On the Littlewood conjecture in $\mathbb{Z}/p\mathbb{Z}$

By

Tomasz Schoen*

Abstract

We show that for every set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ we have $\|\widehat{1}_A\|_1 := \frac{1}{p}\sum_{r=0}^{p-1}|\sum_{a\in A} e^{2\pi i ra/p}| \gg (\log|A|)^{1/16-o(1)}$.

1 Introduction

The following conjecture, known as the Littlewood conjecture, was posed in [6]: for every finite set of integers A we have

$$\int_0^1 |\sum_{a\in A} e^{2\pi i a x}|dx \gg \log|A|.$$

This conjecture attracted attention of many mathematicians (see for example [1], [3], [4], [11]) and finally it was confirmed independently by McGehee, Pigno and Smith [10] and Konyagin [7]. Green and Konyagin asked an analogues question in discrete case for subsets of $\mathbb{Z}/p\mathbb{Z}$: is it true that

$$\|\widehat{1}_A\|_1 := \frac{1}{p}\sum_{r=0}^{p-1}|\sum_{a\in A} e^{2\pi i ra/p}| \gg \log|A|.$$

They proved [5] that

$$\|\widehat{1}_A\|_1 \gg \delta\Big(\frac{\log p}{\log\log p}\Big)^{1/3},$$

then this estimate was improved by Sanders [12]

$$\|\widehat{1}_A\|_1 \gg \Big(\frac{\log p}{(\log\log p)^3}\Big)^{1/2}$$

for sets with positive density. Konyagin and Shkredov [8] solved the problem for sparse sets with size $|A| \leqslant e^{(\log p)^{1/3-o(1)}}$. Furthermore, Konyagin and Shkredov [8], [9] proved the following results, which we will use later.

*The author is supported by NCN grant .

2010 Mathematics Subject Classification: primary 11B75, secondary 11P99.

Theorem 1.1 *Let A be a subset of $\mathbb{Z}/p\mathbb{Z}$. If $e^{(\log p)^{1/3}} \leqslant |A| \leqslant p/3$ then*

$$\|\widehat{1}_A\|_1 \gg (\log(1/\delta))^{1/3-o(1)}, \tag{1}$$

if $\delta \geqslant (\log p)^{-1/4}(\log\log p)^{1/2}$ then

$$\|\widehat{1}_A\|_1 \gg \delta^{3/2}(\log p)^{1/2-o(1)},$$

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

$$\|\widehat{1}_A\|_1 \gg \delta^{1/2}(\log p)^{1/4-o(1)},$$

The above results provides polylogarithmic lower bounds for sparse and very dense sets, however they gives very poor estimates for sets with density

$$e^{-(\log p)^{\varepsilon}} < \delta < (\log p)^{-1/2+\varepsilon}.$$

Our aim is to prove the following theorem.

Theorem 1.2 *Let A be a subset of $\mathbb{Z}/p\mathbb{Z}$. Then*

$$\|\widehat{1}_A\|_1 \gg (\log|A|)^{1/16-o(1)},$$

as $|A| \to \infty$.

We will use the following notation. Let G be a finite abelian group. For a function $f : G \to \mathbb{C}$ we set

$$\|f\|_{L^q} = \big(\frac{1}{|G|}\sum|f(x)|^q\big)^{1/q},$$

$$\|f\|_{\ell^q} = (\sum|f(x)|^q)^{1/q},$$

and if $\gamma \in \widehat{G}$ ia a character of G then we define the Fourier coefficient by

$$\widehat{f}(\gamma) = \frac{1}{|G|}\sum_x f(x)\overline{\gamma(x)}.$$

The convolution of two functions $f, g : G \to \mathbb{C}$ is defined by

$$(f * g)(t) = \sum_{x\in G} f(x)g(t-x),$$

for $t \in G$. Furthermore, we will write 1_A for the indicator function of a set A and $\|\widehat{1}_A\|_1$ for $\|\widehat{1}_A\|_{\ell^1}$.

2 Auxiliary Lemmas

We apply a quasi-periodic lemma due to Croot, Laba and Sisask [2]. To formulate this result we need some basic properties of Bohr sets contained in a finite abelian group G. For a set of characters $\Gamma \subseteq \widehat{G}$ and $0 < \varepsilon \leqslant 1/2$ we define

$$B(\Gamma, \varepsilon) = \{x \in G : |\gamma(x) - 1| \leqslant \varepsilon \text{ for all } \gamma \in \Gamma\}.$$

The size of Γ is the rank of B and ε is its radius. Furthermore, for all ε and Γ we have $B(\Gamma, \varepsilon) \geqslant (\varepsilon/2\pi)^{|\Gamma|}|G|$, see [13].

