ON THE DISTRIBUTION OF EXPONENTIAL SUMS

Sergei V. Konyagin
Department of Mechanics and Mathematics, Moscow State University, Moscow 119899, Russia
kon@nw.math.msu.su

Vsevolod F. Lev[1]
Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel
seva@math.huji.ac.il

Received: 9/3/99, Accepted: 10/12/99, Published: 5/19/00

Abstract

We discuss three problems of the following kind: given a set $A \subseteq \mathbb{F}_p$ of $n := |A|$ residues modulo a prime p, how are the absolute values $|S_A(z)|$ of the corresponding exponential sums

$$S_A(z) := \sum_{a \in A} e^{2\pi i \frac{az}{p}}; \qquad z \in \mathbb{F}_p$$

distributed in the interval $[0, n]$?

1. Introduction

One of the most popular tools in number theory, exponential sums, are usually studied from the following point of view only: given a particular set A of $n = |A|$ residues, integers, or real numbers, show that the absolute values of the exponential sums corresponding to this set are small. In this note we adopt a more general standpoint, trying to understand the distribution of the absolute values of the exponential sums in the interval $[0, n]$. Moreover, we are interested not in the sets A of some special arithmetic structure, but rather in the common properties of the exponential sums, independent of the structure of A. This is primarily a survey note: we review several known results and pose some new problems.

We stick with the case of residues modulo a prime p. For a set $A \subseteq \mathbb{F}_p$ of $n = |A|$ residues we write

$$S_A(z) := \sum_{a \in A} e^{2\pi i \frac{az}{p}}; \qquad z \in \mathbb{F}_p.$$

(More generally, one can consider character sums in any locally compact Abelian group. Local compactness implies the existence of Haar measure on the group of characters, and we can ask

[1] Supported in part by the Edmund Landau Center for Research in Mathematical Analysis and Related Areas, sponsored by the Minerva Foundation (Germany)

"how many" characters with a given property are there.) To avoid trivialities, we often assume tacitly that $2 \le n \le p-1$.

The basic observation is that $0 < |S_A(z)| \le n$ and moreover, $|S_A(z)| = n$ if and only if $z = 0$. (The reason why $S_A(z)$ is not 0 is that it can be considered as a polynomial of a pth root of unity, and this polynomial is not divisible by the minimal polynomial $x^{p-1} + \cdots + x + 1$.) Furthermore, Parseval's identity gives

$$\sum_{z \in \mathbb{F}_p} |S_A(z)|^2 = np. \tag{1}$$

Below we address the following three questions.

1) As we have noticed, $|S_A(z)|$ are distinct from 0, but how close to 0 can they be?

2) How many of the p sums $|S_A(z)|$ can be close to 0?

3) How many of the p sums $|S_A(z)|$ can be close to n?

(The answer to the missed question "How large $|S_A(z)|$ can be?" is immediate: it can be equal to n, if $z = 0$, and plainly the next largest value is $|\sin(\pi n/p)/\sin(\pi/p)|$, attained when A is an arithmetic progression $\pmod p$.)

We discuss these three questions in Sections 2 – 4, respectively.

2. How Small Can Exponential Sums Be?

The first question of this sort was probably first raised in 1975 by Gerry Myerson (see [M86]), who introduced the function $f(n,N)$, the least absolute value of a sum of n Nth roots of unity. Myerson allowed the roots of unity to be equal and proved several estimates for the case of N even. In this note we confine ourselves to N prime and require the roots to be pairwise distinct.

Theorem 1 *Suppose that $A \subseteq \mathbb{F}_p$ is a set of $n = |A| \in [3, p-1]$ residues $\pmod p$, and let $z \in \mathbb{F}_p^\times$. Then*

$$|S_A(z)| > n^{-\frac{p-3}{4}}.$$

Proof. For any fixed $z_0 \in \mathbb{F}_p^\times$, the sum $S_A(z_0)$ is an algebraic integer of the norm $\prod_{z \in \mathbb{F}_p^\times} S_A(z)$. This product is, therefore, at least 1 in absolute value, whence by the arithmetic-geometric means inequality and (1) we have

$$\begin{aligned}1 \le \prod_{z\in\mathbb{F}_p^\times} |S(z)|^2 &= |S_A(z_0)|^4 \prod_{\substack{z\in\mathbb{F}_p^\times\\ z\neq\pm z_0}} |S(z)|^2 \\ &\le |S_A(z_0)|^4 \left(\frac{1}{p-3}\sum_{\substack{z\in\mathbb{F}_p^\times\\ z\neq\pm z_0}} |S(z)|^2\right)^{p-3} \\ &< |S_A(z_0)|^4 \left(\frac{n(p-n)}{p-3}\right)^{p-3} \\ &\le n^{p-3}\,|S_A(z_0)|^4.\end{aligned}$$

□

On the other hand, we were able to prove the following.

