Izvestiya: Mathematics **72**:1 149–168 © 2008 RAS(DoM) and LMS

Izvestiya RAN: Ser. Mat. **72**:1 161–182 DOI 10.1070/IM2008v072n01ABEH002396

On sets of large trigonometric sums

I. D. Shkredov

Abstract. We prove the existence of non-trivial solutions of the equation $r_1+r_2=r_3+r_4$, where r_1, r_2, r_3 and r_4 belong to the set R of large Fourier coefficients of a certain subset A of $\mathbb{Z}/N\mathbb{Z}$. This implies that R has strong additive properties. We discuss generalizations and applications of the results obtained.

§ 1. Introduction

Let N be a positive integer. We denote by $\mathbb{Z}_N=\mathbb{Z}/N\mathbb{Z}$ the set of residues modulo N. Let $f\colon \mathbb{Z}_N\to\mathbb{C}$ be an arbitrary function. The Fourier transform of f is given by the formula

$$\hat{f}(r)=\sum_{n\in\mathbb{Z}_N} f(n)e(-nr), \tag{1}$$

where $e(x)=e^{-2\pi i x/N}$. The following Parseval equality holds for the Fourier coefficients of f:

$$\sum_{r\in\mathbb{Z}_N}|\hat{f}(r)|^2=N\sum_{n\in\mathbb{Z}_N}|f(n)|^2. \tag{2}$$

Let δ and α be real numbers, $0<\alpha\leqslant\delta\leqslant 1$, and let A be a subset of $\mathbb{Z}_N$ of cardinality δN. The symbol A will also stand for the characteristic function of this set. Consider the set $\mathcal{R}_\alpha$ of large trigonometric sums of A:

$$\mathcal{R}_\alpha=\mathcal{R}_\alpha(A)=\{r\in\mathbb{Z}_N\colon |\widehat{A}(r)|\geqslant\alpha N\}. \tag{3}$$

For many problems of the combinatorial theory of numbers it is important to know the structure of $\mathcal{R}_\alpha$, in other words, it is important to know its properties, as will be indicated below. For the moment, we only mention the fact that this problem was posed by Gowers in [1].

The elementary properties of $\mathcal{R}_\alpha$ are as follows. The definition implies that $0\in\mathcal{R}_\alpha$ and $\mathcal{R}_\alpha=-\mathcal{R}_\alpha$, which means that $-r\in\mathcal{R}_\alpha$ if $r\in\mathcal{R}_\alpha$. Further, Parseval's equality (2) implies that $|\mathcal{R}_\alpha|\leqslant\delta/\alpha^2$. Has $\mathcal{R}_\alpha$ any other non-trivial properties? It turns out that the answer to this question is positive.

We denote by log the logarithm to the base 2.

This research was carried out with the financial support of the Russian Foundation for Basic Research (grant no. 06-01-00383), the Programme of the President of the Russian Federation (grant no. 1726.2006.1) and INTAS (grant no. 03-51-5-70).

AMS 2000 *Mathematics Subject Classification.* 11B25, 05D10, 11L07, 37C25, 37B20, 37A05, 28D05.

In 2002, M.-C. Chang proved the following theorem [2].

Theorem 1 (M.-C. Chang). *Let δ and α be real numbers, $0 < \alpha \leqslant \delta \leqslant 1$, let A be an arbitrary subset of $\mathbb{Z}_N$ of cardinality δN and let $\mathcal{R}_\alpha$ be the set defined by* (3). *Then there is a set $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\} \subseteq \mathbb{Z}_N$, $|\Lambda| \leqslant 2(\delta/\alpha)^2 \log(1/\delta)$, such that every element r of $\mathcal{R}_\alpha$ can be represented in the form*

$$r \equiv \sum_{i=1}^{|\Lambda|} \varepsilon_i \lambda_i \pmod N, \tag{4}$$

where $\varepsilon_i \in \{-1, 0, 1\}$.

Developing the approach suggested in [3] (see also [4]), Chang applied her result to the proof of Freiman's theorem [5] on sets with small sum. Recall that $Q \subseteq \mathbb{Z}$ is called a *d-dimensional arithmetic progression* if

$$Q = \{n_0 + n_1\lambda_1 + \dots + n_d\lambda_d \colon 0 \leqslant \lambda_i < m_i\},$$

where the m_i are positive integers and the n_i are integers.

Theorem 2 (G. A. Freiman). *Let $C > 0$ be some number, let $A \subseteq \mathbb{Z}$ be an arbitrary set and let $|A + A| \leqslant C|A|$. Then one can find numbers d and K depending only on C and a d-dimensional arithmetic progression Q such that $|Q| \leqslant K|A|$ and $A \subseteq Q$.*

Another application of Theorem 1 was given by B. Green in [6] (see also the earlier papers [7], [8] and the recent paper [9]). One of the main results of [6] can be stated as follows.

Theorem 3 (B. Green). *Let A be an arbitrary subset of $\mathbb{Z}_N$ of cardinality δN. Then $A + A + A$ contains an arithmetic progression whose length is greater than or equal to*

$$2^{-24}\delta^5 \bigl(\log(1/\delta)\bigr)^{-2} N^{\delta^2/(250 \log(1/\delta))}. \tag{5}$$

In another paper (see [10]), Green showed that Chang's theorem is, in a sense, exact. Let $E = \{e_1, \dots, e_{|E|}\} \subseteq \mathbb{Z}_N$ be an arbitrary set. We denote by $\operatorname{Span}(E)$ the set of all sums of the form $\sum_{i=1}^{|E|} \varepsilon_i e_i$, where $\varepsilon_i \in \{-1, 0, 1\}$.

Theorem 4 (B. Green). *Let δ and α be real numbers, $\delta \leqslant 1/8$, $0 < \alpha \leqslant \delta/32$. Assume that*

$$\left(\frac{\delta}{\alpha}\right)^2 \log\frac{1}{\delta} \leqslant \frac{\log N}{\log\log N}. \tag{6}$$

Then there is an $A \subseteq \mathbb{Z}_N$, $|A| = [\delta N]$, such that the set $\mathcal{R}_\alpha$ defined by (3) *is not contained in* $\operatorname{Span}(\Lambda)$ *for any Λ with $|\Lambda| \leqslant 2^{-12}(\delta/\alpha)^2 \log(1/\delta)$.*

The structure of $\mathcal{R}_\alpha$ in the case when α is close to δ was studied in [11]–[13] (see also [14]).

We see that results on the structure of $\mathcal{R}_\alpha$ are of importance in the combinatorial theory of numbers. In this paper we prove the following theorem.

Theorem 5. *Let δ and α be real numbers, $0<\alpha\leqslant\delta$, let A be an arbitrary subset of $\mathbb{Z}_N$ of cardinality δN, let $k\geqslant 2$ be an even number and let $\mathcal{R}_\alpha$ be the set defined by (3). Assume $B\subseteq\mathcal{R}_\alpha\setminus\{0\}$ is an arbitrary set. Then the quantity*

$$T_k(B):=|\{(r_1,\dots,r_k,r_1',\dots,r_k')\in B^{2k}\colon r_1+\dots+r_k=r_1'+\dots+r_k'\}| \tag{7}$$

is greater than or equal to

$$\frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}}|B|^{2k}. \tag{8}$$

We claim that the assertion of Theorem 5 is non-trivial in the case when δ tends to zero as N tends to infinity (if δ does not tend to zero as $N\to\infty$, then the structure of $\mathcal{R}_\alpha$ can be arbitrary [15]–[17]). Consider the simplest case $k=2$. Let the order of the cardinality of $\mathcal{R}_\alpha$ be equal to δ/α^2. By Theorem 5, the order of the number of solutions of the equation

$$r_1+r_2=r_3+r_4,\qquad r_1,r_2,r_3,r_4\in\mathcal{R}_\alpha\setminus\{0\}, \tag{9}$$

is greater than or equal to δ/α^4. Among these solutions there are three series of trivial solutions. In the first series $r_1=r_3$, $r_2=r_4$, in the second $r_1=r_4$, $r_2=r_3$ and, finally, in the third $r_1=-r_2$, $r_3=-r_4$. Therefore, equation (9) has at most $3|\mathcal{R}_\alpha|^2$ trivial solutions. The cardinality of $\mathcal{R}_\alpha$ does not exceed δ/α^2. Therefore, $3|\mathcal{R}_\alpha|^2$ is less than $3\delta^2/\alpha^4$. We see that this quantity is less than δ/α^4 as δ tends to zero. Thus, Theorem 5 states that equation (9) has non-trivial solutions. Hence, $\mathcal{R}_\alpha$ has some additive structure.

The proof of Theorem 5 will be given in § 2, where we begin with a detailed consideration of the case when $k=2$ and then prove it in the general situation.

In § 3 we generalize Theorem 5 to systems of linear equations. In our proof we use properties of the Gowers norms (see [18]).

In § 4 we apply our main result to some problems in the combinatorial theory of numbers. We show that M.-C. Chang's theorem can be derived from Theorem 5 and Rudin's inequality [19]. Moreover, we strengthen Theorem 1 (see Theorem 8). We also apply Theorem 5 to Theorem 2 .

In subsequent papers on this topic, the author intends to obtain other applications of results on large trigonometric sums to problems in the combinatorial theory of numbers.

The author is grateful to S. V. Konyagin, who suggested two ideas that enabled the author to strengthen the statement of the main result, and to N. G. Moshchevitin for his constant interest in this work.

§ 2. Proof of Theorem 5

We begin with some preliminary arguments. Let N be a positive integer and let $\widehat{A}(r)$ be the Fourier transform of the characteristic function A. As mentioned above, the following equality holds for the Fourier coefficients of A:

$$\sum_{r\in\mathbb{Z}_N}|\widehat{A}(r)|^2=N|A|. \tag{10}$$

Are there any non-trivial relations between the Fourier coefficients $\widehat{A}(r)$ other than (10)? It is obvious that the answer to this question is positive.

