LINEAR EQUATIONS OVER $\mathbb{Z}/p\mathbb{Z}$ AND MOMENTS OF EXPONENTIAL SUMS

VSEVOLOD F. LEV*

Preprint No. 1
1998/9

Abstract. Our principal results (in a simplified form) are as follows.

Theorem. For p prime, the number of solutions of the equation

$$c_1a_1 + \cdots + c_ka_k = \lambda; \quad a_i \in A_i$$

(where $c_i \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $\lambda \in \mathbb{Z}/p\mathbb{Z}$ are fixed coefficients, and the variables a_i range over sets $A_i \subseteq \mathbb{Z}/p\mathbb{Z}$ of pre-assigned cardinalities) does not exceed that when A_i are arithmetic progressions modulo p sharing a common difference, $c_i = 1$, and λ is chosen appropriately.

This readily implies an integer version, which strengthens a result of Gabriel, Hardy and Littlewood.

Theorem. Let A be a set of $n = |A|$ residues modulo a prime p. For $z \in \mathbb{Z}/p\mathbb{Z}$, write

$$S_A(z) = \sum_{a\in A} e^{2\pi i \frac{az}{p}}.$$

Then for $\varepsilon > 0$ we have

$$\#\{z \in (\mathbb{Z}/p\mathbb{Z})^\times : |S_A(z)| > n(1-\varepsilon)\} < \frac{2\sqrt{6}}{\pi}\,\frac{p}{n}\,\varepsilon^{1/2}\,(1+o(1)),$$

provided $n \to \infty$ and $\varepsilon \to 0$. This bound is attained when A is an arithmetic progression modulo p.

This implies an integer version which is due to Yudin.

1. Historical background and summary of results. Inequalities, rearrangements and linear equations over finite sets

The scalar product $\sum \mathfrak{a}_{\sigma(i)}\mathfrak{b}_{\tau(i)}$ of the rearrangements $\{\mathfrak{a}_{\sigma(i)}\}$ and $\{\mathfrak{b}_{\tau(i)}\}$ of two non-negative real sequences $\{\mathfrak{a}_i\}$ and $\{\mathfrak{b}_i\}$ is maximized when these rearrangements are similarly ordered. The concluding chapter of [HLP88] deals with generalizations of this well-known fact onto products of three and more sequences and onto "rearrangements of functions". The central result for sequences can be stated as follows.

1991 *Mathematics Subject Classification.* Primary: 11B75; Secondary: 11D04, 11L07, 11P99, 11B25, 11D72.

*nPartially supported by the Edmund Landau Center for Research in Mathematical Analysis and Related Areas, sponsored by the Minerva Foundation (Germany).

Theorem 1 ([HLP88, Theorem 374]). *For $j = 1, \dots, k$ let $\{\mathfrak{a}_i^{(j)}\}_{i=-\infty}^{\infty}$ be sequences of non-negative real numbers, such that only a finite number of elements of each sequence is distinct from zero. Suppose that*

$$\mathfrak{a}_0^{(1)} \ge \mathfrak{a}_1^{(1)} \ge \mathfrak{a}_{-1}^{(1)} \ge \mathfrak{a}_2^{(1)} \ge \mathfrak{a}_{-2}^{(1)} \ge \cdots,$$
$$\mathfrak{a}_0^{(2)} \ge \mathfrak{a}_{-1}^{(2)} \ge \mathfrak{a}_1^{(2)} \ge \mathfrak{a}_{-2}^{(2)} \ge \mathfrak{a}_2^{(2)} \ge \cdots,$$
$$\mathfrak{a}_0^{(j)} \ge \mathfrak{a}_1^{(j)} = \mathfrak{a}_{-1}^{(j)} \ge \mathfrak{a}_2^{(j)} = \mathfrak{a}_{-2}^{(j)} \ge \cdots \quad \text{for} \quad 3 \le j \le k.$$

Then for any system of permutations $\sigma^{(j)}\colon \mathbb{Z} \to \mathbb{Z}$ $(j = 1, \dots, k)$ we have

$$\sum_{i_1+\dots+i_k=0} \mathfrak{a}_{\sigma^{(1)}(i_1)}^{(1)} \cdots \mathfrak{a}_{\sigma^{(k)}(i_k)}^{(k)} \le \sum_{i_1+\dots+i_k=0} \mathfrak{a}_{i_1}^{(1)} \cdots \mathfrak{a}_{i_k}^{(k)}.$$

This theorem is due to Gabriel [G32]; it generalizes an earlier result of Hardy and Littlewood [HL28] where *all* sequences $\{\mathfrak{a}^{(j)}\}$ (including those with $j = 1$ and $j = 2$) were required to be symmetrical.

An important particular case, on which the proof of Theorem 1 in its full generality relies, is that of $\{\mathfrak{a}^{(j)}\}$ being the indicator functions of finite sets of integers A_j:

$$\mathfrak{a}_i^{(j)} = \begin{cases} 1, & \text{if } i \in A_j, \\ 0, & \text{if } i \notin A_j. \end{cases}$$

Theorem 1 reduces then to

Theorem 2. *Let $A_1, \dots, A_k$ be finite non-empty sets of integers of the cardinalities $n_j = |A_j|$ such that $n_3, \dots, n_k$ are odd. Define $\bar{A}_j$ to be arithmetic progressions of difference one, balanced around zero as follows:*

$$\bar{A}_1 = [-(n_1 - 1 - \delta_1)/2, (n_1 - 1 + \delta_1)/2],$$
$$\bar{A}_2 = [-(n_2 - 1 + \delta_2)/2, (n_2 - 1 - \delta_2)/2],$$
$$\bar{A}_j = [-(n_j - 1)/2, (n_j - 1)/2] \quad (j = 3, \dots, k),$$

where for $j = 1, 2$ we put

$$\delta_j = \begin{cases} 0, & \textit{if } n_j \textit{ is odd}, \\ 1, & \textit{if } n_j \textit{ is even} \end{cases}$$

Then the number of solutions of the equation

$$a_1 + \dots + a_k = 0$$

in the variables $a_j \in A_j$ does not exceed the number of solutions of this equation in the variables $a_j \in \bar{A}_j$.

In [L98], we disposed of the restrictions on the parity of $|A_j|$ in this latter theorem and somewhat strengthened it at the same time. (It is worth noting that in Theorem 1 these parity restrictions are principal and cannot be dropped.) To formulate the results of [L98], we need some notation.