Theorem 2 *For any $n = 2^k < p/20$ (where k is a positive integer) there exists $A \subseteq \mathbb{F}_p$ of the cardinality n such that*

$$|S_A(1)| < n^{-\frac{\ln p}{2\ln 2}}.$$

Proof. Let $p' = (p-1)/2$ and define A to be the set of all the subset sums of

$$\{p'+1, p'+2, p'+4, \dots, p'+2^{k-1}\} \subseteq \mathbb{F}_p.$$

We first show that all these subset sums are distinct, and therefore $|A| = 2^k$.

We assume that

$$\sum_{i\in I}(p'+2^i) \equiv \sum_{j\in J}(p'+2^j) \pmod p \tag{2}$$

for two subsets $I, J \subseteq \{0, \dots, k-1\}$ and we prove that $I = J$. Define $\xi := \sum_{i\in I} 2^i$ and $\eta := \sum_{j\in J} 2^j$. Then

$$0 \le \xi, \eta, |I|, |J| \le 2^k - 1 < p/20$$

and (2) implies

$$\begin{aligned}2\xi - |I| &\equiv 2\eta - |J| \pmod p,\\ 2\xi - |I| &= 2\eta - |J|.\end{aligned}$$

Next, it is easily seen that

$$\begin{aligned}|I| &= \xi - \left\lfloor\frac{\xi}{2}\right\rfloor - \left\lfloor\frac{\xi}{4}\right\rfloor - \dots,\\ |J| &= \eta - \left\lfloor\frac{\eta}{2}\right\rfloor - \left\lfloor\frac{\eta}{4}\right\rfloor - \dots,\end{aligned}$$

whence

$$\xi + \left\lfloor \frac{\xi}{2} \right\rfloor + \left\lfloor \frac{\xi}{4} \right\rfloor + \dots = \eta + \left\lfloor \frac{\eta}{2} \right\rfloor + \left\lfloor \frac{\eta}{4} \right\rfloor + \dots .$$

As $x + \lfloor x/2 \rfloor + \lfloor x/4 \rfloor + \dots$ is a strictly increasing function of x, we obtain $\xi = \eta$ and therefore $I = J$.

It follows that

$$S_A(1) = \prod_{j=0}^{k-1} \left(1 + e^{2\pi i \frac{p' + 2^j}{p}} \right),$$

and the absolute value of this product is easy to estimate:

$$\begin{aligned} |S_A(1)| &= 2^k \prod_{j=0}^{k-1} \left| \cos \pi \, \frac{p - 1 + 2^{j+1}}{2p} \right| \\ &= 2^k \prod_{j=1}^{k} \left| \sin \frac{\pi}{2p} \left(2^j - 1 \right) \right| \\ &< \left(\frac{\pi}{p} \right)^k 2^{\frac{k(k+1)}{2}} \\ &= n^{-\frac{\ln(p/\pi\sqrt{2})}{\ln 2} + \frac{\ln n}{2 \ln 2}} \\ &< n^{-\frac{\ln p}{2 \ln 2}}. \end{aligned}$$

□

It is clear from the proof that $\ln p/(2\ln 2)$ in the exponent can be replaced with $(1 - \varepsilon) \ln p / \ln 2$ for any positive ε. However, the gap between the estimates of Theorems 1 and 2 makes refinements of this sort senseless.