Consider a slightly more general situation. Let $f\colon \mathbb{Z}_N \to \mathbb{C}$ be an arbitrary complex function. The following inversion formula holds for the Fourier coefficients of $f(x)$:

$$f(x) = \frac{1}{N} \sum_{r \in \mathbb{Z}_N} \hat{f}(r) e(rx). \tag{11}$$

The function $f(x)$ is the characteristic function of some subset of $\mathbb{Z}_N$ if and only if

$$|f(x)|^2 = f(x) \tag{12}$$

for all x in $\mathbb{Z}_N$. Substituting (11) into (12), we obtain that

$$\frac{1}{N^2} \sum_{r', r''} \hat{f}(r') \overline{\hat{f}(r'')} e(r'x - r''x) = \frac{1}{N} \sum_u \hat{f}(u) e(ux). \tag{13}$$

Hence,

$$\sum_u \left(\frac{1}{N} \sum_r \hat{f}(r) \overline{\hat{f}(r-u)} \right) e(ux) = \sum_u \hat{f}(u) e(ux). \tag{14}$$

Since (14) holds for all $x \in \mathbb{Z}_N$, we have

$$\hat{f}(u) = \frac{1}{N} \sum_r \hat{f}(r) \overline{\hat{f}(r-u)}. \tag{15}$$

Hence, $f\colon \mathbb{Z}_N \to \mathbb{C}$ is a characteristic function if and only if equality (15) holds for its Fourier coefficients. It is clear that (15) also holds for the characteristic function $A(x)$ of the set A. Moreover, (15) contains all the relations between the Fourier coefficients of A: for example, Parseval's equality (2) can be obtained by putting $u = 0$.

We shall need the following generalization of (15). Let $f, g\colon \mathbb{Z}_N \to \mathbb{C}$ be arbitrary complex functions. Then

$$\frac{1}{N} \sum_r \hat{f}(r) \overline{\hat{g}(r-u)} = \sum_x f(x) \overline{g(x)} e(-xu), \tag{16}$$

and (15) obviously follows from (16).

Let us explain the basic idea of the proof of Theorem 5. Let $A \subseteq \mathbb{Z}_N$ be an arbitrary set, $|A| = \delta N$, and let $\mathcal{R}_\alpha$ be the set of large trigonometric sums given by (3). Consider a model situation. Assume that $|\widehat{A}(r)| = \alpha N$ for all $r \in \mathcal{R}_\alpha \setminus \{0\}$ and let $\widehat{A}(r) = 0$ for all $r \notin \mathcal{R}_\alpha$, $r \neq 0$ (the justification of such a hypothesis will be discussed below). Let $\delta \leqslant 1/4$ and let u be an arbitrary non-zero residue belonging to $\mathcal{R}_\alpha$. Then $|\widehat{A}(u)| = \alpha N$. Using formula (15) and the triangle inequality, we obtain that

$$\begin{aligned} \alpha N = |\widehat{A}(u)| &\leqslant \frac{1}{N} \sum_r |\widehat{A}(r)| |\widehat{A}(r-u)| \\ &\leqslant \frac{1}{N} \delta N |\widehat{A}(-u)| + \frac{1}{N} |\widehat{A}(u)| \delta N + \frac{1}{N} \sum_{r \neq 0, u} |\widehat{A}(r)| |\widehat{A}(r-u)|. \end{aligned} \tag{17}$$

Hence,

$$\frac{1}{N} \sum_{r \neq 0, u} |\widehat{A}(r)| |\widehat{A}(r-u)| \geqslant \frac{\alpha N}{2}.$$

We have $|\widehat{A}(r)| = \alpha N \mathcal{R}_\alpha(r)$ for all $r \neq 0$. Therefore,

$$\sum_{r \neq 0, u} \mathcal{R}_\alpha(r) \mathcal{R}_\alpha(r-u) \geqslant \frac{1}{2\alpha}. \tag{18}$$

It follows from (18) that for all $u \in \mathcal{R}_\alpha \setminus \{0\}$ the equation $r_1 - r_2 = u$, where $r_1, r_2 \in \mathcal{R}_\alpha \setminus \{0\}$, has at least $1/(2\alpha)$ solutions. Therefore, $\mathcal{R}_\alpha$ has non-trivial additive relations.

We now proceed to the rigorous proof of Theorem 5. We shall prove it first in the case when $k = 2$ and then in the general case. Let $k = 2$ and let B be an arbitrary subset of $\mathcal{R}_\alpha \setminus \{0\}$. We denote by $[N]$ the segment $\{1, 2, \dots, N\}$ of the positive integers.

We need the following lemma.

Lemma 1. *Let δ and α' be real numbers, $0 < \alpha' \leqslant \delta$, and let A be an arbitrary subset of $\mathbb{Z}_N$ of cardinality δN. Assume also that*

$$\mathcal{R}'_{\alpha'} = \{r \in \mathbb{Z}_N \colon \alpha' N \leqslant |\widehat{A}(r)| < 2\alpha' N\} \tag{19}$$

and let B' be an arbitrary subset of $\mathcal{R}'_{\alpha'} \setminus \{0\}$. Then

$$T_2(B') \geqslant \frac{(\alpha')^4 |B'|^4}{16\delta^3}.$$

Proof. Let

$$f_{B'}(x) = \frac{1}{N} \sum_{r \in B'} \widehat{A}(r) e(rx).$$

Generally speaking, $f_{B'}(x)$ is a complex function. It is obvious that $\hat{f}_{B'}(r) = \widehat{A}(r) B'(r)$. Consider the sum

$$\sigma = \sum_s \left| \sum_r \hat{f}_{B'}(r) \overline{\widehat{A}(r-s)} \right|^2. \tag{20}$$

Using formula (16) and Parseval's equality, we obtain that

$$\sigma = N^2 \sum_s \left| \sum_x f_{B'}(x) \overline{A(x)} e(-xs) \right|^2 = N^3 \sum_x |f_{B'}(x)|^2 A^2(x). \tag{21}$$

We estimate $\sum_x |f_{B'}(x)|^2 A^2(x)$ from below using Parseval's equality and the definition of $\mathcal{R}'_{\alpha'}$:

$$\begin{aligned} \left(\sum_x f_{B'}(x) A(x) \right)^2 &= \left(\frac{1}{N} \sum_r \hat{f}_{B'}(r) \overline{\widehat{A}(r)} \right)^2 = \left(\frac{1}{N} \sum_r |\hat{f}_{B'}(r)|^2 \right)^2 \\ &\geqslant \left(N(\alpha')^2 |B'| \right)^2 = (\alpha')^4 |B'|^2 N^2. \end{aligned} \tag{22}$$

On the other hand, we have

$$\begin{aligned} \left(\sum_x f_{B'}(x) A(x) \right)^2 &\leqslant \left(\sum_x |f_{B'}(x)|^2 A^2(x) \right) \left(\sum_x A^2(x) \right) \\ &= \delta N \left(\sum_x |f_{B'}(x)|^2 A^2(x) \right). \end{aligned} \tag{23}$$

Using inequalities (22) and (23), we obtain that

$$\sigma^2 \geqslant \frac{(\alpha')^8}{\delta^2} |B'|^4 N^8. \tag{24}$$

To obtain an upper bound for σ^2, we note that

$$\sigma = \sum_s \sum_{r,r'} \hat{f}_{B'}(r)\overline{\hat{f}_{B'}(r')}\,\overline{\widehat{A}(r-s)}\widehat{A}(r'-s)$$

$$= \sum_u \Bigl(\sum_r \hat{f}_{B'}(r)\overline{\hat{f}_{B'}(r-u)} \Bigr) \overline{\Bigl(\sum_r \widehat{A}(r)\overline{\widehat{A}(r-u)} \Bigr)}, \tag{25}$$

whence

$$\sigma^2 \leqslant \sum_u \Bigl| \sum_r \hat{f}_{B'}(r)\overline{\hat{f}_{B'}(r-u)} \Bigr|^2 \sum_u \Bigl| \sum_r \widehat{A}(r)\overline{\widehat{A}(r-u)} \Bigr|^2 = \sigma_1\sigma_2. \tag{26}$$

Using formula (15) and Parseval's equality, we obtain that

$$\sigma_2 = N^2 \sum_u |\widehat{A}(u)|^2 = \delta N^4. \tag{27}$$

Since $\hat{f}_{B'}(r) = \widehat{A}(r)B'(r)$ and $B' \subseteq \mathcal{R}'_{\alpha'} \setminus \{0\}$, we have $|\hat{f}_{B'}(r)| \leqslant 2\alpha' B'(r)N$. Hence,

$$\sigma_1 \leqslant 16(\alpha')^4 T_2(B')N^4. \tag{28}$$

Substituting (27) and (28) into (24), we obtain that $T_2(B') \geqslant (\alpha')^4|B'|^4/(16\delta^3)$. The lemma is proved.

Let

$$B_i = \{r \in B\colon 2^{i-1}\alpha N \leqslant |\widehat{A}(r)| < 2^i\alpha N\}, \qquad i \geqslant 1.$$

It is clear that $B = \bigsqcup_{i\geqslant 1} B_i$. Applying Lemma 1 to every B_i, we obtain that $T_2(B_i) \geqslant (2^{i-1}\alpha)^4|B_i|^4/(16\delta^3)$, $i \geqslant 1$. Hence,

$$T_2(B) \geqslant \sum_i T_2(B_i) \geqslant \frac{\alpha^4}{2^8\delta^3} \sum_i 2^{4i}|B_i|^4. \tag{29}$$

We have $|B| = \sum_i |B_i|$. The Cauchy–Bunyakovsky inequality implies that

$$|B|^4 = \Bigl(\sum_i 2^i 2^{-i}|B_i| \Bigr)^4 \leqslant \Bigl(\sum_i 2^{4i}|B_i|^4 \Bigr) \Bigl(\sum_i 2^{-4i/3} \Bigr)^3 \leqslant \sum_i 2^{4i}|B_i|^4. \tag{30}$$

Substituting (30) into (29), we obtain the inequality

$$T_2(B) \geqslant \frac{\alpha^4}{2^8\delta^3}|B|^4. \tag{31}$$

Now consider the general case when $k \geqslant 2$.