Lemma 2.1 *Let $q > 2$ and $0 < \varepsilon < 1$ be parameters. Let G be a finite abelian group and let $f : G \to \mathbb{C}$. Then there exists a Bohr set B of rank $\ll q/\varepsilon^2$ and radius $\gg \varepsilon$ such that for each $t \in B$*

$$\|f(x+t) - f(x)\|_{L^q} \leqslant \varepsilon \|\widehat{f}\|_1.$$

Corollary 2.2 *Suppose that A is a subset of finite abelian group G, $|A| = \delta|G|$ and that $\max_{t\neq 0}(1_A * 1_{-A})(t) < (1-\beta)|A|$ for some $0 < \beta \leqslant 1$. Then*

$$\|\widehat{1}_A\|_1 \gg \Big(\frac{\log |G|}{\log(1/\beta\delta) \log\log |G|}\Big)^{1/2}.$$

Proof. We apply Lemma 2.1 with $f = 1_A$ and ε, q to be determined later. Let B be a Bohr set given by the lemma. Observe that for each $t \in G$

$$\|1_A(x+t) - 1_A(x)\|^q_{L^q} = 2|G|^{-1}(|A| - (1_A * 1_{-A})(t)),$$

hence, for every $t \in B$

$$(1_A * 1_{-A})(t) \geqslant |A| - \frac{1}{2}\varepsilon^q \|\widehat{1}_A\|_1^q |G|.$$

By our assumption $(1_A * 1_{-A})(t) < (1-\beta)|A|$ for every $t \neq 0$, so if $t \in B \setminus \{0\}$ then $\varepsilon^q \|\widehat{1}_A\|_1^q |G| \geqslant \beta|A|$, hence

$$\|\widehat{1}_A\|_1 \geqslant (\beta\delta)^{1/q}\varepsilon^{-1}.$$

Taking $q = \log(1/\beta\delta)$ and $\varepsilon = c\Big(\frac{\log|G|}{q \log\log|G|}\Big)^{-1/2}$, we see that $|B| > 1$ and it gives the required bound. ■

Put $A_d = A \cap (A + d)$. The next lemma provides a straightforward dependence between $\|\widehat{1}_A\|_1$ and $\|\widehat{1}_{A_d}\|_1$, which is very important in our approach.

Lemma 2.3 *Let A be a finite subset of $\mathbb{Z}/p\mathbb{Z}$. Then for every $d \in A - A$ we have*

$$\|\widehat{1}_A\|_1 \geqslant \|\widehat{1}_{A_d}\|_1^{1/2}$$

Proof. We have

$$\widehat{1}_{A_d}(r) = \frac{1}{p}\sum_x 1_A(x)1_A(x-d)e^{-2\pi irx/p},$$

and applying the Fourier inversion formula $1_A(x) = \sum_{r=0}^{p-1}\widehat{1}_A(r)e^{2\pi irx/p}$ we see that

$$\widehat{1}_{A_d}(r) = \sum_s \widehat{1}_A(s)\widehat{1}_A(r-s)e^{2\pi id(r-s)/p},$$

hence

$$\|\widehat{1}_{A_d}\|_1 \leqslant \sum_r\sum_s |\widehat{1}_A(s)||\widehat{1}_A(r-s)| = \|\widehat{1}_A\|_1^2$$

and the assertion follows. ■

3 Proof of Theorem 1.2

In view of Theorem 1.1 we can restrict our attention to sets with density

$$e^{-(\log p)^{1/4}} < \delta < (\log p)^{-1/4}.$$

By Cauchy-Davenport theorem (see [13]) we have

$$|A-A| \geqslant \min(2|A|-1,\, p) \geqslant \frac{3}{2}|A|,$$

provided that $|A| \geqslant 2$, so there exists $d \in A-A$ such that

$$|A_d| = (1_A * 1_{-A})(d) \leqslant \frac{|A|^2}{\frac{3}{2}|A|} = \frac{2}{3}|A|.$$