By a *balanced* set of integers we mean a non-empty block of consecutive integers of the form $\bar{A} = [-\alpha, \alpha + \delta]$, where $\alpha \geq 0$ and $\delta \in \{0, \pm 1\}$. Obviously, δ is uniquely defined by the set $\bar{A}$ and we write $\delta = \delta(\bar{A})$. If the cardinality $|\bar{A}|$ is odd then necessarily $\delta(\bar{A}) = 0$; if $|\bar{A}|$ is even, there are two possibilities: either $\delta(\bar{A}) = 1$, or $\delta(\bar{A}) = -1$. If A is a finite non-empty set of integers, then $\bar{A}$ is used for a balanced set of the same cardinality as A.

For $\lambda \in \mathbb{Z}$ we denote by $N_\lambda(A_1, \dots, A_k)$ the number of representations $\lambda = a_1 + \dots + a_k$ with $a_j \in A_j$.

One of the main results of [L98] in its weak form is

Theorem 3. *Let $A_1, \dots, A_k$ be finite non-empty sets of integers, and assume that $\bar{A}_1, \dots, \bar{A}_k$ are balanced and satisfy $|\delta(\bar{A}_1) + \dots + \delta(\bar{A}_k)| \leq 1$. Then*

$$N_\lambda(A_1, \dots, A_k) \leq N_0(\bar{A}_1, \dots, \bar{A}_k)$$

for any $\lambda \in \mathbb{Z}$.

Given finite non-empty $A_1, \dots, A_k \subseteq \mathbb{Z}$, we write $\{\nu_i(A_1, \dots, A_k)\}_{i=1}^{\infty}$ for the descending rearrangement of the sequence $\{N_\lambda(A_1, \dots, A_k)\}_{\lambda=-\infty}^{\infty}$; thus,

$$\nu_1(A_1, \dots, A_k) = \max_{\lambda \in \mathbb{Z}} N_\lambda(A_1, \dots, A_k),$$
$$\sum_{i=1}^{\infty} \nu_i(A_1, \dots, A_k) = \sum_{\lambda=-\infty}^{\infty} N_\lambda(A_1, \dots, A_k) = |A_1| \cdots |A_k|,$$

and the number of indices i such that $\nu_i(A_1, \dots, A_k) > 0$ is the cardinality of the sumset $A_1 + \dots + A_k$. Furthermore, we write $(A_1, \dots, A_k) \prec (B_1, \dots, B_k)$ if $A_1, \dots, A_k$ and $B_1, \dots, B_k$ are two systems of sets such that

$$\sum_{i=1}^{m} \nu_i(A_1, \dots, A_k) \leq \sum_{i=1}^{m} \nu_i(B_1, \dots, B_k) \tag{1}$$

for all positive integers m. In particular, when $m = 1$ this implies

$$\max_{\lambda \in \mathbb{Z}} N_\lambda(A_1, \dots, A_k) \leq \max_{\lambda \in \mathbb{Z}} N_\lambda(B_1, \dots, B_k).$$

Example. Let $A_1 = \{0, 2\}$, $A_2 = \{1, 5, 7\}$, $\bar{A}_1 = \{0, 1\}$, and $\bar{A}_2 = \{-1, 0, 1\}$. Then $\{\nu_i(A_1, A_2)\} = \{2, 1, 1, 1, 1, 0, \dots\}$ and $\{\nu_i(\bar{A}_1, \bar{A}_2)\} = \{2, 2, 1, 1, 0, \dots\}$, hence $(A_1, A_2) \prec (\bar{A}_1, \bar{A}_2)$.

The strong form of Theorem 3, also given in [L98], is the following.

Theorem 4. *Let $A_1, \dots, A_k$ be finite non-empty sets of integers, and assume that $\bar{A}_1, \dots, \bar{A}_k$ are balanced and satisfy $|\delta(\bar{A}_1) + \dots + \delta(\bar{A}_k)| \le 1$. Then*

$$(A_1, \dots, A_k) \prec (\bar{A}_1, \dots, \bar{A}_k).$$

Moreover, writing for brevity N_λ for $N_\lambda(\bar{A}_1, \dots, \bar{A}_k)$ we have:

– *if $0 \le \delta(\bar{A}_1) + \dots + \delta(\bar{A}_k) \le 1$, then*

$$N_0 \ge N_1 \ge N_{-1} \ge N_2 \ge N_{-2} \ge \cdots ;$$

– *if $-1 \le \delta(\bar{A}_1) + \dots + \delta(\bar{A}_k) \le 0$, then*

$$N_0 \ge N_{-1} \ge N_1 \ge N_{-2} \ge N_2 \ge \cdots .$$

That is, if $\bar{\lambda}_1, \dots, \bar{\lambda}_m$ are the first m terms of either the sequence $\{0, 1, -1, 2, -2, \dots\}$ or the sequence $\{0, -1, 1, -2, 2, \dots\}$ (depending on the sign of the sum $\delta(\bar{A}_1) + \dots + \delta(\bar{A}_k)$), and if $\lambda_1, \dots, \lambda_m$ are any m pairwise distinct integers, then

$$N_{\lambda_1}(A_1, \dots, A_k) + \dots + N_{\lambda_m}(A_1, \dots, A_k) \\ \le N_{\bar{\lambda}_1}(\bar{A}_1, \dots, \bar{A}_k) + \dots + N_{\bar{\lambda}_m}(\bar{A}_1, \dots, \bar{A}_k).$$

Remark. Clearly, the first assertion of Theorem 4 remains valid when $\bar{A}_j$ are arbitrary arithmetic progressions, sharing a common difference — not necessarily balanced around zero and of difference one.

We further proceeded in [L98] to obtain analogs of Theorems 3 and 4 when A_j are sets of residues modulo a prime p, but were only able to bound $\max_{\lambda \in \mathbb{Z}} N_\lambda(A_1, \dots, A_k)$ by an analytic expression, the order of magnitude of which coincides with the order of magnitude of $N_0(\bar{A}_1, \dots, \bar{A}_k)$. In the present paper we obtain a sharp result of this sort, specifically, Theorem A below. We note that the definitions of a balanced set and the ν-sequence are transfered onto the residues case without any difficulties; the only difference is that the latter is now a finite sequence of p terms, and accordingly, $(A_1, \dots, A_k) \prec (B_1, \dots, B_k)$ means that (1) holds for $m = 1, \dots, p$. Alternatively, one can regard $\{\nu_i(A_1, \dots, A_k)\}$ as an infinite sequence, completing it by zeros.