Proof of Theorem 5. First we prove an analogue of Lemma 1.

Lemma 2. *Let δ and α' be real numbers, $0 < \alpha' \leqslant \delta$, let A be an arbitrary subset of $\mathbb{Z}_N$ of cardinality δN and let $k \geqslant 2$ be an even number. Assume also that*

$$\mathcal{R}'_{\alpha'} = \{r \in \mathbb{Z}_N\colon \alpha' N \leqslant |\widehat{A}(r)| < 2\alpha' N\} \tag{32}$$

and let B' be an arbitrary subset of $\mathcal{R}'_{\alpha'} \setminus \{0\}$. Then

$$T_k(B') \geqslant \frac{\delta(\alpha')^{2k}|B'|^{2k}}{(2\delta)^{2k}}.$$

Proof. Let $f_{B'}(x)$ be the function defined by the formula

$$f_{B'}(x) = \frac{1}{N} \sum_{r \in B'} \widehat{A}(r) e(rx).$$

Consider the sum

$$\sigma = \Big(\sum_x f_{B'}(x) A(x) \Big)^k . \tag{33}$$

Estimating σ from below as in Lemma 1, we obtain that

$$\sigma \geqslant \big((\alpha')^2 |B'| N \big)^k . \tag{34}$$

Since k is an even number, it has the form $k = 2k'$, $k' \in \mathbb{N}$. Using Hölder's inequality, we obtain that

$$\begin{aligned} \sigma &= \Big(\sum_x f_{B'}(x) A(x) \Big)^{2k'} \leqslant \Big(\sum_x |f_{B'}(x)|^{2k'} A^2(x) \Big) \Big(\sum_x A(x) \Big)^{k-1} \\ &= \Big(\sum_x |f_{B'}(x)|^{2k'} A^2(x) \Big) (\delta N)^{k-1}. \end{aligned} \tag{35}$$

Hence,

$$(\sigma')^2 = \Big(\sum_x |f_{B'}(x)|^{2k'} A^2(x) \Big)^2 \geqslant \delta^2 \frac{(\alpha')^{4k}}{\delta^{2k}} |B'|^{2k} N^2. \tag{36}$$

On the other hand, the inversion formula (11) implies that

$$\begin{aligned} \sigma' &= \sum_x |f_{B'}(x)|^{2k'} A^2(x) \\ &= \frac{1}{N^{2k'+2}} \sum_x \sum_{r_1, \ldots, r_{k'}, r'_1, \ldots, r'_{k'}} \sum_{y,z} \hat{f}_{B'}(r_1) \cdots \hat{f}_{B'}(r_{k'}) \overline{\hat{f}_{B'}(r'_1)} \cdots \overline{\hat{f}_{B'}(r'_{k'})} \widehat{A}(y) \overline{\widehat{A}(z)} \\ &\qquad \times e\big(x(r_1 + \cdots + r_{k'} - r'_1 - \cdots - r'_{k'}) \big) e\big(x(y-z) \big) \\ &= \frac{1}{N^{2k'+1}} \sum_{u,y} \sum_{\substack{r_1, \ldots, r_{k'}, r'_1, \ldots, r'_{k'} \\ r_1 + \cdots + r_{k'} = r'_1 + \cdots + r'_{k'} - u}} \hat{f}_{B'}(r_1) \cdots \hat{f}_{B'}(r_{k'}) \\ &\qquad \times \overline{\hat{f}_{B'}(r'_1)} \cdots \overline{\hat{f}_{B'}(r'_{k'})} \widehat{A}(y) \overline{\widehat{A}(y-u)} \\ &= \frac{1}{N^{2k'+1}} \sum_u \Big(\sum_y \widehat{A}(y) \overline{\widehat{A}(y-u)} \Big) \\ &\qquad \times \Bigg(\sum_{\substack{r_1, \ldots, r_{k'}, r'_1, \ldots, r'_{k'} \\ r_1 + \cdots + r_{k'} = r'_1 + \cdots + r'_{k'} - u}} \hat{f}_{B'}(r_1) \cdots \hat{f}_{B'}(r_{k'}) \overline{\hat{f}_{B'}(r'_1)} \cdots \overline{\hat{f}_{B'}(r'_{k'})} \Bigg). \end{aligned} \tag{37}$$

Hence,

$$\begin{aligned}(\sigma')^2 &\leqslant \frac{1}{N^{4k'+2}} \sum_u \Bigl| \sum_y \widehat{A}(y)\overline{\widehat{A}(y-u)} \Bigr|^2 \\ &\quad \times \sum_u \Bigl| \sum_{\substack{r_1,\dots,r_{k'},r'_1,\dots,r'_{k'} \\ r_1+\dots+r_{k'}=r'_1+\dots+r'_{k'}-u}} \hat{f}_{B'}(r_1)\cdots\hat{f}_{B'}(r_{k'})\overline{\hat{f}_{B'}(r'_1)}\cdots\overline{\hat{f}_{B'}(r'_{k'})} \Bigr|^2 \\ &= \frac{1}{N^{4k'+2}}\sigma_1\sigma_2. \end{aligned} \tag{38}$$

Using formula (15) and Parseval's equality, we obtain that

$$\sigma_1 = N^2 \sum_u |\widehat{A}(u)|^2 = \delta N^4. \tag{39}$$

Since $B' \subseteq \mathcal{R}'_{\alpha'} \setminus \{0\}$, we have $|\hat{f}_{B'}(r)| \leqslant 2\alpha' B'(r)N$. Hence,

$$\begin{aligned}\sigma_2 &\leqslant \bigl((2\alpha' N)^{2k'}\bigr)^2 \sum_u \Bigl| \sum_{\substack{r_1,\dots,r_{k'},r'_1,\dots,r'_{k'} \\ r_1+\dots+r_{k'}=r'_1+\dots+r'_{k'}-u}} B'(r_1)\cdots B'(r_{k'})B'(r'_1)\cdots B'(r'_{k'}) \Bigr|^2 \\ &= (2\alpha' N)^{2k} T_k(B'). \end{aligned} \tag{40}$$

Using equalities (38), (39) and inequalities (36), (40), we obtain that

$$T_k(B') \geqslant \frac{\delta(\alpha')^{2k}|B'|^{2k}}{(2\delta)^{2k}}. \tag{41}$$

The lemma is proved.

Let

$$B_i = \{r \in B \colon 2^{i-1}\alpha N \leqslant |\widehat{A}(r)| < 2^i \alpha N\}, \qquad i \geqslant 1.$$

It is clear that $B = \bigsqcup_{i\geqslant 1} B_i$. Applying Lemma 2 to every B_i, we obtain that $T_k(B_i) \geqslant \delta(2^{i-1}\alpha)^{2k}|B_i|^{2k}/(2\delta)^{2k}$, $i \geqslant 1$. Hence,

$$T_k(B) \geqslant \sum_i T_k(B_i) \geqslant \frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}} \sum_i 2^{2ki}|B_i|^{2k}. \tag{42}$$

We have $|B| = \sum_i |B_i|$. Using Hölder's inequality, we obtain that

$$\begin{aligned}|B|^{2k} &= \Bigl(\sum_i 2^i 2^{-i}|B_i|\Bigr)^{2k} \leqslant \Bigl(\sum_i 2^{2ki}|B_i|^{2k}\Bigr)\Bigl(\sum_i 2^{-2ki/(2k-1)}\Bigr)^{2k-1} \\ &\leqslant \sum_i 2^{2ki}|B_i|^{2k}. \end{aligned} \tag{43}$$

Substituting (43) into (42), we obtain the inequality

$$T_k(B) \geqslant \frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}}|B|^{2k}. \tag{44}$$

The theorem is proved.

§ 3. Systems of linear equations with elements in the set of large trigonometric sums

Let k be a positive integer and let $d \geqslant 0$ be an integer. Let $A = (a_{ij})$ be the $2^{d+1}k \times (d+1)$ matrix whose elements a_{ij} are defined by the formula

$$a_{ij} = \begin{cases} 1 & \text{if the } (i-1)\text{st coefficient in the binary expansion of } (j-1) \\ & \text{is equal to 1 and } 1 \leqslant j \leqslant 2^d k, \\ -1 & \text{if the } (i-1)\text{st coefficient in the binary expansion of } (j-1) \\ & \text{is equal to 1 and } 2^d k < j \leqslant 2^{d+1}k, \\ 0 & \text{otherwise.} \end{cases} \tag{45}$$

Recall that the binary expansion of a positive integer n is defined by the rule $n = \sum n_l \cdot 2^{l-1}$, where $l \geqslant 1$ and $n_l \in \{0,1\}$.

For example, when $k=2$ and $d=2$ we have

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & -1 & -1 \end{pmatrix}.$$

In this section we prove the following theorem.

Theorem 6. *Let δ and α be real numbers, $0 < \alpha \leqslant \delta$, let A be an arbitrary subset of $\mathbb{Z}_N$ of cardinality δN, let k be a positive integer, let $d \geqslant 0$ be an integer and let $\mathcal{R}_\alpha$ be the set defined by* (3). *Let $B \subseteq \mathcal{R}_\alpha \setminus \{0\}$ be an arbitrary set. Consider the system of equations*

$$\sum_{j=1}^{2^{d+1}k} a_{ij} r_j = 0, \qquad i = 1,2,\dots,d+1, \tag{46}$$

where the elements a_{ij} of the matrix A are defined by formula (45) *and $r_j \in B$ for all j. Then the number of solutions of the system* (46) *is greater than or equal to*

$$\left(\frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}} |B|^{2k} \right)^{2^d}. \tag{47}$$

To make it clear that Theorem 6 is a generalization of Theorem 5, it is sufficient to put the d in Theorem 6 equal to zero.