3. How Many Small Sums Are There?

Suppose that $Z \subseteq \mathbb{F}_p$ is a set of residues such that $|S_A(z)|$ is "small" for all $z \in Z$. Then the sum $\sum_{z \in Z} |S_A(z)|^2$ is small also. We normalize this sum letting

$$G(Z) := \frac{1}{|Z|} \sum_{z \in Z} |S_A(z)|^2.$$

A way to express the fact that not too many of the exponential sums are small is to bound $G(Z)$ from below for $|Z|$ large enough. As $G(\mathbb{F}_p) = n$ by (1), one could expect that $G(Z) \gg n^c$ with a positive constant c and assuming that $|Z|$ is large. This, however, is not the case. In fact, it is easy to show (see Theorem 5 below) that for any $\varepsilon \in (0, 1)$, any positive integer n, and sufficiently large p, there exist A and Z with $|A| = n$ and $|Z| \geq (1 - \varepsilon)p$ such that $G(Z) \leq 1/\varepsilon$. Moreover, there is no $\delta > 0$ such that $G(Z) \geq \delta$ holds for all $A, Z \subseteq \mathbb{F}_p$ with $|Z| \geq p/2$ (see Theorem 6). It is reasonable to expect that $G(Z) \gg n^{-\delta}$ for any $\delta > 0$ and $|Z| > \delta p$; however, the estimate we were able to prove is considerably weaker.

Theorem 3 *Let $Z \subseteq \mathbb{F}_p$, and suppose that $|Z| \geq (1-\varepsilon)p$, where $\varepsilon \in (0,1)$. Then*

$$G(Z) > \frac{1}{e} n^{-\frac{\varepsilon}{1-\varepsilon}}.$$

Proof. Using the inequality between arithmetic and geometric means, we get

$$(G(Z))^{|Z|} \geq \prod_{z \in Z} |S_A(z)|^2 = \prod_{z \in \mathbb{F}_p} |S_A(z)|^2 \prod_{z \notin Z} |S_A(z)|^{-2}.$$

The first product in the right-hand side is $|S_A(0)|^2 = n^2$ times the norm of a non-zero algebraic integer, whence

$$(G(Z))^{|Z|} > \prod_{z \notin Z} |S_A(z)|^{-2}$$

and therefore using the arithmetic-geometric means inequality once again and taking into account (1) we obtain

$$(G(Z))^{-|Z|} < \left(\frac{1}{p-|Z|} \sum_{z \notin Z} |S_A(z)|^2 \right)^{p-|Z|} < \left(\frac{np}{p-|Z|} \right)^{p-|Z|},$$

$$G(Z) > \left(\frac{np}{p-|Z|} \right)^{-\frac{p-|Z|}{|Z|}}. \tag{3}$$

Write $\alpha = (p-|Z|)/|Z|$. Then

$$\left(\frac{p}{p-|Z|} \right)^{-\frac{p-|Z|}{|Z|}} = \left(1 + \frac{1}{\alpha} \right)^{-\alpha} > e^{-1},$$

and the result follows from (3) since

$$\frac{p-|Z|}{|Z|} \leq \frac{\varepsilon}{1-\varepsilon}.$$

□

A continuous analog of the quantity $G(Z)$ was considered by Pichorides, who proved the following.

Theorem 4 ([P80, Lemma 1]) *Let $S(z) = 1 + \sum_{j=1}^{k} a_j e^{2\pi i j z}$, where a_j are real coefficients. For a set $Z \subseteq [0,1)$ of measure $\mu(Z) > 0$ define*

$$G_1(Z) := \frac{1}{\mu(Z)} \int_Z |S(z)|\, dz.$$

Suppose that $\mu(Z) < 1$ and let $\bar{Z}$ be the complement of Z in $[0,1)$. Then

$$(G_1(Z))^{\mu(Z)} (G_1(\bar{Z}))^{\mu(\bar{Z})} \geq 1.$$

We now show that $G(Z)$ can be rather small even for $|Z|$ large.

Theorem 5 *For any $\varepsilon \in (0,1)$, any positive integer n, and p sufficiently large, there exist $A, Z \subseteq \mathbb{F}_p$ such that $|A| = n$, $|Z| \geq (1-\varepsilon)p$, and $G(Z) \leq 1/\varepsilon$.*

Proof. Consider the trigonometric polynomial

$$P(x) = \sum_{j=0}^{n-1} e^{2\pi i j x}.$$

For $0 < x < 1/2$ we have

$$|P(x)| = \left| \frac{e^{2\pi i n x} - 1}{e^{2\pi i x} - 1} \right| = \frac{|\sin(\pi n x)|}{\sin(\pi x)} \leq \frac{1}{\sin(\pi x)} < \frac{1}{2x},$$

whence

$$\int_{\varepsilon/2}^{1/2} |P(x)|^2 dx < \int_{\varepsilon/2}^{1/2} \frac{dx}{4x^2} = \frac{1}{2\varepsilon} - \frac{1}{2}. \tag{4}$$

