Journal of Number Theory **76**, 147–153 (1999)
Article ID jnth.1998.2351, available online at http://www.idealibrary.com on IDEAL®

On the Uniform Distribution in Residue Classes of Dense Sets of Integers with Distinct Sums

Mihail N. Kolountzakis*

Department of Mathematics, University of Crete, 714 09 Iraklio, Greece
E-mail: kolount@math.uch.gr

Communicated by A. Hildebrand

Received July 5, 1998; revised August 5, 1998

m and on the difference $N^{1/2} - |\mathscr{A}|$ (these quantities should not be too large), the elements of $\mathscr{A}$ are uniformly distributed in the residue classes mod m. Quantitative estimates on how uniform the distribution is are also provided. This generalizes recent results of Lindström whose approach was combinatorial. Our main tool is an upper bound on the minimum of a cosine sum of k terms, $\sum_1^k \cos \lambda_j x$, all of whose positive integer frequencies λ_j are at most $(2-\varepsilon)\, k$ in size.

INTRODUCTION AND RESULTS

A set $\mathscr{A} \subseteq \{1, ..., N\}$ is of the type B_2 if all sums

$$a + b, \qquad \text{with } a \geqslant b, \quad a, b \in \mathscr{A},$$

are distinct. (Such sets are also called *Sidon*, but the term has a very different meaning in harmonic analysis.) This is easily seen to be equivalent to all differences $a - b$, with $a \neq b$, $a, b \in \mathscr{A}$, being distinct. It is an old theorem of Erdős and Turán [ET41, HR83, K96] that the size of the largest B_2 subset of $\{1, ..., N\}$ is at most $N^{1/2} + O(N^{1/4})$. It is also known [BC63, HR83] that there exist B_2 subsets of $\{1, ..., N\}$ of size $\sim N^{1/2}$.

In this note we consider such dense B_2 subsets $\mathscr{A}$ of $\{1, ..., N\}$, i.e., sets of size $N^{1/2} + o(N^{1/2})$, and prove, under mild conditions on $|\mathscr{A}|$ and the

* Partially supported by the U.S. National Science Foundation, under Grant DMS 97-05775.

0022-314X/99 $30.00

modulus m, which is also allowed to vary with N, that they are uniformly distributed mod m. More precisely, let

$$a(x)=a_m(x)=|\{a\in\mathscr{A}: a=x \bmod m\}|, \qquad \text{for} \quad x\in\mathbb{Z}_m,$$

be the number of elements of $\mathscr{A}$ with residue x mod m. We shall show, for example, that if $|\mathscr{A}|\sim N^{1/2}$ and m is a constant then, as $N\to\infty$,

$$a(x)=\frac{|\mathscr{A}|}{m}+o\left(\frac{|\mathscr{A}|}{m}\right). \tag{1}$$

We shall also obtain bounds on the error term. These bounds will depend on $|\mathscr{A}|$, m and N.

Previously Lindström [L98] showed precisely (1) using a combinatorial method, thus answering a question posed in [ESS94]. Under the additional assumptions

$$m=2 \qquad \text{and} \qquad |\mathscr{A}|\geqslant N^{1/2} \tag{2}$$

he obtained the bound $O(N^{3/8})$ for the error term in (1).

Here we use an analytic method which has previously been used [K96] to prove and generalize the Erdős–Turán theorem mentioned above. The core of our technique is the following theorem [K96] which was proved in connection with the so called *cosine problem* of classical harmonic analysis.

THEOREM 1. *Suppose* $0\leqslant f(x)=M+\sum_1^N \cos\lambda_j x$, *with the integers* λ_j *satisfying*

$$1\leqslant\lambda_1<\cdots<\lambda_N\leqslant(2-\varepsilon)\,N,$$

for some $\varepsilon>3/N$. *Then*

$$M>A\varepsilon^2 N, \tag{3}$$

for some absolute positive constant A.

Our main theorem, of which Lindström's result is a special case, is the following.

THEOREM 2. *Suppose* $\mathscr{A}\subseteq\{1,...,N\}$ *is a* B_2 *set and that*

$$k=|\mathscr{A}|\geqslant N^{1/2}-l, \qquad \text{with} \quad l=l(N)=o(N^{1/2}).$$

Assume also that $m=o(N^{1/2})$. *Then we have*

$$\left\|a(x)-\frac{k}{m}\right\|_2 \leqslant C \begin{cases} \dfrac{N^{3/8}}{m^{1/4}} & \textit{if} \quad l \leqslant N^{1/4}m^{1/2} \\ \dfrac{N^{1/4}l^{1/2}}{m^{1/2}} & \textit{else}. \end{cases} \tag{4}$$

(In our notation l need not be a positive quantity. If it is negative (i.e., $k > N^{1/2}$) the first of the two alternatives in (4) holds in the upper bound.)