Theorem A. *Let $A_1, \dots, A_k \subseteq \mathbb{Z}/p\mathbb{Z}$ be non-empty sets of residues modulo a prime $p \ge 3$, and assume that $\bar{A}_1, \dots, \bar{A}_k$ are balanced and satisfy $|\delta(\bar{A}_1) + \dots + \delta(\bar{A}_k)| \le 1$. Then*

$$(A_1, \dots, A_k) \prec (\bar{A}_1, \dots, \bar{A}_k).$$

Moreover, writing for brevity N_λ for $N_\lambda(\bar{A}_1, \dots, \bar{A}_k)$ we have:

– *if $0 \le \delta(\bar{A}_1) + \dots + \delta(\bar{A}_k) \le 1$, then*

$$N_0 \ge N_1 \ge N_{-1} \ge N_2 \ge N_{-2} \ge \dots \ge N_{p'} \ge N_{-p'};$$

– *if* $-1 \le \delta(\bar{A}_1) + \dots + \delta(\bar{A}_k) \le 0$, *then*

$$N_0 \ge N_{-1} \ge N_1 \ge N_{-2} \ge N_2 \ge \dots \ge N_{-p'} \ge N_{p'},$$

where $p' = (p-1)/2$.

We show in Section 3 that the first assertion of Theorem A is equivalent to a well-known result of Pollard [P74], while the second assertion is a consequence of the first one.

Remark. Theorem A implies Theorem 4. To see this, given integer sets $A_1, \dots, A_k$ choose p large enough and consider the canonical images of A_j in $\mathbb{Z}/p\mathbb{Z}$.

2. Historical background and summary of results. Moments and large values of exponential sums

For a set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ of $n = |A|$ residues modulo a prime p, let

$$S(z) = \sum_{a \in A} e^{2\pi i \frac{az}{p}} \qquad (z \in \mathbb{Z}/p\mathbb{Z})$$

denote the exponential sums of A. The number of solutions of the linear equation

$$a_1 + \dots + a_k = \lambda \quad (a_i \in A) \tag{2}$$

is

$$\frac{1}{p} \sum_{z=0}^{p-1} S^k(z) e^{-2\pi i \frac{\lambda z}{p}},$$

and for k large the terms that determine the behavior of this sum are those with $|S(z)|$ large. In [L98], we gave an estimate for the number of such z, which allowed us to estimate the number of solutions of (2). Now, armed with Theorem A that establishes a precise bound for the number of solutions of equations of the type (2), we can reverse the procedure and obtain a sharp estimate for the number of z such that $|S(z)|$ is large. In doing so, we follow in general the approach of Yudin [Y73], who solved the parallel problem for integer sets; the technical details are quite different, however.

It is convenient to measure the number of large exponential sums by the function $T(\varphi)$, defined by

$$T(\varphi) := \#\{z \in (\mathbb{Z}/p\mathbb{Z})^{\times} \colon |S(z)| > n \cos\varphi\}\,; \quad 0 \le \varphi \le \pi/2.$$

Thus, $T(\varphi)$ is a non-decreasing, piecewise constant function such that $T(0) = 0$ and $T(\pi/2) = p - 1$. The reason for introducing $T(\varphi)$ for this purpose is clear from the following lemma.

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

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

for any non-empty $A \subseteq \mathbb{Z}/p\mathbb{Z}$.

This lemma follows easily from an observation of Yudin and was first used in [L98]. For the benefit of the reader we will reproduce its proof (which is just a few lines long) in Section 5.

There is an interesting problem associated with Lemma 1. Numerical evidence suggests that perhaps, the condition $\varphi_1 + \varphi_2 \le \pi/2$ automatically implies $T(\varphi_1) + T(\varphi_2) \le p - 1$, which means that the assertion of the lemma can be written in a simpler and nicer form

$$T(\varphi_1 + \varphi_2) \ge T(\varphi_1) + T(\varphi_2).$$

With a little thinking, the problem can be reformulated as follows.

Problem. Is it true that

$$\#\{z \in (\mathbb{Z}/p\mathbb{Z})^\times : |S(z)| < n_1\} \;\ge\; \#\{z \in (\mathbb{Z}/p\mathbb{Z})^\times : |S(z)| > n_2\}$$

for any positive real numbers $n_1 < n_2$, satisfying $n_1^2 + n_2^2 = n^2$?

¿From Lemma 1 we will derive the following property of the function $T(\varphi)$.

Lemma 2. *Suppose that* $n = |A| \ge 4$. *Then for any* $0 < \varphi, \varphi_0 \le \pi/2$ *we have*

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

We note that the integer part brackets cannot be dropped in the formulation of the lemma; indeed, the function $T(\varphi)/\varphi$ is not monotonic.

Remark . Plainly, a positive answer in the above problem would make the proof of Lemma 2 immediate: by induction, we would have $T(j\varphi_0) \ge jT(\varphi_0)$ provided $j\varphi_0 \le \pi/2$, and we choose $j = \lfloor \varphi/\varphi_0 \rfloor$.

Though Lemma 2 is implicit in [L98], we prefer to give an explicit formulation and an independent explicit proof.

We will prove two estimates for the number of large sums $S(z)$. The first is indirect but may turn more useful.

Theorem B. *For any set* $A \subseteq \mathbb{Z}/p\mathbb{Z}$ *of* $n = |A| \ge 3$ *residues modulo a prime* p *and any even integer* $k \ge 2$ *we have*

$$\sum_{z=1}^{p-1} |S(z)|^k \le \sqrt{\frac{6}{\pi k}}\, n^{k-1}\, p\,(1 + n^{-2})(1 + 4k^{-1}).$$

(In fact, we give a somewhat better reminder term, provided $k \geq 16$ — see the proof in Section 5.) It is interesting to compare the estimate of Theorem B with the trivial estimate $\sum |S(z)|^k \leq n^{k-1}p$.

The second is a direct estimate.