Denote

$$E = [\varepsilon/2, 1-\varepsilon/2]$$

and

$$E_\delta = [\varepsilon/2 - \delta, 1 - \varepsilon/2 + \delta]$$

for $\delta > 0$. By (4),

$$\int_E |P(x)|^2 dx = 2 \int_{\varepsilon/2}^{1/2} |P(x)|^2 dx < \frac{1}{\varepsilon} - 1,$$

and therefore for sufficiently small $\delta > 0$ we have

$$\int_{E_\delta} |P(x)|^2 dx < \frac{1}{\varepsilon} - 1. \tag{5}$$

Let $A = \{0, \ldots, n-1\}$. For any p put $Z = \{z : z/p \in E_\delta\}$, so that

$$|Z| \geq (1-\varepsilon)p \tag{6}$$

for p large enough. Also,

$$\lim_{p\to\infty} \sum_{z \in Z} |S_A(z)|^2/p = \int_{E_\delta} |P(x)|^2 dx,$$

and it follows from (5) that for sufficiently large p

$$\sum_{z \in Z} |S_A(z)|^2 < p\left(\frac{1}{\varepsilon} - 1\right). \tag{7}$$

Inequalities (6) and (7) readily imply the required estimate $G(Z) \leq 1/\varepsilon$. □

The following theorem is the main result of [K97].

Theorem 6 (cf. [K97]) *For any $\delta > 0$ there exist a prime number p and sets $A, Z \subseteq \mathbb{F}_p$ such that $|Z| > p/2$ and $G(Z) < \delta$.*

Sketch of proof. The main part of the proof is a construction of a trigonometric polynomial $P(x) = \sum_{a\in A} e^{2\pi iax}$ (where A is a finite set of integers) and a set $E \in [0,1]$ such that E is the union of finitely many segments,

$$\mu(E) > 1/2, \tag{8}$$

and

$$\int_E |P(x)|^2 dx < \delta/2. \tag{9}$$

Once P and E are constructed, it is easy to complete the proof using the same kind of argument as in Theorem 5.

We can assume that $\delta < 1$. Let $\eta_0, \eta_1, \ldots$ be independent random variables, distributed uniformly in $[0,1]$. We define $\xi_j = 2\cos(\pi\eta_j)$ and $\psi_j = \ln|\xi_j|$, and we observe that ψ_j are independent and satisfy

$$\mathbf{E}\psi_j = 0,\ \mathbf{E}|\psi_j|^3 < \infty.$$

It follows from the Berry-Essen theorem (see [B76, Theorem 12.4]) that there exists a constant $C > 0$ such that for any positive integer m

$$\Pr\left(\sum_{j=0}^{m-1}\psi_j \le C\right) > 1/2 \tag{10}$$

and moreover,

$$\Pr\left(-\ln(4/\delta) \le \sum_{j=0}^{m-1}\psi_j \le C\right) < \delta/(4e^{2C}) \tag{11}$$

for m sufficiently large.

We denote by (Ω,ν) the probability space and by $F \subset \Omega$ the event $\sum_{j=0}^{m-1}\psi_j \le C$. By (10),

$$\nu(F) > 1/2 \tag{12}$$

and from (11) (see [K97] for details)

$$\int_F \exp\left(\sum_{j=0}^{m-1}\psi_j\right) d\nu < \delta/2,$$

or equivalently

$$\int_F \prod_{j=0}^{m-1}|\xi_j| d\nu < \delta/2. \tag{13}$$

Using weak convergence of the distribution function of the random vectors $(2\cos(2\pi x),$ $2\cos(2\pi l x), \ldots, 2\cos(2\pi l^{m-1}x))$ to the distribution function of $(\xi_0, \xi_1, \ldots, \xi_{m-1})$ as $l \to \infty$ (cf. [K97])), we get weak convergence of the distribution function of $\prod_{j=0}^{m-1} 2\cos(2\pi l^j x)$ to the distribution function of $\prod_{j=0}^{m-1} \xi_j$ as $l \to \infty$. Therefore, for the 2^m-term trigonometric polynomial

$$P(x) = \prod_{j=0}^{m-1} \left(1 + e^{2\pi i l^j x}\right)$$

and for the set

$$E = \{x \in [0,1] : |P(x)| \le e^C\},$$

using the identity

$$|P(x)| = \prod_{j=0}^{m-1} |2\cos(\pi l^j x)|$$

one can deduce from (12) and (13) the required inequalities (8) and (9), provided that l is large enough. □