To prove Theorem 6, we need some properties of the Gowers norms (see [18]).

Let $d \geqslant 0$ be an integer and let $\{0,1\}^d = \{\omega = (\omega_1,\dots,\omega_d) \colon \omega_j \in \{0,1\}, j = 1,2,\dots,d\}$ be the ordinary d-dimensional cube. If $\omega \in \{0,1\}^d$, then $|\omega|$ is defined to be $\omega_1 + \dots + \omega_d$. If $h = (h_1,\dots,h_d) \in \mathbb{Z}_N^d$, then $\omega \cdot h := \omega_1 h_1 + \dots + \omega_d h_d$. Let $\mathcal{C}$ be the operator of complex conjugation. If n is a positive integer, then $\mathcal{C}^n$ stands for the nth power of this operator. Let $\|\omega\| = \sum_{i=1}^d \omega_i \cdot 2^{i-1} + 1$. For every $\omega \in \{0,1\}^d$ we define a map from $\mathbb{Z}_N^{2^d}$ to $\mathbb{Z}_N$, which we denote by the same symbol ω, by the rule: if $\vec{r} \in \mathbb{Z}_N^{2^d}$, then $\omega(\vec{r})$ is the $\|\omega\|$th component of the vector $\vec{r}$.

Definition 1. Let $f \colon \mathbb{Z}_N \to \mathbb{C}$ be an arbitrary function. The *uniform Gowers norm* (or, briefly, the *Gowers norm*) of f is defined to be

$$\|f\|_{U^d} := \left(\frac{1}{N^{d+1}} \sum_{x \in \mathbb{Z}_N, h \in \mathbb{Z}_N^d} \prod_{\omega \in \{0,1\}^d} \mathcal{C}^{|\omega|} f(x + \omega \cdot h) \right)^{1/2^d}. \tag{48}$$

We shall need the following lemma (see [18]).

Lemma 3 (the motonicity inequality for Gowers norms). *Let $f\colon \mathbb{Z}_N \to \mathbb{C}$ be an arbitrary function and let d be a positive integer. Then*

$$\|f\|_{U^d} \leqslant \|f\|_{U^{d+1}}. \tag{49}$$

Other properties of the Gowers norms can be found in [18].

Let us prove the following lemma.

Lemma 4. *Let δ and α' be real numbers, $0 < \alpha' \leqslant \delta$, let A be an arbitrary subset of $\mathbb{Z}_N$ of cardinality δN, let k be a positive integer and let $d \geqslant 0$ be an integer. Assume, moreover, that*

$$\mathcal{R}'_{\alpha'} = \{r \in \mathbb{Z}_N \colon \alpha' N \leqslant |\widehat{A}(r)| < 2\alpha' N\} \tag{50}$$

and let B' be an arbitrary subset of $\mathcal{R}'_{\alpha'} \setminus \{0\}$. Then the number of solutions of the system (46) with $r_j \in B'$ is greater than or equal to

$$\left(\frac{\delta(\alpha')^{2k}}{2^{2k}\delta^{2k}} |B'|^{2k} \right)^{2^d}. \tag{51}$$

Proof. Let $f(x)$ be the function defined by the formula

$$f(x) = \frac{1}{N} \sum_{r \in B'} \widehat{A}(r) e(rx).$$

Using Hölder's inequality, we obtain that

$$\begin{aligned} \left| \sum_x f(x)A(x) \right|^{2k} &\leqslant \left(\sum_x |f(x)|^{2k} \right) \left(\sum_x A(x) \right)^{2k-1} \\ &= \left(\sum_x |f(x)|^{2k} \right) (\delta N)^{2k-1}. \end{aligned} \tag{52}$$

On the other hand, using Parseval's equality and the definition of $\mathcal{R}'_{\alpha'}$, we obtain that

$$\sum_x f(x)A(x) = \frac{1}{N} \sum_r \hat{f}(r) \overline{\widehat{A}(r)} = \frac{1}{N} \sum_r |\hat{f}(r)|^2 \geqslant (\alpha')^2 |B'| N. \tag{53}$$

Consider the sum

$$\sigma = \| \, |f|^{2k} \, \|_{U^0} = \| \, |f|^{2k} \, \|_{U^1} = \frac{1}{N} \sum_x |f(x)|^{2k}. \tag{54}$$

It follows from (52) and (53) that

$$\sigma \geqslant \frac{\delta (\alpha')^{4k}}{\delta^{2k}} |B'|^{2k}. \tag{55}$$

Using Lemma 3, we obtain that

$$\begin{aligned} \sigma^{2^d} &\leqslant \frac{1}{N^{d+1}} \sum_{x \in \mathbb{Z}_N} \sum_{h \in \mathbb{Z}_N^d} \prod_{\omega \in \{0,1\}^d} |f(x + \omega \cdot h)|^{2k} \\ &= \frac{1}{N^{d+1}} \sum_{x \in \mathbb{Z}_N} \sum_{h \in \mathbb{Z}_N^d} \left| \prod_{\omega \in \{0,1\}^d} f(x + \omega \cdot h) \right|^{2k}. \end{aligned} \tag{56}$$

Using the inversion formula (11), we obtain that

$$\prod_{\omega\in\{0,1\}^d} f(x+\omega\cdot h) = \frac{1}{N^{2d}} \sum_{\vec{r}\in\mathbb{Z}_N^{2d}} \prod_{\omega\in\{0,1\}^d} \hat{f}\big(\omega(\vec{r})\big)e\big(\omega(\vec{r})(x+\omega\cdot h)\big). \tag{57}$$

Hence,

$$\begin{aligned}\sigma^{2^d} = \frac{1}{N^{2^{d+1}k+d+1}} &\sum_{x\in\mathbb{Z}_N} \sum_{h\in\mathbb{Z}_N^d} \sum_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}\in\mathbb{Z}_N^{2^d}} \\ &\times \prod_{i=1}^{k} \prod_{\omega^{(i)}\in\{0,1\}^d} \hat{f}\big(\omega^{(i)}(r^{(i)})\big)e\big(\omega^{(i)}(r^{(i)})(x+\omega^{(i)}\cdot h)\big) \\ &\times \prod_{i=k+1}^{2k} \prod_{\omega^{(i)}\in\{0,1\}^d} \overline{\hat{f}\big(\omega^{(i)}(r^{(i)})\big)}e\big(-\omega^{(i)}(r^{(i)})(x+\omega^{(i)}\cdot h)\big). \end{aligned} \tag{58}$$

We denote by Σ the system of equations

$$\begin{gathered} \sum_{i=1}^{k} \sum_{\omega^{(i)}\in\{0,1\}^d} \omega^{(i)}(r^{(i)}) = \sum_{i=k+1}^{2k} \sum_{\omega^{(i)}\in\{0,1\}^d} \omega^{(i)}(r^{(i)}), \\ \sum_{i=1}^{k} \sum_{\omega^{(i)}\in\{0,1\}^d,\omega_1^{(i)}=1} \omega^{(i)}(r^{(i)}) = \sum_{i=k+1}^{2k} \sum_{\omega^{(i)}\in\{0,1\}^d,\omega_1^{(i)}=1} \omega^{(i)}(r^{(i)}), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \sum_{i=1}^{k} \sum_{\omega^{(i)}\in\{0,1\}^d,\omega_d^{(i)}=1} \omega^{(i)}(r^{(i)}) = \sum_{i=k+1}^{2k} \sum_{\omega^{(i)}\in\{0,1\}^d,\omega_d^{(i)}=1} \omega^{(i)}(r^{(i)}). \end{gathered}$$

Then

$$\begin{aligned}\sigma^{2^d} &= \frac{1}{N^{2^{d+1}k+d+1}} \sum_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}\in\mathbb{Z}_N^{2^d}} \prod_{i=1}^{k} \prod_{\omega^{(i)}\in\{0,1\}^d} \hat{f}\big(\omega^{(i)}(r^{(i)})\big) \\ &\quad\times \prod_{i'=k+1}^{2k} \prod_{\omega^{(i')}\in\{0,1\}^d} \overline{\hat{f}\big(\omega^{(i')}(r^{(i')})\big)} \\ &\quad\times \sum_{x\in\mathbb{Z}_N} \sum_{h\in\mathbb{Z}_N^d} e\big(\omega^{(i)}(r^{(i)})(x+\omega^{(i)}\cdot h) - \omega^{(i')}(r^{(i')})(x+\omega^{(i')}\cdot h)\big) \\ &= \frac{1}{N^{2^{d+1}k}} \sum_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}\in\Sigma} \prod_{i=1}^{k} \prod_{\omega^{(i)}\in\{0,1\}^d} \hat{f}\big(\omega^{(i)}(r^{(i)})\big) \\ &\quad\times \prod_{i=k+1}^{2k} \prod_{\omega^{(i)}\in\{0,1\}^d} \overline{\hat{f}\big(\omega^{(i)}(r^{(i)})\big)}. \end{aligned} \tag{59}$$

The sum in (59) is taken over the $r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}$ that satisfy Σ. It is easy to verify that this system coincides with (46).