Theorem C. *For any set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ of $n = |A| \geq 4$ residues modulo a prime p and any $\varphi \in [0, \pi/6]$ we have*

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

In Section 4 we consider the case of an arithmetic progression $A = \{0, \dots, n-1\}$ and show that Theorems B and C are best possible save for the reminder terms.

3. Pollard's theorem and the proof of Theorem A

Theorem 5 (Pollard, [P74, Theorem 1])**.** *Let $A_1, \dots, A_k \subseteq \mathbb{Z}/p\mathbb{Z}$ be non-empty sets of residues modulo a prime $p \geq 3$, and assume that $\bar{A}_1, \dots, \bar{A}_k$ are arithmetic progressions modulo p sharing a common difference and such that $|A_j| = |\bar{A}_j|$ $(j = 1, \dots, k)$. Write $\nu_i = \nu_i(A_1, \dots, A_k)$, $\bar{\nu}_i = \nu_i(\bar{A}_1, \dots, \bar{A}_k)$, and define*

$$f(t) := \sum_{i=1}^{\infty} \min\{\nu_i, t\}, \quad \bar{f}(t) := \sum_{i=1}^{\infty} \min\{\bar{\nu}_i, t\}; \qquad t \geq 0.$$

Then

$$f(t) \geq \bar{f}(t)$$

for any non-negative real t.

Remark. For $k = 2$, this theorem is better known in an apparently different, but equivalent form: writing K_i for the number of elements $c \in A_1 + A_2$ that have at least i representations as $c = a_1 + a_2$ $(a_j \in A_j)$, for any integer $1 \leq t \leq \min\{|A_1|, |A_2|\}$ we have

$$K_1 + \cdots + K_t \geq t \min\{|A_1| + |A_2| - t, p\}.$$

The first assertion of Theorem A follows immediately from Pollard's theorem and our next lemma.

Lemma 3. *Let $\nu_1 \geq \nu_2 \geq \cdots$ and $\bar{\nu}_1 \geq \bar{\nu}_2 \geq \cdots$ be two sequences of non-negative real numbers, such that $\nu_1 + \nu_2 + \cdots = \bar{\nu}_1 + \bar{\nu}_2 + \cdots$, and only a finite number of elements of each sequence is distinct from zero. For non-negative real t define $f(t)$ and $\bar{f}(t)$ as in Theorem 5. Then the two following assertions are equivalent:*

(a) *$\nu_1 + \cdots + \nu_m \leq \bar{\nu}_1 + \cdots + \bar{\nu}_m$ for any $m = 1, 2, \dots$;*

(b) *$f(t) \geq \bar{f}(t)$ for any $t \geq 0$.*

Proof. Put $\sigma = \nu_1+\nu_2+\dots = \bar\nu_1+\bar\nu_2+\cdots$, so that both $f(t)$ and $\bar f(t)$ are continuous, non-decreasing functions, satisfying $f(0) = \bar f(0) = 0$, $f(\nu_1) = \bar f(\bar\nu_1) = \sigma$ and $\sigma = \max f = \max \bar f$.

i) We first show that (a) implies (b). We assume that $t \le \nu_1$, as otherwise $f(t) = \sigma \ge \bar f(t)$. Thus, $t \le \bar\nu_1$ also, and there exist indices $i, j \ge 1$ such that

$$\nu_{i+1} \le t \le \nu_i, \quad \bar\nu_{j+1} \le t \le \bar\nu_j,$$

whence

$$f(t) = \sigma - \nu_1 - \dots - \nu_i + it, \quad \bar f(t) = \sigma - \bar\nu_1 - \dots - \bar\nu_j + jt.$$

What we want to prove is, therefore,

$$\nu_1 + \dots + \nu_i - it \le \bar\nu_1 + \dots + \bar\nu_j - jt,$$

and we show that, moreover,

$$\bar\nu_1 + \dots + \bar\nu_i - it \le \bar\nu_1 + \dots + \bar\nu_j - jt. \tag{3}$$

Indeed, if $i \le j$ then (3) is equivalent to

$$(j-i)t \le \bar\nu_{i+1} + \dots + \bar\nu_j,$$

which is evident in view of $t \le \bar\nu_j \le \dots \le \bar\nu_{i+1}$; otherwise, $i \ge j$ and (3) is equivalent to

$$(i-j)t \ge \bar\nu_{j+1} + \dots + \bar\nu_i,$$

which follows from $t \ge \bar\nu_{j+1} \ge \dots \ge \bar\nu_i$.

ii) We now use induction by m to show that (b) implies (a). First, we have $\sigma = \bar f(\bar\nu_1) \le f(\bar\nu_1) \le \sigma$, whence $f(\bar\nu_1) = \sigma$ and therefore $\nu_1 \le \bar\nu_1$. Next, assuming $\nu_1 + \dots + \nu_m \le \bar\nu_1 + \dots + \bar\nu_m$ for some $m \ge 1$, we show that

$$\nu_1 + \dots + \nu_{m+1} \le \bar\nu_1 + \dots + \bar\nu_{m+1}. \tag{4}$$

Indeed, this is obvious if $\nu_{m+1} \le \bar\nu_{m+1}$, while otherwise $\nu_{m+1} \ge \bar\nu_{m+1}$ and then

$$\begin{aligned} \sigma - \bar\nu_1 - \dots - \bar\nu_m + m\bar\nu_{m+1} &= \bar f(\bar\nu_{m+1}) \le f(\bar\nu_{m+1}) \\ &= (m+1)\bar\nu_{m+1} + \sum_{j=m+2}^{\infty} \min\{\nu_j, \bar\nu_{m+1}\} \le (m+1)\bar\nu_{m+1} + \sum_{j=m+2}^{\infty} \nu_j \\ &= (m+1)\bar\nu_{m+1} + \sigma - \nu_1 - \dots - \nu_{m+1}, \end{aligned}$$

from which (4) follows. □

To complete the proof of Theorem A, it remains to show how its first assertion implies the second one. We use induction by k. The case $k = 2$ is easy, and we consider $k \geq 3$. For definiteness, we suppose that $0 \leq \delta(\bar{A}_1) + \cdots + \delta(\bar{A}_k) \leq 1$. Moreover, changing the indices, if necessary, we can assume that $\delta(A_k) \geq 0$, and then

$$|\delta(\bar{A}_1) + \cdots + \delta(\bar{A}_{k-1})| \leq 1. \tag{5}$$

For $m \in [1, p]$, let $\lambda_1, \dots, \lambda_m \in \mathbb{Z}/p\mathbb{Z}$ be any pairwise distinct residues modulo p. We put $\Lambda = \{-\lambda_1, \dots, -\lambda_m\}$, and we define $\bar{\lambda}_1, \dots, \bar{\lambda}_m$ to be the first m elements of the sequence $\{0, 1, -1, 2, -2, \dots\}$, so that $\bar{\Lambda} = \{-\bar{\lambda}_1, \dots, -\bar{\lambda}_m\}$ is balanced and

$$\delta(\bar{\Lambda}) \leq 0, \quad |\delta(\bar{A}_k) + \delta(\bar{\Lambda})| \leq 1. \tag{6}$$