Analysis of the proof shows that if n is a power of 2, then one can have $G(Z) \ll (\ln n)^{-1/2}$ with $|Z| > p/2$ and $G(Z) \ll \exp(-c(\alpha)(\ln n)^{1/2})$ with $|Z| \ge \alpha p$, $0 < \alpha < 1/2$. Also, for arbitrary $n \ge 2$ we can give examples with the same estimates for $G(Z)$ under weaker restrictions for $|Z|$: $G(Z) \ll (\ln n)^{-1/2}$ with $|Z| > p/4$ and $G(Z) \ll \exp(-c(\alpha)(\ln n)^{1/2})$ with $|Z| \ge \alpha p$, $0 < \alpha < 1/4$.

4. Large Exponential Sums

For exponential sums corresponding to a set A of *integers*, a rather precise estimate for the number of “large” sums was obtained by Yudin in [Y73]. Yudin proved that

$$\operatorname{mes}\{z \in [0,1) \colon |S_A(z)| > (1-\varepsilon)n\} \le \frac{2\sqrt{6}}{\pi}\,\frac{1}{n}\,\varepsilon^{1/2}(1+o(1)), \tag{14}$$

where

$$S_A(z) = \sum_{a \in A} e^{2\pi i a z}; \quad z \in \mathbb{R}$$

and assuming that $n \to \infty$ and $\varepsilon = o(1)$. Equality is attained when A is an arithmetic progression. In [B99], Besser replaced the assumption $\varepsilon = o(1)$ by $\varepsilon < c$ with an absolute constant $c > 0$; this required numerous fresh ideas and the final result differs considerably from (14).

Yudin’s argument was based on a “rearrangement theorem” due to Hardy and Littlewood. In [L00, Theorem 1], the second of the present authors was able to obtain residue analogs of the results of Hardy and Littlewood, which allowed him to extend Yudin’s theorem onto the residues case.

We now return back to our original notation, assuming $A \subseteq \mathbb{F}_p$ and $z \in \mathbb{F}_p$. It turns out that a convenient way to measure the number of large exponential sums is provided by the function

$$T_A(\varphi) := \{z \in \mathbb{F}_p^\times : |S_A(z)| > n\cos\varphi\}; \quad 0 \le \varphi \le \pi/2.$$

Evidently, $T_A(\varphi)$ is piecewise constant, monotonically increasing, and satisfies $T_A(0) = 0$ and $T_A(\pi/2) = p-1$. A non-trivial property of $T_A(\varphi)$ which explains why it arises naturally in this context is its sup-additivity, expressed in the following lemma.

Lemma 1 ([L00, Lemma 1]) *Suppose that* $\varphi_1, \varphi_2 \ge 0$ *and* $\varphi_1 + \varphi_2 \le \pi/2$. *Then*

$$T_A(\varphi_1 + \varphi_2) \ge \min\{T_A(\varphi_1) + T_A(\varphi_2),\, p-1\}.$$

(A parallel lemma for sets of integers is implicit in [Y73].)

Assume for a moment that the assertion of the lemma can be strengthened to

$$T_A(\varphi_1 + \varphi_2) \ge T_A(\varphi_1) + T_A(\varphi_2). \tag{15}$$

By induction, it follows then that $T_A(j\varphi_0) \ge jT_A(\varphi_0)$ provided $j\varphi_0 \le \pi/2$. Choosing $j = \lfloor \varphi/\varphi_0 \rfloor$ and taking into account that $T_A(\varphi) \ge T_A(j\varphi_0)$ as T_A is increasing, we obtain

Corollary 1 ([L00, Lemma 2]) *Suppose that* $0 < \varphi, \varphi_0 \le \pi/2$. *Then*

$$T_A(\varphi) \ge \left\lfloor \frac{\varphi}{\varphi_0} \right\rfloor T_A(\varphi_0).$$

Though it can be shown that (15) *does not* hold in general, Corollary 1 is true and is established in [L00]. In conjunction with a rearrangement theorem for residues, it was used to prove the following analog of (14).