Since $\hat{f}_{B'}(r) = \widehat{A}(r)B'(r)$ and $B' \subseteq \mathcal{R}'_{\alpha'} \setminus \{0\}$, we have $|\hat{f}_{B'}(r)| \leqslant 2\alpha' B'(r)N$. Hence,

$$\sigma^{2^d} \leqslant (2^{2k}(\alpha')^{2k})^{2^d} N^{2^{d+1}k}. \tag{60}$$

Using inequalities (55), (56) and (60), we finally obtain that

$$\begin{aligned}\sum_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)} \in \Sigma} 1 &\geqslant \left(\frac{\delta(\alpha')^{4k}}{\delta^{2k}}|B'|^{2k}\right)^{2^d} \frac{1}{(2^{2k}(\alpha')^{2k})^{2^d}} \\ &= \left(\frac{\delta(\alpha')^{2k}}{2^{2k}\delta^{2k}}|B'|^{2k}\right)^{2^d}. \end{aligned} \tag{61}$$

The sum in (61) is taken over the $r^{(i)}$, $i = 1, 2, \dots, 2k$, whose components belong to B'. In other words, the number of solutions of the system (46) with $r_i \in B'$ is greater than or equal to

$$\left(\frac{\delta(\alpha')^{2k}}{2^{2k}\delta^{2k}}|B'|^{2k}\right)^{2^d}.$$

The lemma is proved.

Proof of Theorem 6. Let

$$B_i = \{r \in B \colon 2^{i-1}\alpha N \leqslant |\widehat{A}(r)| < 2^i \alpha N\}, \qquad i \geqslant 1.$$

It is clear that $B = \bigsqcup_{i \geqslant 1} B_i$.

Let E be a set. We denote by $S_{k,d}(E)$ the number of solutions of the system (46) with $r_i \in E$. Applying Lemma 4 to every B_i, we obtain that

$$S_{k,d}(B_i) \geqslant \left(\frac{\delta(2^{i-1}\alpha)^{2k}}{2^{2k}\delta^{2k}}|B_i|^{2k}\right)^{2^d},$$

where $i \geqslant 1$. Hence,

$$S_{k,d}(B) \geqslant \sum_i S_{k,d}(B_i) \geqslant \left(\frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}}\right)^{2^d} \sum_i (2^{2ki}|B_i|^{2k})^{2^d}. \tag{62}$$

We have $|B| = \sum_i |B_i|$. Using Hölder's inequality, we obtain that

$$\begin{aligned}|B|^{2^{d+1}k} &= \left(\sum_i 2^i 2^{-i}|B_i|\right)^{2^{d+1}k} \\ &\leqslant \left(\sum_i (2^{2ki}|B_i|^{2k})^{2^d}\right)\left(\sum_i 2^{-(2^{d+1}ki)/(2^{d+1}k-1)}\right)^{2^{d+1}k-1} \\ &\leqslant \sum_i (2^{2ki}|B_i|^{2k})^{2^d}. \end{aligned} \tag{63}$$

Substituting (63) into (62), we obtain the desired inequality

$$S_{k,d}(B) \geqslant \left(\frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}}|B|^{2k}\right)^{2^d}. \tag{64}$$

The theorem is proved.

§ 4. Applications to problems in the combinatorial theory of numbers

In the proof of Theorem 1, Chang used Rudin's theorem [19] (see also [20]) on the dissociative subsets of $\mathbb{Z}_N$. A set $\mathcal{D} = \{d_1, \dots, d_{|\mathcal{D}|}\} \subseteq \mathbb{Z}_N$ is said to be *dissociative* if the congruence

$$\sum_{i=1}^{|\mathcal{D}|} \varepsilon_i d_i \equiv 0 \pmod N, \tag{65}$$

where $\varepsilon_i \in \{-1, 0, 1\}$, implies that all the ε_i are equal to zero.

Theorem 7 (W. Rudin). *There is an absolute constant $C > 0$ such that for any dissociative set $\mathcal{D} \subseteq \mathbb{Z}_N$ and any complex numbers $a_n \in \mathbb{C}$ the inequality*

$$\frac{1}{N} \sum_{x \in \mathbb{Z}_N} \biggl| \sum_{n \in \mathcal{D}} a_n e(nx) \biggr|^p \leqslant (C\sqrt{p})^p \biggl(\sum_{n \in \mathcal{D}} |a_n|^2 \biggr)^{p/2} \tag{66}$$

holds for all integers $p \geqslant 2$.

The proofs of Theorem 7 and Chang's theorem can also be found in [9], [21]. We shall use Rudin's theorem and Theorem 5 to derive an analogue of Theorem 1, which only differs from Chang's theorem in that it gives a somewhat weaker estimate for the cardinality of Λ.

Proposition 1. *Let δ and α be real numbers, $0 < \alpha \leqslant \delta \leqslant 1$, let A be an arbitrary subset of $\mathbb{Z}_N$ of cardinality δN and let $\mathcal{R}_\alpha$ be the set defined by* (3). *Then there is a set $\mathcal{D} = \{d_1, \dots, d_{|\mathcal{D}|}\} \subseteq \mathbb{Z}_N$, $|\mathcal{D}| \leqslant 2^8 C^2 (\delta/\alpha)^2 \log(1/\delta)$, such that every element r of $\mathcal{R}_\alpha$ can be represented in the form*

$$r \equiv \sum_{i=1}^{|\mathcal{D}|} \varepsilon_i d_i \pmod N, \tag{67}$$

where $\varepsilon_i \in \{-1, 0, 1\}$ and C is the absolute constant occurring in Rudin's inequality (66).

Proof. Let $k = 2\lceil \log(1/\delta) \rceil$ and let $\mathcal{D} \subseteq \mathcal{R}_\alpha$ be a *maximal* dissociative set. Since $\mathcal{D}$ is dissociative, we have $0 \notin \mathcal{D}$. Using Theorem 5, we obtain the estimate

$$T_k(\mathcal{D}) \geqslant \frac{\delta \alpha^{2k}}{2^{4k} \delta^{2k}} |\mathcal{D}|^{2k}. \tag{68}$$

On the other hand,

$$T_k(\mathcal{D}) \leqslant C^{2k} 2^k k^k |\mathcal{D}|^k, \tag{69}$$

where C is the absolute constant occurring in Theorem 7. Indeed, let the a_n in (66) be equal to $\mathcal{D}(n)$ and let $p = 2k$. Then the left-hand side of (66) is $T_k(\mathcal{D})$ while the right-hand side is equal to $C^{2k} 2^k k^k |\mathcal{D}|^k$. We have $k = 2\lceil \log(1/\delta) \rceil$. Using (68) and (69), we obtain that $|\mathcal{D}| \leqslant 2^8 C^2 (\delta/\alpha)^2 \log(1/\delta)$. Since $\mathcal{D}$ is a maximal dissociative subset of $\mathcal{R}_\alpha$, every element r of $\mathcal{R}_\alpha$ can be represented in the form $r \equiv \sum_{i=1}^{|\mathcal{D}|} \varepsilon_i d_i \pmod N$, where $d_i \in \mathcal{D}$ and $\varepsilon_i \in \{-1, 0, 1\}$. Note that it is only the constant factors in the estimate $|\mathcal{D}| \leqslant 2^8 C^2 (\delta/\alpha)^2 \log(1/\delta)$ that are different from those in the corresponding estimate in Chang's theorem. The proposition is proved.

We shall now strengthen Chang's theorem. Our method of proof has much in common with the methods used in [22]–[24].

Theorem 8. *Let N be a positive integer, $(N,2)=1$, let δ and α be real numbers, $0<\alpha\leqslant\delta\leqslant 1/16$, let A be an arbitrary subset of $\mathbb{Z}_N$ of cardinality δN and let $\mathcal{R}_\alpha$ be the set defined by* (3). *Then there is a $\Lambda^*\subseteq\mathbb{Z}_N$,*

$$|\Lambda^*|\leqslant\max\bigl(2^{12}(\delta/\alpha)^2\log(1/\delta),2^6\log^2(1/\delta)\bigr), \tag{70}$$

such that for any residue $r\in\mathcal{R}_\alpha$ there is a set $\lambda_1^*,\dots,\lambda_M^*$ of at most $8\log(1/\delta)$ elements of Λ^* such that

$$r\equiv\sum_{i=1}^{M}\varepsilon_i\lambda_i^* \pmod N, \tag{71}$$

where $\varepsilon_i\in\{-1,0,1\}$.

If, moreover, N is a prime, then there is a set $\widetilde{\Lambda}\subseteq\mathbb{Z}_N$,

$$|\widetilde{\Lambda}|\leqslant 2^{12}(\delta/\alpha)^2\log(1/\delta)\log\log(1/\delta), \tag{72}$$

such that for every residue $r\in\mathcal{R}_\alpha$ there is a set $\tilde{\lambda}_1,\dots,\tilde{\lambda}_M$ of at most $8\log(1/\delta)$ elements of $\widetilde{\Lambda}$ such that

$$r\equiv\sum_{i=1}^{M}\varepsilon_i\tilde{\lambda}_i \pmod N, \tag{73}$$

where $\varepsilon_i\in\{-1,0,1\}$.

Remark 1. Unlike the residues in Theorem 1, the residues $\lambda_1^*,\dots,\lambda_M^*\in\Lambda^*$ in (71), as well as the residues $\tilde{\lambda}_1,\dots,\tilde{\lambda}_M\in\widetilde{\Lambda}$ in (73) (see Theorem 8), need not be distinct.

Corollary 1. *Let N be a positive integer, $(N,6)=1$, let δ and α be real numbers, $0<\alpha\leqslant\delta\log^{1/2}(1/\delta)$, and let $\mathcal{R}_\alpha$ be the set defined by* (3). *Then there is a $\Lambda^*\subseteq\mathbb{Z}_N$, $|\Lambda^*|\leqslant 2^{12}(\delta/\alpha)^2\log(1/\delta)$, such that for any residue $r\in\mathcal{R}_\alpha$ there is a set $\lambda_1^*,\dots,\lambda_M^*$ of at most $8\log(1/\delta)$ elements of Λ^* such that $r\equiv\sum_{i=1}^{M}\varepsilon_i\lambda_i^*$ $\pmod N$, where $\varepsilon_i\in\{-1,0,1\}$.*

In the proof of Theorem 8 we shall use several auxiliary assertions and definitions.

