$ . Let  $z$  be the least integer number such that

$$\sum_{j=1}^{l-1} s_j 4^j \leq s_l \frac{4^{l+z}}{2}. \quad (14)$$

Then the number of the sets  $A_{i_l}$  is bounded by  $z+1$ . Indeed, without losing of generality, we can suppose that  $i_j = j$ ,  $j \in [l-1]$  and  $i_l = l+z'$ ,  $z' > z$ . Then the set  $A_{i_l}$  is defined uniquely because otherwise we have a solution of the equation

$$\mu_1 + \cdots + \mu_{l-1} + \mu_l = x = \mu'_1 + \cdots + \mu'_{l-1} + \mu'_l, \quad (15)$$

where  $\mu_j, \mu'_j \in s_j A_{i_j}$ ,  $j \in [l-1]$ , and, similarly,  $\mu_l \in s_l A_{l+z'}$ ,  $\mu'_l \in s_l A_{i_l}$ ,  $i_l < l+z'$ . If (15) takes place then

$$s_l \frac{4^{l+z}}{2} \leq s_l \frac{4^{l+z'}}{2} < \mu'_l - \mu_l \leq \mu_1 + \cdots + \mu_{l-1} \leq \sum_{j=1}^{l-1} s_j 4^j$$

with a contradiction. It follows that

$$\Delta_l(\vec{s}) \leq \log\left(2 \sum_{j=1}^{l-1} s_j 4^{j-l}\right) + 1 \leq \log\left(2 \max_{1 \leq j \leq l-1} \{s_j 2^{j-l}\}\right) + 1.$$

Let  $m_1 < m_2 < \cdots < m_t$  be the local maximums of the sequence  $\max_{1 \leq j \leq l-1} \{s_j 2^{j-l}\}$ ,  $l \in [b-1]$ . Let also  $d_j$  be the number of appearing of the maximum  $m_j$ . Then  $\sum_{j=1}^t d_j = k$ . Further, by the construction of the sequence  $\max_{1 \leq j \leq l-1} \{s_j 2^{j-l}\}$ ,  $l \in [b-1]$  one can see that  $d_j \leq \log 2s_j$ ,  $j \in [t]$ . Returning to (12), and having (13), we get

$$N_k(x) \leq M^{k-1} \sum_{\vec{s}} \frac{k!}{s_1! \cdots s_b!} \cdot (\log 2s_{m_1} + 1)^{d_1} \cdots (\log 2s_{m_t} + 1)^{d_t} \leq$$

$$\begin{aligned}
&\leq M^{k-1} e^k k! \sum_{s_{m_1}, \dots, s_{m_t}} \prod_{j=1}^t \frac{(\log 2s_{m_j} + 1)^{\log 2s_{m_j}}}{s_{m_j}!} \leq \\
&\leq M^{k-1} e^{2k} k! \left( \sum_s \frac{(\log 2s + 1)^{\log 2s}}{s^s} \right)^t \leq 2^{6k} k^k M^{k-1}
\end{aligned}$$

as required. Thus, we have proved our lemma and, hence, Lemma 15.  $\square$

**Remark 17** *If one allows an additional multiplies of the form  $(\log k)^k$  in bound (11) then the result follows immediately. Indeed, we can split our set  $A$  onto sets  $B_1, \dots, B_r$ ,  $r \sim \log k$  such that each  $B_j$  contains  $A_l$  with  $l \equiv j \pmod{r}$ . Thus we lose exactly  $(\log k)^k$  multiple but any set  $A_{i_l}$  in each  $B_j$  is defined uniquely, all  $\Delta_j(\vec{s}) = 1$  (see formulas (13), (14)), and, hence,  $\mathbf{T}_k(B_j) \leq C^k k^k M^{k-1} |B_j|^k$ , where  $C > 0$  is an absolute constant.*

## 5 Proof of Theorem 3

We fix an arbitrary  $\varepsilon > 0$  and assume that

$$\|\chi_A\|_A \leq K, \quad K_\varepsilon \leq K \leq (\log(p/|A|))^{1/3} (\log \log(p/|A|))^{-1-\varepsilon}. \quad (16)$$

Our aim is to prove that (16) cannot hold provided that  $p/|A|$  exceeds some quantity depending on  $\varepsilon$ . Since  $\varepsilon > 0$  is arbitrary, the theorem will follow.