Theorem 7 ([L00, Theorem 5]) *For any set* $A \subseteq \mathbb{F}_p$ *of* $n = |A| \ge 4$ *residues modulo a prime* p *and any* $\varphi \in [0, \pi/6]$ *we have*

$$T_A(\varphi) \le \frac{2\sqrt{3}}{\pi}\,\frac{p}{n}\,\varphi\,(1+n^{-2})(1+2\varphi^{2/3}).$$

This theorem is sharp in the sense that equality is attained asymptotically (for $n \to \infty$ and $\varphi \to 0$) if A is an arithmetic progression modulo p.

We conclude by outlining the proof of Theorem 7.

Sketch of proof. For brevity we drop below the subscript A in $S_A(z)$ and $T_A(\varphi)$, and we define

$$A_0 := \{0, \dots, n-1\},\ S_0(z) := S_{A_0}(z),\ T_0(z) := T_{A_0}(z).$$

For $k \ge 1$ consider the moments

$$\frac{1}{p}\sum_{z\in\mathbb{F}_p} |S(z)|^{2k} \quad \text{and} \qquad \frac{1}{p}\sum_{z\in\mathbb{F}_p} |S_0(z)|^{2k}.$$

The former is the number of solutions of the equation $a_1 + \cdots + a_k = a'_1 + \cdots + a'_k$ in the variables $a_i, a'_i \in A$, the latter is the number of solutions of the same equation in the variables $a_i, a'_i \in A_0$. By [L00, Theorem 1], the number of solution is maximized when the variables range over an arithmetic progression; thus,

$$\sum_{z\in\mathbb{F}_p} |S(z)|^{2k} \le \sum_{z\in\mathbb{F}_p} |S_0(z)|^{2k},$$

and partial integration allows one to rewrite it as

$$\int_0^{\pi/2} T(\varphi)\cos^{2k-1}\varphi\,\sin\varphi\,d\varphi \le \int_0^{\pi/2} T_0(\varphi)\cos^{2k-1}\varphi\,\sin\varphi\,d\varphi.$$

Furthermore, $T_0(\varphi)$ can be estimated explicitly and it can be shown that the integral at the right does not exceed

$$\sqrt{\frac{6}{\pi}}\,\frac{p}{n}\,(2k)^{-3/2}(1+o(1))$$

(as $n, k \to \infty$). As to the integral at the left, we use Corollary 1 to estimate it from below by

$$T(\varphi_0)\int_0^{\pi/2}\left\lfloor\frac{\varphi}{\varphi_0}\right\rfloor\cos^{2k-1}\varphi\,\sin\varphi\,d\varphi \ge \frac{T(\varphi_0)}{\varphi_0}\sqrt{\frac{\pi}{2}}\,(2k)^{-3/2}(1+o(1))$$

for any fixed φ_0. Therefore,

$$\frac{T(\varphi_0)}{\varphi_0}\sqrt{\frac{\pi}{2}}\,(2k)^{-3/2} \le \sqrt{\frac{6}{\pi}}\,\frac{p}{n}\,(2k)^{-3/2}(1+o(1))$$

and the result follows. □

Acknowledgment

The work on this paper was initiated in July 1999 when the authors attended the "Paul Erdős and his mathematics" conference in Budapest and its satellite workshop on combinatorial number theory. Our visit was partially supported by the Erdős center. It is our pleasure to thank the Erdős center for its hospitality and the excellent working environment.

References

[B76]R. N. Bhattacharya, R. Rao, Normal approximation and asymptotic expansions, John Wiley & Sons, New York, 1976.

[B99] A. Besser, Sets of integers with large trigonometric sums, *Astérisque* **258** (1999), 35–76.

[K97] S. V. Konyagin, On a question of Pichorides, *C. R. Acad. Sci. Paris Ser. I Math.* **324** (1997), 385–388.

[L98] V.F. Lev, On the number of solutions of a linear equation over finite sets, *J. Comb. Theory, Ser. A* **83** (1998), 251–267.

[L00] V.F. Lev, Linear equations over $\mathbb{F}_p$ and moments of exponential sums, Duke Math. Journal, *to appear.*

[M86] G. Myerson, How small can a sum of roots of unity be? *American Math. Monthly* **93** (1986) , 457–459.

[P80] S.K. Pichorides, On the L^1-norm of exponential sums, *Annales de l'Inst. Fouier* **30** (2) (1980), 79–89.

[Y73] A.A. Yudin, On the measure of large values of a trigonometric sum, *in:* Number Theory (under the edition of G.A. Freiman, A.M. Rubinov, E.V. Novosyolov), Kalinin State Univer., Moscow (1973), 163–174.