Moreover, if $\delta(\bar{A}_k) = 0$, then

$$\delta(\bar{A}_1) + \cdots + \delta(\bar{A}_{k-1}) \geq 0, \text{ and } \delta(\bar{A}_k) + \delta(\bar{\Lambda}) \leq 0,$$

and if $\delta(\bar{A}_k) = 1$, then

$$\delta(\bar{A}_1) + \cdots + \delta(\bar{A}_{k-1}) \leq 0, \text{ and } \delta(\bar{A}_k) + \delta(\bar{\Lambda}) \geq 0.$$

By (5), (6), the latter observation, the first assertion of Theorem A and the induction hypothesis, we have

$$\begin{aligned}
\sum_{i=1}^{m} N_{\lambda_i}(\bar{A}_1,\dots,\bar{A}_k) &= N_0(\bar{A}_1,\dots,\bar{A}_k,\Lambda) \\
&= \sum_{u+v=0} N_u(\bar{A}_1,\dots,\bar{A}_{k-1}) N_v(\bar{A}_k,\Lambda) \\
&\le \sum_{i=1}^{p} \nu_i(\bar{A}_1,\dots,\bar{A}_{k-1})\nu_i(\bar{A}_k,\Lambda) \\
&= \sum_{m=1}^{p-1} \big(\nu_m(\bar{A}_1,\dots,\bar{A}_{k-1}) - \nu_{m+1}(\bar{A}_1,\dots,\bar{A}_{k-1})\big) \sum_{i=1}^{m} \nu_i(\bar{A}_k,\Lambda) \\
&\qquad\qquad + \nu_p(\bar{A}_1,\dots,\bar{A}_{k-1}) \sum_{i=1}^{p} \nu_i(\bar{A}_k,\Lambda) \\
&\le \sum_{m=1}^{p-1} \big(\nu_m(\bar{A}_1,\dots,\bar{A}_{k-1}) - \nu_{m+1}(\bar{A}_1,\dots,\bar{A}_{k-1})\big) \sum_{i=1}^{m} \nu_i(\bar{A}_k,\bar{\Lambda}) \\
&\qquad\qquad + \nu_p(\bar{A}_1,\dots,\bar{A}_{k-1}) \sum_{i=1}^{p} \nu_i(\bar{A}_k,\bar{\Lambda}) \\
&= \sum_{i=1}^{p} \nu_i(\bar{A}_1,\dots,\bar{A}_{k-1})\nu_i(\bar{A}_k,\bar{\Lambda}) \\
&= \sum_{u+v=0} N_u(\bar{A}_1,\dots,\bar{A}_{k-1}) N_v(\bar{A}_k,\bar{\Lambda}) \\
&= N_0(\bar{A}_1,\dots,\bar{A}_k,\bar{\Lambda}) \\
&= \sum_{i=1}^{m} N_{\bar{\lambda}_i}(\bar{A}_1,\dots,\bar{A}_k),
\end{aligned}$$

which is to be proven.

4. Large exponential sums: the case of an arithmetic progression

Let $A_0 = \{0,\dots,n-1\} \pmod p$, so that the corresponding sums $S_0(z)$ satisfy

$$|S_0(z)| = \frac{|\sin \pi \frac{nz}{p}|}{\sin \pi \frac{z}{p}} \qquad (z = 1,\dots,p-1). \tag{7}$$

We write

$$G(x) = \frac{\sin x}{x} \qquad (0 < x \le \pi)$$

and we define $G(0) = 1$ by continuity; thus, the inverse function $G^{-1}(x)$ is a continuous, monotonically decreasing function of $[0,1]$, satisfying $G^{-1}(0) = \pi,\ G^{-1}(1) = 0$.

Lemma 4. *For $\kappa \in (0.5, 1)$ and $n \geq 2$ the equation*

$$\frac{|\sin(nx)|}{\sin x} = \kappa n \tag{8}$$

has exactly one solution $x = x(n, \kappa)$ on the interval $(0, \pi/2)$, and this solution satisfies

$$x = \frac{1}{n}\, G^{-1}(\kappa) \left(1 + \frac{\theta}{n^2}\right),$$

where $\theta = \theta(n, \kappa) \in (0, 1)$.

Proof. As the function $f(x) = \sin(nx)/\sin x$ decreases on $(0, \pi/n)$ and $f(0+) = n > n\kappa > 0 = f(\pi/n)$, equation (8) has precisely one solution on $(0, \pi/n)$. Moreover, if $x \in (\pi/n, \pi/2)$, then

$$|f(x)| \leq \left(\frac{2}{\pi} x\right)^{-1} \leq \frac{n}{2} < \kappa n,$$

which shows that $(\pi/n, \pi/2)$ contains no solutions. We now estimate the solution $x = x(n, \kappa) \in (0, \pi/n)$.