We take  $x_0, q, m$ , and  $B$  accordingly with Lemma 14. Since

$$\hat{\chi}_B(\gamma) = e_p(-qx_0\gamma) \hat{\chi}_A(q\gamma),$$

we conclude that  $\|\chi_B\|_A = \|\chi_A\|_A$ . Thus,

$$\|\chi_B\|_A \leq K. \quad (17)$$

Let  $l_0$  be the maximal positive integer  $l$  with  $2^l m < p/3$ ,

$$D_l = \{b \in B : |b| \leq 2^l m\}, \quad 0 \leq l \leq l_0,$$

$$\eta = \exp(-CK)$$

for a large constant  $C$ , and

$$M = \lceil \eta |A| e^{-d_\varepsilon} \rceil.$$

If for some  $l \geq 1$  we have  $|D_l \setminus D_{l-1}| < M$  then applying Lemma 8 to  $n = 2^{l-1}m$  and taking into account the inequality  $|D_l| \geq |D_0|$  and the lower bound for  $|D_0|$  from Lemma 14 we find

$$\|\hat{\chi}_B\|_1 \gg \min \left( \log \frac{1}{\eta}, \log |D_0| \right).$$

Since

$$\log |D_0| \geq \log |A| - d_\varepsilon \gg (\log p / \log \log p)^{1/3} > K (\log \log p)^{2/3} > \log \frac{1}{\eta},$$

we see that

$$\|\hat{\chi}_B\|_1 \gg \log \frac{1}{\eta},$$

and we get contradiction with (17) provided that  $C$  is large enough.

Thus, it is enough to consider the case where  $|D_l \setminus D_{l-1}| \geq M$  for all  $l = 1, \dots, l_0$ . For each  $l$  with  $l \equiv 0 \pmod{2}$  we take  $S_l \subset D_l \setminus D_{l-1}$  with  $|S_l| = M$ . Define

$$Q = \bigsqcup_l S_l.$$

Now we are in position to use Lemma 15 with  $k = \lceil K \rceil$  and the sets  $Q_i$  that are the sets  $S_l$  in another numeration ( $I = \lfloor l_0/2 \rfloor$ ). Let us compare the upper estimate (11) for  $\mathbf{T}_k(Q)$  with the lower estimate from Lemma 9 taking into account that  $|Q| = IM$ . After simple calculations we obtain

$$\frac{|Q|}{|A|} I^{k-1} \leq K^{3k-2} 2^{8k}$$

implying (because of  $|Q|/|A| \leq \exp(\log^{3+\varepsilon} K)$ )

$$I \ll K^3. \tag{18}$$

We have

$$I \geq l_0/2 - 1 \gg \log(p/m) \geq d_\varepsilon^{-1} \log(p/|A|) - \log d_\varepsilon.$$

Recalling (16) and (10) we see that

$$|I| \gg d_\varepsilon^{-1} \log(p/|A|) \gg \log(p/|A|) (\log \log(p/|A|))^{-3-\varepsilon}.$$

So, (18) does not agree with (16) as required.  $\square$

## References

- [1] J. BOURGAIN AND M.Z. GARAEV. On a variant of sum-product estimates and explicit exponential sum bounds in prime fields // *Math. Proc. Cambridge Philos. Soc.*, **146**:1, 1–21, 2009.
- [2] B.J. GREEN, S.V. KONYAGIN. On the Littlewood problem modulo a prime // *Canad. J. Math.*, **61**:1, 141–164, 2009.
- [3] S.V. KONYAGIN. On a problem of Littlewood // *Izvestiya of Russian Academy of Sciences*, **45**:2, 243–265, 1981.
- [4] S.V. KONYAGIN, I.D. SHKREDOV. Quantitative version of Beurling–Helson theorem // submitted.
- [5] V.V. LEBEDEV. Absolutely convergent Fourier series. An improvement of Beurling–Helson theorem. // *Funct. Anal. Appl.*, **46**:2, 52–65, 2012.
- [6] O.C. MCGEHEE, L. PIGNO, B. SMITH. Hardy’s inequality and the  $L^1$  norm of exponential sums // *Annals of Math.*, **113**, 613–618, 1981.
- [7] T. SANDERS. The Littlewood–Gowers problem // *J. Anal. Math.*, **101**, 123–162, 2007.
- [8] T. SANDERS. The structure theory of set addition revisited // *Bull. AMS*, **50**:1, 93–127, 2013.
- [9] T. SCHOEN. New bounds in Balog–Szemerédi–Gowers theorem // *Combinatorica*, accepted.
- [10] T. TAO, V. VU. *Additive combinatorics* / CUP, 2006.
- [11] A. ZYGMUND. *Trigonometric series* / V. 2, CUP, 2002.

S.V. Konyagin  
Steklov Mathematical Institute,  
ul. Gubkina, 8, Moscow, Russia, 119991  
and  
MSU,  
Leninskie Gory, Moscow, Russia, 119992  
konyagin@mi.ras.ru

I.D. Shkredov  
Steklov Mathematical Institute,  
ul. Gubkina, 8, Moscow, Russia, 119991  
and  
IITP RAS,  
Bolshoy Karetny per. 19, Moscow, Russia, 127994  
[ilya.shkredov@gmail.com](mailto:ilya.shkredov@gmail.com)