Definition 2. Let k and s be positive integers. Consider a family $\Lambda(k,s)$ of subsets of $\mathbb{Z}_N$ that has the following property. If $\Lambda=\{\lambda_1,\dots,\lambda_{|\Lambda|}\}$ belongs to $\Lambda(k,s)$, then the congruence

$$\sum_{i=1}^{|\Lambda|}\lambda_i s_i\equiv 0 \pmod N,\qquad \lambda_i\in\Lambda,\quad s_i\in\mathbb{Z},\quad |s_i|\leqslant s,\quad \sum_{i=1}^{|\Lambda|}|s_i|\leqslant 2k, \tag{74}$$

implies that all the s_i are equal to zero.

The definition of $\Lambda(k,1)$ can be found in [25].

Note that for every $\Lambda\in\Lambda(k,s)$ we have $0\notin\Lambda$ and $\Lambda\cap(-\Lambda)=\varnothing$. It is implicit in what follows that the equality of two elements of $\mathbb{Z}_N$ will always mean that they are equal modulo N. For sets belonging to $\Lambda(k,s)$, the following upper bound holds for the quantities T_k.

Assertion 1. *Let k and s be positive integers, let Λ be an arbitrary set belonging to the family $\Lambda(k,s)$ and assume that $|\Lambda| \geqslant k$. Then*

$$T_k(\Lambda) \leqslant 2^{3k} k^k |\Lambda|^k \max\left\{1, \left(\frac{k}{|\Lambda|}\right)^k |\Lambda|^{k/s}\right\}. \tag{75}$$

Example 1. Let $\log|\Lambda| \geqslant \log^2 k$ and let Λ be an arbitrary set belonging to the family $\Lambda(k,3)$. Using the inequality (75), we obtain that $T_k(\Lambda) \leqslant 2^{20k} k^k |\Lambda|^k$. It is obvious that the order of this estimate cannot be improved, which means that $T_k(\Lambda) \geqslant \binom{|\Lambda|}{k}(k!)^2 \gg e^{-k} k^k |\Lambda|^k$ for every Λ and every positive integer k such that $\log|\Lambda| \geqslant \log^2 k$.

Proof of Assertion 1. Let $x \in \mathbb{Z}_N$ be an arbitrary residue and let $N_k(x)$ be the number of $(\lambda_1,\dots,\lambda_k)$ such that the λ_i belong to Λ and $\lambda_1 + \dots + \lambda_k = x$. Then $T_k(\Lambda) = \sum_{x\in\mathbb{Z}_N} N_k^2(x)$. Let $s_1,\dots,s_l$ be positive integers such that $s_1+\dots+s_l = k$. To fix ideas, we assume that $s_1,\dots,s_l$ are arranged in descending order: $s_1 \geqslant s_2 \geqslant \dots \geqslant s_l \geqslant 1$.

Let $E(s_1,\dots,s_l)(x) = \{(\lambda_1,\dots,\lambda_k)$: among $\lambda_1,\dots,\lambda_k$ there are precisely s_1 numbers equal to $\tilde\lambda_1$, precisely s_2 numbers equal to $\tilde\lambda_2, \dots$ and precisely s_l numbers equal to $\tilde\lambda_l$, so that $s_1\tilde\lambda_1 + \dots + s_l\tilde\lambda_l = x$, and the $\tilde\lambda_i$ are all distinct$\}$. For brevity we denote $E(s_1,\dots,s_l)(x)$ by $E(\vec s)(x)$. Recall that the numbers $s_1,\dots,s_l$ in the definition of $E(\vec s)(x) = E(s_1,\dots,s_l)(x)$ are such that $\sum_{i=1}^l s_i = k$. Then

$$N_k(x) = \sum_{\vec s} |E(\vec s)(x)|,$$

where the sum is taken over all vectors for which $\sum_{i=1}^l s_i = k$. Hence,

$$\sigma = T_k(\Lambda) = \sum_{x\in\mathbb{Z}_N} \left(\sum_{\vec s} |E(\vec s)(x)|\right)^2. \tag{76}$$

Let $\vec s = (s_1,\dots,s_l)$ and $G = G(\vec s) = \{i\colon s_i \leqslant s\}$, $B = B(\vec s) = \{i\colon s_i > s\}$. Then $|G(\vec s)| + |B(\vec s)| = l(\vec s) = l$. We claim that

$$l \leqslant k - s|B|. \tag{77}$$

Indeed,

$$k = \sum_{i\in G} s_i + \sum_{i\in B} s_i' \geqslant |G| + (s+1)|B| = l + s|B|, \tag{78}$$

and (77) follows.

Lemma 5.

$$|E(\vec s)(x)| \leqslant \frac{k!}{s_1!\cdots s_l!} |\Lambda|^{|B(\vec s)|} \tag{79}$$

for all $\vec s$ with $\sum_{i=1}^l s_i = k$ and all $x \in \mathbb{Z}_N$.

Proof. Let $(\lambda_1,\dots,\lambda_k)$ be an arbitrary set belonging to $E(\vec s)(x)$. Then $\sum_{i=1}^k \lambda_i = \sum_{i=1}^l s_i\tilde\lambda_i = x$, where the $\tilde\lambda_i \in \{\lambda_1,\dots,\lambda_k\}$ are distinct. Consider another element $(\lambda_1',\dots,\lambda_k')$ of $E(\vec s)(x)$ with $\sum_{i=1}^k \lambda_i' = \sum_{i=1}^l s_i\tilde\lambda_i' = x$, where the $\tilde\lambda_i' \in \{\lambda_1',\dots,\lambda_k'\}$

are distinct. Assume that $\tilde{\lambda}_i = \tilde{\lambda}'_i$ for all $i \in B(\vec{s})$. We claim that $\tilde{\lambda}_i = \tilde{\lambda}'_i$ for all $i \in G(\vec{s})$. We have $\sum_{i=1}^{l} s_i \tilde{\lambda}_i = x = \sum_{i=1}^{l} s_i \tilde{\lambda}'_i$. Hence,

$$\sum_{i \in G} s_i \tilde{\lambda}_i = \sum_{i \in G} s_i \tilde{\lambda}'_i.$$

Moreover, $\Lambda \cap (-\Lambda) = \varnothing$. Therefore,

$$\sum_{i \in G} s_i \tilde{\lambda}_i - \sum_{i \in G} s_i \tilde{\lambda}'_i = \sum_{i} s'_i \lambda^0_i = 0,$$

where $s'_i \in \mathbb{Z}$, $|s'_i| \leqslant s$, $\sum_i |s'_i| \leqslant 2k$ and the $\lambda^0_i \in \Lambda$ are distinct. The definition of $\Lambda(k, s)$ implies that all the s'_i are equal to zero. Hence, $\tilde{\lambda}_i = \tilde{\lambda}'_i$ for all $i \in G(\vec{s})$. Therefore, $(\lambda'_1, \dots, \lambda'_k)$ can be obtained from $(\lambda_1, \dots, \lambda_k)$ by a permutation. By the definition of $E(\vec{s})(x)$, among $\lambda_1, \dots, \lambda_k$ there are precisely s_1 equal to $\tilde{\lambda}_1$, s_2 equal to $\tilde{\lambda}_2, \dots$ and s_l equal to $\tilde{\lambda}_l$, and $s_1\tilde{\lambda}_1 + \dots + s_l\tilde{\lambda}_l = x$, where the $\tilde{\lambda}_i$ are all distinct. Therefore, the number of permutations of $(\lambda_1, \dots, \lambda_k)$ is equal to $k!/(s_1! \cdots s_l!)$. Hence, for a fixed $\tilde{\lambda}_i$, $i \in B$, the number of $(\lambda_1, \dots, \lambda_k)$ belonging to $E(\vec{s})(x)$ does not exceed $k!/(s_1! \cdots s_l!)$. Therefore, the cardinality of $E(\vec{s})(x)$ does not exceed $|\Lambda|^{|B(\vec{s})|} k!/(s_1! \cdots s_l!)$. The lemma is proved.

We now return to the proof of the assertion and estimate the sum σ. Let b be a non-negative integer and let

$$\sigma_b = \sum_{x \in \mathbb{Z}_N} \Bigg(\sum_{\vec{s}\colon\ |B(\vec{s})| = b} |E(\vec{s})(x)| \Bigg)^2. \tag{80}$$

It follows from (77) that $|B(\vec{s})| \leqslant [k/s]$ for all $\vec{s}$. Combining this with the Cauchy–Bunyakovsky inequality, we obtain that $\sigma \leqslant \big([(k-1)/s] + 1\big)^2 \sum_{b=0}^{[k/s]} \sigma_b$. We now fix a b and estimate σ_b as follows. We have

$$\sigma_b \leqslant \Bigg(\sum_{x \in \mathbb{Z}_N} \sum_{\vec{s}\colon\ |B(\vec{s})| = b} |E(\vec{s})(x)| \Bigg) \Bigg(\max_{x \in \mathbb{Z}_N} \sum_{\vec{s}\colon\ |B(\vec{s})| = b} |E(\vec{s})(x)| \Bigg). \tag{81}$$

Let $P_k(\vec{s}) = k!/(s_1! \cdots s_l!)$. Then

$$\sum_{\vec{s}} P_k(\vec{s}) \leqslant \sum_{l=1}^{k} \sum_{\substack{s_1, \dots, s_l = 0 \\ s_1 + \dots + s_l = k}}^{k} \frac{k!}{s_1! \cdots s_l!} = \sum_{l=1}^{k} l^k \leqslant 2k^k. \tag{82}$$