Since (8) implies $G(nx) = \kappa G(x) < \kappa$, we have $nx > G^{-1}(\kappa)$, whence $x > n^{-1} G^{-1}(\kappa)$. To obtain the upper bound, we first note that

$$G(nx) = \kappa G(x) > \kappa \left(1 - \frac{x^2}{6}\right). \tag{9}$$

Next, we let $\mu = n/(n^2 + 1)$, and we show that

$$G(nx) \leq \left(1 - \frac{x^2}{6}\right) G((n - \mu)x). \tag{10}$$

Notice, that (10) along with (9) yield

$$\begin{aligned} G((n-\mu)x) &> \kappa, \\ (n-\mu)x &< G^{-1}(\kappa), \\ x &< \frac{1}{n-\mu}\, G^{-1}(\kappa) = \frac{1}{n}\left(1 + \frac{1}{n^2}\right) G^{-1}(\kappa), \end{aligned}$$

and it remains to prove (10). To this end we rewrite it as

$$G((n - \mu)x) - G(nx) \geq \frac{x^2}{6}\, G((n - \mu)x), \tag{11}$$

and we observe that

$$G((n - \mu)x) - G(nx) \geq \mu x \left(-G'((n - \mu)x)\right).$$

Letting $\xi = (n - \mu)x$ and using the inequality

$$\sin \xi \geq \xi \cos \xi + \frac{1}{3}\, \xi^2 \sin \xi$$

(valid for any $\xi \in [0, \pi/2]$), we get

$$\begin{aligned} G((n-\mu)x) - G(nx) &\geq \mu x \, \frac{\sin\xi - \xi\cos\xi}{\xi^2} \\ &\geq \frac{1}{3}\,\mu x \sin\xi \\ &= \frac{x^2}{6}\, 2\mu(n-\mu)\, G(\xi) \\ &\geq \frac{x^2}{6}\, G(\xi), \end{aligned}$$

which proves (11). $\square$

Corollary 1. *For $0 < \varphi < \pi/3$, the number of $z \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $|S_0(z)| > n\cos\varphi$ is*

$$T_0(\varphi) = 2\lceil Z \rceil - 2,$$

where

$$Z = \frac{1}{\pi}\,\frac{p}{n}\, G^{-1}(\cos\varphi)\left(1 + \frac{\theta}{n^2}\right); \qquad \theta \in (0,1).$$

We next estimate the function $G^{-1}(x)$.

Lemma 5.

$$\sqrt{6(1-x)} \leq G^{-1}(x) \leq \sqrt{6(1-x)}\left(1 + \frac{1}{4}(1-x)\right),$$

provided $7/15 \leq x \leq 1$. (In fact, the lower bound holds true for all $x \in [0,1]$.)

Proof. i) Given $x \in [0,1]$, we define $z = \sqrt{6(1-x)}$. Then

$$G(z) \geq 1 - \frac{z^2}{6} = x,$$
$$G^{-1}(x) \geq z = \sqrt{6(1-x)}.$$

ii) To prove the upper bound, we use the inequality

$$G(z) \leq 1 - \frac{z^2}{6} + \frac{z^4}{120} \qquad (z \geq 0). \tag{12}$$

Given $x \in [7/15, 1]$, we define $z \in [0,2]$ by

$$x = 1 - \frac{z^2}{6} + \frac{z^4}{120}, \tag{13}$$

and we get then

$$6(1-x) = z^2\left(1 - \frac{z^2}{20}\right) \geq \frac{4}{5}z^2,$$

whence

$$\frac{z^2}{20} \leq \frac{3}{8}(1-x).$$

The latter inequality and (13) give

$$6(1-x) = z^2\left(1-\frac{z^2}{20}\right) \geq z^2\left(1-\frac{3}{8}(1-x)\right) \geq \frac{z^2}{1+\frac{1}{2}(1-x)},$$

$$z^2 \leq 6(1-x)\left(1+\frac{1}{2}(1-x)\right). \tag{14}$$

Now by (12), (13) and (14),

$$G^{-1}(x) \leq z \leq \sqrt{6(1-x)}\sqrt{1+\frac{1}{2}(1-x)} \leq \sqrt{6(1-x)}\left(1+\frac{1}{4}(1-x)\right).$$

□

5. Large exponential sums: Proofs of Theorems B and C

We first prove several auxiliary lemmas.

Proof of Lemma 1. The observation of Yudin, mentioned in Section 2, is that

$$|S(z_1+z_2)| > n\cos(\varphi_1+\varphi_2), \tag{15}$$

provided

$$|S(z_1)| > n\cos\varphi_1,\ |S(z_2)| > n\cos\varphi_2,\ \text{and } 0 \leq \varphi_1, \varphi_2, \varphi_1+\varphi_2 \leq \pi/2. \tag{16}$$

(See [Y73, Lemma 1].) Consider the subsets of $\mathbb{Z}/p\mathbb{Z}$

$$E(\varphi) := \{z \in \mathbb{Z}/p\mathbb{Z} \colon |S(z)| > n\cos\varphi\},$$

so that $T(\varphi) = |E(\varphi)| - 1$. What (15) and (16) mean is

$$E(\varphi_1) + E(\varphi_2) \subseteq E(\varphi_1+\varphi_2),$$

provided $0 \leq \varphi_1, \varphi_2, \varphi_1+\varphi_2 \leq \pi/2$. By Cauchy-Davenport theorem we have then

$$|E(\varphi_1+\varphi_2)| \geq \min\{|E(\varphi_1)| + |E(\varphi_2)| - 1, p\},$$

and the result follows. □

Proof of Lemma 2. We assume $0 < \varphi_0 < \varphi \leq \pi/2$, as otherwise the assertion is trivial. Let $j = \lfloor \varphi/\varphi_0 \rfloor$; then $0 < j\varphi_0 \leq \varphi \leq \pi/2$ and by Lemma 1,

$$T(\varphi) \geq T(j\varphi_0) \geq \min\{jT(\varphi_0), p-1\}.$$

Thus, the desired estimate follows unless

$$\left\lfloor \frac{\varphi}{\varphi_0} \right\rfloor T(\varphi_0) \geq p, \tag{17}$$

and we suppose (17) to hold for the rest of the proof. We define

$$l := \left\lfloor \frac{p-1}{T(\varphi_0)} \right\rfloor \geq 1,$$

so that

$$lT(\varphi_0) \le p-1 \tag{18}$$

whence, by (17),

$$l \le \left\lfloor \frac{\varphi}{\varphi_0} \right\rfloor - 1, \tag{19}$$

and therefore,

$$l\varphi_0 < \varphi \le \pi/2. \tag{20}$$

Now by Lemma 1, (18), and (20), $T(i\varphi_0) \ge iT(\varphi_0)$ for $i = 1, \dots, l$, and it follows that there exist l pairwise disjoint residue sets $\mathcal{E}_1, \dots, \mathcal{E}_l \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$ such that $|\mathcal{E}_1| = \dots = |\mathcal{E}_l| = T(\varphi_0)$ and $|S(z)| > n\cos(i\varphi_0)$ for $z \in \mathcal{E}_i$. We conclude that

$$\begin{aligned} n(p-n) &= \sum_{z=1}^{p-1} |S(z)|^2 \\ &\ge n^2(\cos^2\varphi_0 + \dots + \cos^2(l\varphi_0))T(\varphi_0) \\ &= n^2\left(\frac{1}{2}l + \frac{1}{4}\,\frac{\sin(2l+1)\,\varphi_0 - \sin\varphi_0}{\sin\varphi_0}\right)T(\varphi_0). \end{aligned} \tag{21}$$