We put $B = A \setminus A_d$ and observe that $|B| \geqslant \frac{1}{3}|A|$ and $d \notin B-B$. We consider two cases. First, let us assume that $\max_{t\neq 0}(1_B * 1_{-B})(t) < (1-\beta)|B|$, where $\beta = e^{-(\log p)^{3/4}}$. Then, by Corollary 2.2 we obtain

$$\|\widehat{1}_B\|_1 \gg (\log p)^{1/8-o(1)}.$$

Next let us assume that there exists $t \neq 0$ with $(1_B * 1_{-B})(t) \geqslant (1-\beta)|B|$. We show that then there is $s \in B-B$ such that $\beta|B| < |B_s| \leqslant 3\beta|B|$. Suppose to the contradiction. Let x be any element satisfying

$$(1_B * 1_{-B})(x) \geqslant 3\beta|B|,$$

so there are representations $x = a_i - b_i$, where $a_i, b_i \in B$ and $1 \leqslant i \leqslant \lceil 3\beta|B|\rceil$. Notice that from $(1_B * 1_{-B})(t) \geqslant (1-\beta)|B|$ it follows that among $a_i's$ there are at least

$$(1_B * 1_{-B})(x) - \beta|B| \geqslant 2\beta|B|$$

such that $a_i + t \in B$. Therefore, we infer that $(1_B * 1_{-B})(x+t) \geqslant 2\beta|B|$, but from our assumption it follows that

$$(1_B * 1_{-B})(x+t) \geqslant 3\beta|B|.$$

Since $(1_B * 1_{-B})(0) = |B|$ we see that $B - B = \mathbb{Z}/p\mathbb{Z}$, which is a contradiction. If $\beta|B| < |B_s| \leqslant 3\beta|B|$ then by Lemma 2.3 and (1) we have

$$\|\widehat{1}_B\|_1 \geqslant \|\widehat{1}_{B_s}\|_1^{1/2} \gg (\log p)^{1/8-o(1)}.$$

To finish the proof it is enough to observe that $\widehat{1}_A(r) = \widehat{1}_B(r) + \widehat{1}_{A_d}(r)$, so that $|\widehat{1}_A(r)| \geqslant |\widehat{1}_B(r)| - |\widehat{1}_{A_d}(r)|$ and $\|\widehat{1}_A\|_1 \geqslant \|\widehat{1}_B\|_1 - \|\widehat{1}_{A_d}\|_1$. Again, by Lemma 2.3

$$\|\widehat{1}_A\|_1 \geqslant \max(\|\widehat{1}_B\|_1 - \|\widehat{1}_{A_d}\|_1, \|\widehat{1}_{A_d}\|_1^{1/2}) \gg (\log p)^{1/16-o(1)},$$

which completes the proof. ■

References

[1] P. J. Cohen, *On a conjecture of Littlewood and idempotent measures,* Amer. J. Math. 82 1960, 191-212.

[2] E. Croot, I. Laba, O. Sisask, *Arithmetic progressions in sumsets and L^p-almost-periodicity,* Combin. Probab. Comput. 22 (2013), 351–365.

[3] H. Davenport, *On a theorem of P. J. Cohen,* Mathematika 7 (1960), 93–97.

[4] J. J. F. Fournier, *On a theorem of Paley and the Littlwood conjecture,* Arkiv för Mathematik 17 (1979), 199–216.

[5] B. J. Green, S. V. Konyagin, *On the Littlewood problem modulo a prime,* Canad. J. Math. 61 (2009), 141–164.

[6] G. H. Hardy, J. E. Littlewood, *A new proof of a theorem on rearrangements,* J. London Math. Soc. 23 (1948), 163–168.

[7] S. V. Konyagin, *On a problem of Littlewood,* Izvestiya of Russian Academy of Sciences, 45 (1981), 243–265.

[8] S. V. Konyagin, I. D. Shkredov, *A quantitative version of Beurling Helson theorem,* Functional Analysis and Its Applications, 49 (2015), 110–121.

[9] S. V. Konyagin, I. D. Shkredov, *On Wiener norm of subsets of $\mathbb{Z}_p$ of medium size,* Journal of Mathematical Sciences, 218 (2016), 599–608.

[10] O. C. McGehee, L. Pigno, B. Smith, *Hardy's inequality and the L^1 norm of exponential sums,* Annals of Math. 113 (1981), 613–618.

[11] S. K. Pichorides, *On the L^1 norm of exponential sums,* Annales de l'institut Fourier 30 (1980), 79–89.

[12] T. Sanders, *The Littlewood-Gowers problem,* J. Anal. Math. 101 (2007), 123–162.

[13] T. Tao, V. Vu, Additive combinatorics, Cambridge University Press 2006.

Faculty of Mathematics and Computer Science,
Adam Mickiewicz University,
Umultowska 87, 61-614 Poznań, Poland
schoen@amu.edu.pl