Using Lemma 5, we obtain that $|E(\vec{s})(x)| \leqslant P_k(\vec{s}) |\Lambda|^{|B(\vec{s})|}$. Combining this with inequality (82), we obtain that

$$\max_{x \in \mathbb{Z}_N} \sum_{\vec{s}\colon\ |B(\vec{s})| = b} |E(\vec{s})(x)| \leqslant 2k^k |\Lambda|^b. \tag{83}$$

Consider the sum

$$\sum_{x \in \mathbb{Z}_N} \sum_{\vec{s}\colon\ |B(\vec{s})| = b} |E(\vec{s})(x)|. \tag{84}$$

It follows from (77) that this sum is bounded above by the number of $(\lambda_1,\dots,\lambda_k)\in\Lambda^k$ such that at most $k-sb$ of the numbers $\lambda_1,\dots,\lambda_k$ are distinct. Therefore,

$$\sum_{x\in\mathbb{Z}_N}\ \sum_{\vec{s}\colon\,|B(\vec{s})|=b}|E(\vec{s})(x)|\leqslant\binom{|\Lambda|}{k-sb}(k-sb)^k$$
$$\leqslant\frac{|\Lambda|^{k-sb}}{(k-sb)!}(k-sb)^k\leqslant e^kk^{sb}|\Lambda|^{k-sb}. \tag{85}$$

Combining this with (83), we obtain that

$$\sigma_b\leqslant 2e^kk^k|\Lambda|^b\left(\frac{k}{|\Lambda|}\right)^{sb}|\Lambda|^k. \tag{86}$$

Hence,

$$\sigma\leqslant 2\big([(k-1)/s]+1\big)^2e^kk^k|\Lambda|^k\sum_{b=0}^{[(k-1)/s]}\left(\frac{k^s}{|\Lambda|^{s-1}}\right)^b$$
$$=2\big([(k-1)/s]+1\big)^2e^kk^k|\Lambda|^k\sigma^*. \tag{87}$$

We estimate σ^* as follows. If $k^s\leqslant|\Lambda|^{s-1}$, then it is obvious that $\sigma^*\leqslant[(k-1)/s]+1$. If $k^s>|\Lambda|^{s-1}$, then $\sigma^*\leqslant\big([(k-1)/s]+1\big)(k/|\Lambda|)^k|\Lambda|^{k/s}|\Lambda|^{1-1/s}/k$. In any case we have $\sigma^*\leqslant\big([(k-1)/s]+1\big)\max\{1,(k/|\Lambda|)^k|\Lambda|^{k/s}|\Lambda|^{1-1/s}/k\}$. Therefore,

$$\sigma=T_k(\Lambda)\leqslant 2^{3k}k^k|\Lambda|^k\max\left\{1,\left(\frac{k}{|\Lambda|}\right)^k|\Lambda|^{k/s}\right\}. \tag{88}$$

The assertion is proved.

Proof of Theorem 8. Let $k=2\lceil\log(1/\delta)\rceil$, let $s=2$ and let $\Lambda=\{\lambda_1,\dots,\lambda_{|\Lambda|}\}$ be a maximal subset of $\mathcal{R}_\alpha\setminus\{0\}$ belonging to $\Lambda(k,s)$. If $\mathcal{R}_\alpha=\{0\}$, then the proof is obvious. If $\mathcal{R}_\alpha\setminus\{0\}$ is non-empty, then Λ is also non-empty. Let $\Lambda^*=\big(\bigcup_{j=1}^s j^{-1}\Lambda\big)\cup\{0\}$. Then $|\Lambda^*|\leqslant 4|\Lambda|$ and $0\in\Lambda^*$. We claim that for any $x\in\mathcal{R}_\alpha\setminus\{0\}$ there is a $j\in[s]$ such that

$$xj=\sum_{i=1}^{|\Lambda|}\lambda_is_i,\qquad s_i\in\mathbb{Z},\quad |s_i|\leqslant s,\quad \sum_{i=1}^{|\Lambda|}|s_i|\leqslant 2k. \tag{89}$$

Then since $j^{-1}\lambda_i\in\Lambda^*$ for all $i\in[|\Lambda|]$, $j\in[s]$, the desired assertion will follow from (89).

Thus, let x be an arbitrary element of $\mathcal{R}_\alpha\setminus\Lambda$, $x\neq 0$. Consider relations of the form $\sum_{i=1}^{|\Lambda|+1}\tilde{\lambda}_is_i=0$, where $\tilde{\lambda}_i\in\Lambda\bigsqcup\{x\}$ and $s_i\in\mathbb{Z}$, $|s_i|\leqslant s$, $\sum_{i=1}^{|\Lambda|+1}|s_i|\leqslant 2k$. If all these relations are trivial, that is, if for each of them we have $s_i=0$, $i\in[|\Lambda|+1]$, then we obtain a contradiction to the maximality of Λ. Hence, there is a non-trivial relation of the form (89) such that $j,s_1,\dots,s_{|\Lambda|}$ are not all equal to zero. We have $j\in[-s,\dots,s]$. If $j=0$, then we obtain a contradiction to the fact that Λ belongs to $\Lambda(k,s)$. Therefore, we can assume that $j\in[s]$. Since $2k\leqslant 8\log(1/\delta)$, we obtain that for any $x\in\mathcal{R}_\alpha$ there is a $\{\lambda_1^*,\dots,\lambda_M^*\}\subset\Lambda^*$, $M\leqslant 8\log(1/\delta)$, such that (71) holds.

We claim that $|\Lambda^*| \leqslant \max\bigl(2^{12}(\delta/\alpha)^2 \log(1/\delta), 2^6 \log^2(1/\delta)\bigr)$.

If $|\Lambda| \leqslant k^2$, then $|\Lambda| \leqslant 2^4 \log^2(1/\delta)$, whence $|\Lambda^*| \leqslant 2^6 \log^2(1/\delta)$. If $|\Lambda| > k^2$, then Assertion 1 implies that $T_k(\Lambda) \leqslant 2^{3k} k^k |\Lambda|^k$. On the other hand, using Theorem 5 we obtain that $T_k(\Lambda) \geqslant \delta\alpha^{2k}|\Lambda|^{2k}/(2^{4k}\delta^{2k})$. Therefore, $|\Lambda| \leqslant 2^{10}(\delta/\alpha)^2 \log(1/\delta)$, whence $|\Lambda^*| \leqslant 2^{12}(\delta/\alpha)^2 \log(1/\delta)$.

In any case we have $|\Lambda^*| \leqslant \max\bigl(2^{12}(\delta/\alpha)^2 \log(1/\delta), 2^6 \log^2(1/\delta)\bigr)$.

We now prove the existence of $\widetilde{\Lambda}$. Let $s = [\log\log(1/\delta)]$ and let Λ_1 be a maximal subset of $\mathcal{R}_\alpha \setminus \{0\}$ belonging to $\Lambda(k, s)$, $k = 2\lceil \log(1/\delta) \rceil$. Let $\widetilde{\Lambda} = \bigcup_{j=1}^{s} j^{-1}\Lambda_1$. Then $|\widetilde{\Lambda}| \leqslant s|\Lambda_1|$. Arguments similar to those used above enable us to show that for any residue $r \in \mathcal{R}_\alpha$ there is a set $\{\tilde{\lambda}_1, \dots, \tilde{\lambda}_M\} \subset \widetilde{\Lambda}$, $M \leqslant 8\log(1/\delta)$, such that (73) holds.

We prove (72) as follows. If $|\Lambda_1| \leqslant k^{s/(s-1)}$, then $|\Lambda_1| \leqslant 2^{10}\log(1/\delta)$ and $|\widetilde{\Lambda}| \leqslant s|\Lambda_1| \leqslant 2^{12}\log(1/\delta)\log\log(1/\delta)$. We see that in this case (72) is proved. Now let $|\Lambda_1| > k^{s/(s-1)}$. Using Assertion 1, we obtain that $T_k(\Lambda_1) \leqslant 2^{3k}k^k|\Lambda_1|^k$. On the other hand, Theorem 5 implies that $T_k(\Lambda_1) \geqslant \delta\alpha^{2k}|\Lambda_1|^{2k}/(2^{4k}\delta^{2k})$. Therefore, $|\Lambda_1| \leqslant 2^{10}(\delta/\alpha)^2\log(1/\delta)$, whence $|\widetilde{\Lambda}| \leqslant 2^{12}(\delta/\alpha)^2 \log(1/\delta)\log\log(1/\delta)$. The theorem is proved.

We shall now apply Theorems 5 and 8 to problems in the combinatorial theory of numbers.

Let K be an arbitrary subset of $\mathbb{Z}_N$ and $\varepsilon \in (0,1)$ any real number. Then the corresponding *Bohr set* is defined as

$$B(K,\varepsilon) = \left\{ x \in \mathbb{Z}_N : \left\| \frac{rx}{N} \right\| < \varepsilon \quad \forall\, r \in K \right\},$$

where $\|\cdot\|$ denotes the integer part of a real number. Information on the properties of Bohr sets can be found in [26], where, in particular, it is proved that

$$|B(K,\varepsilon)| \geqslant \frac{1}{2}\varepsilon^{|K|}N. \tag{90}$$

In her proof of the quantitative version of Freiman's theorem (see [2] and [9]), Chang used the following proposition.

Proposition 2. *Let N be a positive integer, $\delta \in (0,1)$ a real number and A an arbitrary subset of $\mathbb{Z}_N$ with $|A| = \delta N$. Then $2A - 2A$ contains a Bohr set $B(K,\varepsilon)$ with $|K| \leqslant 8\delta^{-1}\log(1/\delta)$ and $\varepsilon = \delta/\bigl(2^8\log(1/\delta)\bigr)$.*

We claim that Proposition 2 can be strengthened as follows.