Also, by (19),

$$(2l+1)\varphi_0 \le 2\varphi - \varphi_0 \le \pi - \varphi_0,$$

whence

$$\sin(2l+1)\,\varphi_0 \ge \sin\varphi_0. \tag{22}$$

¿From (21) and (22),

$$\begin{gathered} p - n \ge \frac{1}{2}\,nlT(\varphi_0), \\ \frac{p-n}{T(\varphi_0)} \ge \frac{n}{2}\,l \ge 2l \ge 2\left\lfloor \frac{p-n}{T(\varphi_0)} \right\rfloor, \\ \left\lfloor \frac{p-n}{T(\varphi_0)} \right\rfloor \le \left\{ \frac{p-n}{T(\varphi_0)} \right\}, \\ T(\varphi_0) > p - n. \end{gathered} \tag{23}$$

On the other hand, $\varphi/\varphi_0 \ge l+1 \ge 2$, hence $\varphi_0 \le \pi/4$, $\cos^2\varphi_0 \ge 1/2$ and therefore

$$n(p-n) = \sum_{z=1}^{p-1} |S(z)|^2 \ge n^2\cos^2\varphi_0 T(\varphi_0) \ge \frac{1}{2}n^2 T(\varphi_0) \ge 2nT(\varphi_0),$$

$$T(\varphi_0) \le \frac{p-n}{2}.$$

This, however, contradicts (23). □

In the course of the proof of Theorems B and C we need estimates of the Euler beta function

$$B(u,v)=\int_0^1 t^{u-1}(1-t)^{v-1}\,dt.$$

Lemma 6. *For $k>0$,*

$$B(k,3/2)<\frac{\sqrt{\pi}}{2}\,k^{-3/2},$$
$$B(k,5/2)<\frac{3\sqrt{\pi}}{4}\,k^{-5/2}.$$

Proof.

$$\begin{aligned}B(k,3/2)&=\int_0^1 t^{1/2}\,\frac{-1}{k}\,((1-t)^k)'\,dt\\&=\frac{1}{2k}\int_0^1 t^{-1/2}(1-t)^k\,dt<\frac{1}{2k}\int_0^1 t^{-1/2}e^{-kt}\,dt=\frac{1}{2}\,k^{-3/2}\int_0^k \tau^{-1/2}e^{-\tau}\,d\tau\\&\qquad<\frac{1}{2}\,k^{-3/2}\Gamma(1/2)=\frac{\sqrt{\pi}}{2}\,k^{-3/2}.\end{aligned}$$

Similarly,

$$\begin{aligned}B(k,5/2)&=\int_0^1 t^{3/2}\,\frac{-1}{k}\,((1-t)^k)'\,dt\\&=\frac{3}{2k}\int_0^1 t^{1/2}(1-t)^k\,dt<\frac{3}{2k}\int_0^1 t^{1/2}e^{-kt}\,dt=\frac{3}{2}\,k^{-5/2}\int_0^k \tau^{1/2}e^{-\tau}\,d\tau\\&\qquad<\frac{3}{2}\,k^{-5/2}\Gamma(3/2)=\frac{3\sqrt{\pi}}{4}\,k^{-5/2}.\end{aligned}$$

□

We prove Theorems B and C together.

Proof of Theorems B and C. Using partial summation, we write

$$\sum_{z=1}^{p-1}|S_0(z)|^k=kn^k\int_0^{\pi/2}T_0(\varphi)\cos^{k-1}\varphi\sin\varphi\,d\varphi, \tag{24}$$
$$\sum_{z=1}^{p-1}|S(z)|^k=kn^k\int_0^{\pi/2}T(\varphi)\cos^{k-1}\varphi\sin\varphi\,d\varphi, \tag{25}$$

and we denote the integrals in the right-hand sides by I_0 and I, respectively. Since for $k=2m$ the sums count the solutions of the linear equation

$$a_1+\cdots+a_m=a_{m+1}+\cdots+a_{2m}$$

with $a_i \in A_0$ in (24) and $a_i \in A$ in (25) (up to the constant term $|S(0)|^k = n^k$ and the multiplicative coefficient p), by Theorem A

$$I \le I_0 \tag{26}$$

for k even. We first estimate I_0.

By Corollary 1 and Lemmas 5 and 6 we have

$$\begin{aligned}
I_0 &\le \frac{2}{\pi}\frac{p}{n}\left(1+\frac{1}{n^2}\right)\int_0^{\pi/3} G^{-1}(\cos\varphi)\cos^{k-1}\varphi\sin\varphi\,d\varphi \\
&\qquad\qquad + \cos^{k-2}(\pi/3)\int_{\pi/3}^{\pi/2} T_0(\varphi)\cos\varphi\sin\varphi\,d\varphi \\
&\le \frac{2}{\pi}\frac{p}{n}\left(1+\frac{1}{n^2}\right)\int_{1/2}^{1} t^{k-1}G^{-1}(t)\,dt + 2^{2-k}\int_0^{\pi/2} T_0(\varphi)\cos\varphi\sin\varphi\,d\varphi \\
&\le \frac{2\sqrt{6}}{\pi}\frac{p}{n}\left(1+\frac{1}{n^2}\right)\left(\int_{1/2}^{1} t^{k-1}(1-t)^{1/2}\,dt + \frac{1}{4}\int_{1/2}^{1} t^{k-1}(1-t)^{3/2}\,dt\right) \\
&\qquad\qquad + 2^{2-k}\,\frac{n(p-n)}{2n^2} \\
&< \sqrt{\frac{6}{\pi}}\,\frac{p}{n}\,k^{-3/2}\left(1+\frac{1}{n^2}\right)\left(1+\frac{3}{8k}\right) + 2^{1-k}\,\frac{p}{n}.
\end{aligned}$$