We use the notation $\|f\|_p = (\sum_{x \in \mathbb{Z}_m} |f(x)|^p)^{1/p}$, for $f: \mathbb{Z}_m \to \mathbb{C}$ and $1 \leqslant p < \infty$, and also $\|f\|_\infty = \max_{x \in \mathbb{Z}_m} |f(x)|$. We obviously have $\|f\|_\infty \leqslant \|f\|_p$, for all f and $1 \leqslant p < \infty$.

Remarks. It follows easily from Theorem 2 that in the following two cases we have uniform distribution in residue classes mod m.

1. When $l \leqslant N^{1/4}m^{1/2}$ and $m = o(N^{1/6})$ we have

$$\left\|a(x)-\frac{k}{m}\right\|_\infty \leqslant \left\|a(x)-\frac{k}{m}\right\|_2 \leqslant C\frac{N^{3/8}}{m^{1/4}} = o\left(\frac{k}{m}\right). \tag{5}$$

2. When $l \geqslant N^{1/4}m^{1/2}$ and $m = o(N^{1/2}/l)$ we have

$$\left\|a(x)-\frac{k}{m}\right\|_\infty \leqslant \left\|a(x)-\frac{k}{m}\right\|_2 \leqslant C\frac{N^{1/4}l^{1/2}}{m^{1/2}} = o\left(\frac{k}{m}\right). \tag{6}$$

In these two cases we have uniform distribution "in the l^2 sense" as well as in the l^∞ sense.

As a comparison to the result that Lindström obtained under assumptions (2), we obtain that whenever m is a constant and $l \leqslant CN^{1/4}$ we have

$$\left\|a(x)-\frac{k}{m}\right\|_2 \leqslant C\frac{N^{1/4}l^{1/2}}{m^{1/2}} \leqslant C_m N^{3/8}.$$

As is customary, C denotes an absolute positive constant, not necessarily the same in all its occurences, while C with a subscript denotes a constant depending at most on the parameter indicated in the subscript.

PROOFS

For the proof of Theorem 2 we shall need the following two lemmas, the first of which is elementary and the second a consequence of Theorem 1.

Lemma 1. *If* $a\colon \mathbb{Z}_m \to \mathbb{C}$ *and* $S = \sum_{x\in\mathbb{Z}_m} a(x)$ *then*

$$\sum_{x\in\mathbb{Z}_m} \left| a(x) - \frac{S}{m} \right|^2 = \sum_{x\in\mathbb{Z}_m} |a(x)|^2 - \frac{S^2}{m}.$$

Proof. Let $a(x) = S/m + \delta(x)$ for $x \in \mathbb{Z}_m$. It follows that $\sum_{x\in\mathbb{Z}_m} \delta(x) = 0$. Then

$$\sum_{x\in\mathbb{Z}_m} |a(x)|^2 = \sum_{x\in\mathbb{Z}_m} \left(\frac{S^2}{m^2} + |\delta(x)|^2 + 2\frac{S}{m} \operatorname{Re} \delta(x) \right)$$
$$= \frac{S^2}{m} + \sum_{x\in\mathbb{Z}_m} |\delta(x)|^2. \quad \blacksquare$$

Lemma 2. *Suppose* $\lambda_j \in \mathbb{N}$, $j = 1, ..., N$, *are distinct positive integers and define*

$$N_m = |\{\lambda_j : \lambda_j = 0 \bmod m\}|.$$

If

$$0 \leqslant p(x) = M + \sum_{j=1}^{N} \cos \lambda_j x, \qquad (x \in \mathbb{R}),$$

and

$$\lambda_j \leqslant (2-\varepsilon)\, N_m\, m, \qquad \textit{for all } \lambda_j = 0 \bmod m,$$

for some $\varepsilon > 3/N_m$, *then we have*

$$M > A\varepsilon^2 N_m,$$

for some absolute positive constant A.

Proof. The measure μ on $[0, 2\pi)$ with $\hat{\mu}(n) = 1$ if m divides n and $\hat{\mu}(n) = 0$ otherwise is nonnegative. Let

$$q(x) = p(x) \star \mu = M + \sum_{m \mid \lambda_j} \cos \lambda_j x \geqslant 0.$$

Define also the polynomial

$$r(x) = q\left(\frac{x}{m}\right) = M + \sum_{m \mid \lambda_j} \cos \frac{\lambda_j}{m} x \geqslant 0.$$

By Theorem 1 and the assumption

$$\frac{\lambda_j}{m} \leqslant (2-\varepsilon) N_m$$

we get $M \geqslant A\varepsilon^2 N_m$ as desired. ∎

Proof of Theorem 2. Write

$$d(j) = |\{(a, b) \in A^2 : a - b = j \bmod m\}|, \qquad (j \in \mathbb{Z}_m),$$

and notice that, by the Cauchy–Schwarz inequality,

$$d(j) = \sum_{i \in \mathbb{Z}_m} a(i)\, a(i+j) \leqslant \sum_{i \in \mathbb{Z}_m} (a(i))^2 = d(0), \qquad (j \in \mathbb{Z}_m).$$