Proposition 3. *Let N be a positive integer, $(N,2) = 1$, let $0 < \delta \leqslant 2^{-256}$ be a real number and let A be an arbitrary subset of $\mathbb{Z}_N$ with $|A| = \delta N$. Then $2A - 2A$ contains a Bohr set $B(K,\varepsilon)$ with $|K| \leqslant 2^{15}\delta^{-1}\log(1/\delta)$ and $\varepsilon = 1/\bigl(2^8\log(1/\delta)\bigr)$.*

Using formula (90), we obtain that the cardinality of $B(K,\varepsilon)$ in Proposition 2 is greater than or equal to $(1/2)\cdot 2^{-8\delta^{-1}(\log(1/\delta))^2}N$. The cardinality of the Bohr set in Proposition 3 is greater than or equal to $(1/2)\cdot 2^{-2^{20}\delta^{-1}\log(1/\delta)\log\log(1/\delta)}N$.

To prove Proposition 3 we need the following definition.

Definition 3. Let $f, g\colon \mathbb{Z}_N \to \mathbb{C}$ be arbitrary functions. The *convolution* of f and g is defined to be the function

$$(f * g)(x) = \sum_{y \in \mathbb{Z}_N} f(y)\overline{g(y-x)}. \tag{91}$$

It is obvious that

$$\widehat{(f * g)}(r) = \hat{f}(r)\overline{\hat{g}(r)}. \tag{92}$$

Proof of Proposition 3. Let $\alpha = \delta^{3/2}/(2\sqrt{2})$. Applying Corollary 1 to $\mathcal{R}_\alpha(A)$, we obtain a set $\Lambda^* \subseteq \mathbb{Z}_N$, $|\Lambda^*| \leqslant 2^{15}\delta^{-1}\log(1/\delta)$, such that for any residue $r \in \mathcal{R}_\alpha$ there is a set $\lambda_1^*, \dots, \lambda_M^*$ of at most $8\log(1/\delta)$ elements of Λ^* such that (71) holds. Let $\mathcal{R}_\alpha^* = \mathcal{R}_\alpha \setminus \{0\}$. Consider the Bohr set $B_1 = B(\mathcal{R}_\alpha^*, 1/20)$. For all $x \in B_1$ and all $r \in \mathcal{R}_\alpha^*$ we have

$$|1 - e(rx)| = 2\left|\sin\left(\frac{\pi r x}{N}\right)\right| \leqslant \frac{2\pi}{20} < \frac{1}{2}. \tag{93}$$

The expression $(A * A * A * A)(x)$ is obviously equal to the number of quadruples $(a_1, a_2, a_3, a_4) \in A^4$ such that $a_1 + a_2 - a_3 - a_4 = x$. Hence, $(A * A * A * A)(x) > 0$ if and only if $x \in 2A - 2A$. Using formulae (11) and (92), we obtain that x belongs to $2A - 2A$ if and only if $\sum_r |\widehat{A}(r)|^4 e(rx) > 0$. Let $x \in B_1$. Then, using Parseval's equality (2)), we have

$$\begin{aligned}
\sum_r |\widehat{A}(r)|^4 e(rx) &= \sum_r |\widehat{A}(r)|^4 - \sum_r |\widehat{A}(r)|^4 \bigl(1 - e(rx)\bigr) \\
&> \frac{1}{2}\sum_r |\widehat{A}(r)|^4 - 2\sum_{r \notin R, r \neq 0} |\widehat{A}(r)|^4 \geqslant \frac{1}{2}\delta^4 N^4 - 2\max_{r \notin R, r\neq 0} |\widehat{A}(r)|^2 \sum_r |\widehat{A}(r)|^2 \\
&\geqslant \frac{1}{2}\delta^4 N^4 - 2 \cdot \frac{\delta^3 N^2}{8}\delta N^2 = \frac{\delta^4 N^4}{4} > 0.
\end{aligned} \tag{94}$$

It follows from (94) that the Bohr set B_1 is contained in $2A - 2A$. Consider another Bohr set $B_2 = B\bigl(\Lambda^*, 1/\bigl(2^8\log(1/\delta)\bigr)$. We claim that $B_2 \subseteq B_1$. Since for any residue $r \in \mathcal{R}_\alpha^*$ there is a set $\lambda_1^*, \dots, \lambda_M^*$ of at most $8\log(1/\delta)$ elements of Λ^* such that (71) holds, the inequality

$$\left\|\frac{rx}{N}\right\| \leqslant \sum_{i=1}^{M}\left\|\frac{\lambda_i^* x}{N}\right\| \leqslant 8\log\left(\frac{1}{\delta}\right)\frac{1}{2^8\log(1/\delta)} < \frac{1}{20} \tag{95}$$

holds for all $x \in B_2$. Hence, every $x \in B_2$ belongs to B_1, and we have obtained a Bohr set $B_2 \subseteq 2A - 2A$ with the desired properties. The proposition is proved.

Bibliography

[1] W. T. Gowers, "Rough structure and classification", *GAFA* 2000 (Tel Aviv 1999), Geom. Funct. Anal., Special Volume, Part I, Birkhäuser, Basel 2000, pp. 79–117.

[2] Mei-Chu Chang, "A polynomial bound in Freiman's theorem", *Duke Math. J.* **113**:3 (2002), 399–419.

[3] I. Z. Ruzsa, "Generalized arithmetical progressions and sumsets", *Acta Math. Hungar.* **65**:4 (1994), 379–388.

[4] Yu. Bilu, "Structure of sets with small sumset", *Structure theory of set addition* (J.-M. Deshouillers et al., eds.), Astérisque, vol. 258, Soc. Math. France, Paris 1999, pp. 77–108.

[5] G. A. Freiman, *Foundations of a structural theory of set addition*, Kazansk. Gos. Ped. Institute, Kazan' 1966; English transl., Transl. Math. Monogr., vol. 37, Amer. Math. Soc., Providence, RI 1973.

[6] B. Green, "Arithmetic progressions in sumsets", *Geom. Funct. Anal.* **12**:3 (2002), 584–597.

[7] J. Bourgain, "On arithmetic progressions in sums of sets of integers", *A tribute to Paul Erdős*, Cambridge Univ. Press, Cambridge 1990, pp. 105–109.

[8] G. A. Freiman, H. Halberstam, and I. Z. Ruzsa, "Integer sum sets containing long arithmetic progressions", *J. London Math. Soc.* (2) **46**:2 (1992), 193–201.

[9] B. Green, *Structure theory of set addition*, ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis, Edinburgh 2002; `http://www.dpmms.cam.ac.uk/~bjg23/papers/icmsnotes.pdf`.

[10] B. Green, "Some constructions in the inverse spectral theory of cyclic groups", *Combin. Probab. Comput.* **12**:2 (2003), 127–138.

[11] A. A. Yudin, "On the measure of large values of the modulus of a trigonometric sum", *Number-theoretic studies in the Markov spectrum and the structure theory of set addition* (G. A. Freiman, A. M. Rubinov, E. V. Novoselov, eds.), Kalininsk. Gos. Univ., Kalinin 1973, pp. 163–171. (Russian)

[12] A. Besser, "Sets of integers with large trigonometric sums", *Structure theory of set addition* (J.-M. Deshouillers et al., eds.), Astérisque, vol. 258, Soc. Math. France, Paris 1999, pp. 35–76.

[13] V. F. Lev, "Linear equations over $\mathbb{F}_p$ and moments of exponential sums", *Duke Math. J.* **107**:2 (2001), 239–263.

[14] S. V. Konyagin and V. F. Lev, "On the distribution of exponential sums", *Integers* **0** (2000), paper A1 (electronic).

[15] K. de Leeuw, Y. Katznelson, and J.-P. Kahane, "Sur les coefficients de Fourier des fonctions continues", *C. R. Acad. Sci. Paris Sér. A* **285**:16 (1977), 1001–1003.

[16] F. L. Nazarov, "The Bang solution of the coefficient problem", *Algebra i Analiz* **9**:2 (1997), 272–287; English transl., *St. Petersburg Math. J.* **9**:2 (1998), 407–419.

[17] K. Ball, "Convex geometry and functional analysis", *Handbook of the geometry of Banach spaces*, vol. 1, Elsevier, Amsterdam 2001, pp. 161–194.

[18] W. T. Gowers, "A new proof of Szemerédi's theorem", *Geom. Funct. Anal.* **11**:3 (2001), 465–588.

[19] W. Rudin, *Fourier analysis on groups*, Wiley, New York 1990, reprint of the 1962 original.

[20] W. Rudin, "Trigonometric series with gaps", *J. Math. Mech.* **9** (1960), 203–227.

[21] B. Green, "Spectral structure of sets of integers", *Fourier analysis and convexity*, Appl. Numer. Harmon. Anal., Birkhäuser, Boston, MA 2004, pp. 83–96.

[22] I. M. Vinogradov, *The method of trigonometric sums in number theory*, Nauka, Moscow 1971. (Russian)

[23] Yu. V. Linnik, "On Weyl's sums", *Mat. Sb.* **12 (54)**:1 (1943), 28–39. (English)

[24] Yu. V. Nesterenko, "On I. M. Vinogradov's mean value theorem", *Trudy Moskov. Mat. Obshch.* **48** (1985), 97–105; English transl., *Trans. Moscow Math. Soc.*, 1986, 105–113.

[25] B. Bajnok and I. Ruzsa, "The independence number of a subset of an Abelian group", *Integers* **3** (2003), paper A02 (electronic).

[26] J. Bourgain, "On triples in arithmetic progression", *Geom. Funct. Anal.* **9**:5 (1999), 968–984.

I. D. Shkredov
Department of Mechanics and Mathematics,
Moscow State University
E-mail: `ishkredov@rambler.ru`

Received 12/JUL/06
Translated by V. M. MILLIONSHCHIKOV