Using elementary calculus, one can easily derive the two following estimates:

$$I_0 \le \sqrt{\frac{6}{\pi}}\,\frac{p}{n}\,k^{-3/2}\left(1+\frac{1}{n^2}\right)\left(1+\frac{4}{k}\right); \quad k \ge 2,$$

and

$$I_0 \le \sqrt{\frac{6}{\pi}}\,\frac{p}{n}\,k^{-3/2}\left(1+\frac{1}{n^2}\right)\left(1+\frac{2}{5k}\right); \quad k \ge 16. \tag{27}$$

The first estimate, in view of (24), proves Theorem B, and we proceed with the proof of Theorem C. Fix $\varphi_0 \in (0, \pi/6]$. Our plan is to apply Lemma 2 to show that large value of $T(\varphi_0)$ results in a large value of I, while I cannot be "too large" by (26) and (27). Indeed, for $k \geq 16$ even, by Lemma 2 and using Stirling formula we have

$$\begin{aligned}
I &\geq \int_0^{\pi/2} \left\lfloor \frac{\varphi}{\varphi_0} \right\rfloor T(\varphi_0) \cos^{k-1}\varphi \sin\varphi \, d\varphi \\
&\geq \frac{T(\varphi_0)}{\varphi_0} \int_0^{\pi/2} \frac{-1}{k}\, \varphi\, (\cos^k\varphi)' \, d\varphi - T(\varphi_0) \int_0^{\pi/2} \frac{-1}{k}\, (\cos^k\varphi)' \, d\varphi \\
&= \frac{1}{k} \frac{T(\varphi_0)}{\varphi_0} \int_0^{\pi/2} \cos^k\varphi \, d\varphi - \frac{1}{k} T(\varphi_0) \\
&= \frac{1}{k} \frac{T(\varphi_0)}{\varphi_0}\, 2^{-k} \binom{k}{k/2} \frac{\pi}{2} - \frac{1}{k} T(\varphi_0) \\
&\geq \sqrt{\frac{\pi}{2}}\, k^{-3/2}\, \frac{T(\varphi_0)}{\varphi_0}\, e^{-1/3k} - \frac{1}{k} T(\varphi_0) \\
&= \sqrt{\frac{\pi}{2}}\, k^{-3/2}\, \frac{T(\varphi_0)}{\varphi_0} \left(1 - \sqrt{\frac{2}{\pi}}\, e^{1/3k} \varphi_0 \sqrt{k}\right) e^{-1/3k} \\
&> \sqrt{\frac{\pi}{2}}\, k^{-3/2}\, \frac{T(\varphi_0)}{\varphi_0} \left(1 - \frac{5}{6}\, \varphi_0 \sqrt{k}\right) e^{-1/3k}.
\end{aligned}$$

Along with (26) and (27), this yields

$$\sqrt{\frac{\pi}{2}}\, k^{-3/2}\, \frac{T(\varphi_0)}{\varphi_0} \left(1 - \frac{5}{6}\, \varphi_0 \sqrt{k}\right) e^{-1/3k} < \sqrt{\frac{6}{\pi}}\, \frac{p}{n}\, k^{-3/2} \left(1 + \frac{1}{n^2}\right) \left(1 + \frac{2}{5k}\right).$$

Using the inequality

$$\left(1 + \frac{2}{5k}\right) e^{1/3k} < 1 + \frac{3}{4k} \qquad (k \geq 16)$$

and replacing for brevity φ_0 by φ, we get

$$T(\varphi) < \frac{2\sqrt{3}}{\pi}\, \frac{p}{n}\, \varphi \left(1 + \frac{1}{n^2}\right) \frac{1 + \frac{3}{4k}}{1 - \frac{5}{6}\, \varphi \sqrt{k}}. \tag{28}$$

We now recall the estimate of [L98, Lemma 2]:

$$T(\varphi) < \frac{4}{\pi}\, \frac{p}{n}\, \varphi(1 + \varphi); \qquad 0 < \varphi \leq \pi/6.$$

This supersedes Theorem C for $\varphi \geq 0.03$, and therefore we can suppose that $\varphi < 0.03$.

To optimize by k in (28) we choose $k = 2\lceil 0.75\varphi^{-2/3} \rceil$; this leads to $k \geq 16$ by the above assumption $\varphi < 0.03$. We have

$$\frac{1 + \frac{3}{4k}}{1 - \frac{5}{6}\, \varphi\sqrt{k}} = 1 + \frac{\frac{3}{4k} + \frac{5}{6}\, \varphi\sqrt{k}}{1 - \frac{5}{6}\, \varphi\sqrt{k}}, \tag{29}$$

and

$$
\begin{aligned}
\frac{3}{4k} + \frac{5}{6}\,\varphi\sqrt{k} &\le \frac{1}{2}\,\varphi^{2/3} + \frac{5}{6}\,\varphi\sqrt{2 + \frac{3}{2}\,\varphi^{-2/3}} \\
&= \varphi^{2/3}\left(\frac{1}{2} + \frac{5}{6}\sqrt{\frac{3}{2} + 2\varphi^{2/3}}\right) \\
&\le \frac{8}{5}\,\varphi^{2/3}, \\
1 - \frac{5}{6}\,\varphi\sqrt{k} &> 1 - \frac{5}{6}\,\varphi\sqrt{2 + \frac{3}{2}\,\varphi^{-2/3}} \\
&= 1 - \frac{5}{6}\,\varphi^{2/3}\sqrt{\frac{3}{2} + 2\varphi^{2/3}} \\
&> \frac{8}{9}.
\end{aligned}
$$

The result now follows from (28) and (29). □

References

[G32] R.M. Gabriel, The rearrangement of positive Fourier coefficients, *Proc. London Math. Soc. (Second Series)* **33** (1932), 32–51.

[HL28] G.H. Hardy and J.E. Littlewood, Notes on the theory of series (VIII): an inequality, *J. London Math. Soc.* **3** (1928), 105–110.

[HLP88] G.H. Hardy, J.E. Littlewood and G. Polya, Inequalities, 2d ed., Camb. Univer. Press, 1988.

[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.

[P74] J.M. Pollard, Addition properties of residue classes, *J. London Math. Soc.* **2** (11) (1975), 147–152. 460–462.

[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.

Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel.

E-mail address: `seva@math.huji.ac.il`