We also clearly have $\sum_{i \in \mathbb{Z}_m} d(i) = k^2$ which implies

$$d(0) \geqslant \frac{k^2}{m}.$$

Define the nonnegative polynomial

$$\begin{aligned} f(x) &= \left| \sum_{a \in \mathscr{A}} e^{iax} \right|^2 \\ &= k + \sum_{a \neq b,\, a,\, b \in \mathscr{A}} e^{i(a-b)x} \\ &= k + 2 \sum_j \cos \lambda_j x, \end{aligned}$$

where the set $\{\lambda_j\}$ consists of all differences $a - b$, with $a, b \in \mathscr{A}$, $a > b$, which are all distinct since $\mathscr{A}$ is of type B_2. (Notice that $1 \leqslant \lambda_j \leqslant N$.) With the notation of Lemma 2 we have

$$d(0) = k + 2N_m.$$

Since $k \sim N^{1/2}$ and $m = o(N^{1/2}) = o(k)$ we may suppose that, for N large enough,

$$\tfrac{1}{2} N^{1/2} < k < 2N^{1/2}$$

and

$$m < \tfrac{1}{2}k.$$

Hence

$$\frac{3}{N_m} = \frac{6}{d(0)-k} \leqslant \frac{6}{k^2/m-k} \leqslant \frac{12m}{k^2} < \frac{48m}{N} < 48N^{-1/2}.$$

Let

$$\varepsilon = c(mN^{-1/2})^{1/2},$$

with the positive constant c to be chosen later. Since $m = o(N^{1/2})$, ε can be made as small as we please and

$$\frac{3}{N_m} < \varepsilon,$$

if N is large enough. We also have (since $N_m > N/16m$)

$$\varepsilon^2 N_m = c^2 \frac{m}{N^{1/2}} N_m > \frac{c^2}{16} \cdot \frac{m}{N^{1/2}} \cdot \frac{N}{m} = \frac{c^2}{16} N^{1/2},$$

so that

$$A\varepsilon^2 N_m > A \frac{c^2}{16} N^{1/2} > k$$

if c is suitably chosen, i.e., by $Ac^2/32 = 1$. (Here A is the constant in Lemma 2.)

Hence the hypothetis of Lemma 2 must fail, and we obtain (since N is larger than all λ_j)

$$N \geqslant (2-\varepsilon)\, mN_m,$$

i.e.,

$$\frac{N}{m} \geqslant \left(1 - c\frac{m^{1/2}}{N^{1/4}}\right)(d(0)-k).$$

Since $m^{1/2}N^{-1/4}=o(1)$ we have

$$d(0)-k \leqslant \left(1+C\frac{m^{1/2}}{N^{1/4}}\right)\frac{N}{m}$$
$$\leqslant \left(1+C\frac{m^{1/2}}{N^{1/4}}\right)\left(\frac{k^2}{m}+\frac{2lk}{m}+\frac{l^2}{m}\right)$$
$$\leqslant \frac{k^2}{m}+C\frac{k^2}{m^{1/2}N^{1/4}}+C\frac{lk}{m}.$$

We also have $k=o(k^2/m^{1/2}N^{1/4})$ since $m=o(N^{1/2})$ and $k\sim N^{1/2}$. It follows that

$$\left|\sum_{x\in\mathbb{Z}_m}(a(x))^2-\frac{k^2}{m}\right| \leqslant C\left(\frac{k^2}{m^{1/2}N^{1/4}}+\frac{lk}{m}\right),$$

and by Lemma 1 we obtain (with $k\sim N^{1/2}$)

$$\left\|a(x)-\frac{k^2}{m}\right\|_2 \leqslant C\frac{N^{1/4}}{m^{1/4}}\left(N^{1/4}+\frac{l}{m^{1/2}}\right)^{1/2}$$
$$\leqslant C\begin{cases}\dfrac{N^{3/8}}{m^{1/4}} & \text{if} \quad l\leqslant N^{1/4}m^{1/2}\\[2ex] \dfrac{N^{1/4}l^{1/2}}{m^{1/2}} & \text{else}\end{cases}$$

as we had to prove. ∎

REFERENCES

[BC63] R. C. Bose and S. Chowla, Theorems in the additive theory of numbers, *Comment. Math. Helv.* **37** (1962–63), 141–147.

[ESS94] P. Erdős, A. Sárközy, and T. Sós, On sum sets of Sidon sets, I, *J. Number Theory* **47** (1994), 329–347.

[ET41] P. Erdős and P. Turán, On a problem of Sidon in additive number theory and some related problems, *J. London Math. Soc.* **16** (1941), 212–215; addendum (by P. Erdős), *J. London Math. Soc.* **19** (1944), 208.

[HR83] H. Halberstam and K. F. Roth, "Sequences," Springer-Verlag, New York, 1983.

[K96] M. Kolountzakis, The density of $B_h[g]$ sequences and the minimum of dense cosine sums, *J. Number Theory* **56** (1996), 4–11.

[L98] B. Lindström, Well distribution of Sidon sets in residue classes, *J. Number Theory* **69** (1998), 197–200.