ISSN 1064–5624, Doklady Mathematics, 2006, Vol. 74, No. 3, pp. 860–864. © Pleiades Publishing, Inc., 2006.
Original Russian Text © I.D. Shkredov, 2006, published in Doklady Akademii Nauk, 2006, Vol. 411, No. 4, pp. 455–459.

MATHEMATICS

On Sets of Large Exponential Sums

I. D. Shkredov

Presented by Academician V.V. Kozlov April 24, 2006

Received May 16, 2006

DOI: 10.1134/S1064562406060196

1. INTRODUCTION

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

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

where $e(x) = e^{2\pi ix/N}$. The Fourier coefficients of f satisfy Parseval's identity

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

Let δ and α be real numbers such that $0 < \alpha \le \delta \le 1$, and let A be a subset of $\mathbb{Z}_N$ of cardinality δN. The characteristic function of this set is denoted by the same letter. Consider the set $\mathcal{R}_\alpha$ of large exponential sums of A defined as

$$\mathcal{R}_\alpha = \mathcal{R}_\alpha(A) = \{r \in \mathbb{Z}_N\colon |\hat{A}(r)| \ge \alpha N\}. \qquad (3)$$

For many problems in combinatorial number theory, it is important to know the structure of $\mathcal{R}_\alpha$. In other words, what are the properties of $\mathcal{R}_\alpha$? The answer to this question is very important, which will be shown below. Note that this question was asked by the Fields winner W.T. Gowers in [1].

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

Theorem 1 (Chang). *Let δ and α be real numbers such that $0 < \alpha \le \delta \le 1$, A be an arbitrary subset of $\mathbb{Z}_N$ of cardinality δN, and the set $\mathcal{R}_\alpha$ be defined by* (3).

Then there exists a set $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_{|\Lambda|}\} \subseteq \mathbb{Z}_N$ with $|\Lambda| \le 2\left(\frac{\delta}{\alpha}\right)^2 \log_2 \frac{1}{\delta}$ such that any element r of $\mathcal{R}_\alpha$ can be represented as

$$r = \sum_{i=1}^{|\Lambda|} \varepsilon_i \lambda_i \pmod N, \qquad (4)$$

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

Developing the approach taken in [3] (see also [4]), Chang used her result to prove the famous theorem of Freiman on sets with a small sum [5]. Another application of Theorem 1 was made by Green in [6] (see also [8, 9]). In [7] Green showed that Chang's theorem is sharp in a sense. Let $E = \{e_1, e_2, \ldots, e_{|E|}\} \subseteq \mathbb{Z}_N$ be an arbitrary set. Denote by $\mathrm{Span}(E)$ the set of all sums of the form $\sum_{i=1}^{|E|} \varepsilon_i e_i$, where $\varepsilon_i \in \{-1, 0, 1\}$.

Theorem 2 (Green). *Let δ and α be real numbers such that $\delta \le \frac{1}{8}$ and $0 < \alpha \le \frac{\delta}{32}$. Let $\left(\frac{\delta}{\alpha}\right)^2 \log_2\left(\frac{1}{\delta}\right) \le \frac{\log_2 N}{\log_2 \log_2 N}$.*

Then there exists a set $A \subset \mathbb{Z}_N$ with $|A| = [\delta N]$ such that the set $\mathcal{R}_\alpha$ defined by (3) *is not contained in* $\mathrm{Span}(\Lambda)$ *for any set Λ of cardinality $2^{-12}\left(\frac{\delta}{\alpha}\right)^2 \log_2\left(\frac{1}{\delta}\right)$.*

The structure of $\mathcal{R}_\alpha$ with α close to δ was studied in [10–12].

We see that the results on the structure of $\mathcal{R}_\alpha$ are important for combinatorial number theory. In this paper, we prove the following result.

Theorem 3. *Suppose that δ and α are real numbers such that $0 < \alpha \le \delta$, A is an arbitrary subset of $\mathbb{Z}_N$ of cardinality δN, $k \ge 2$ is even, and the set $\mathcal{R}_\alpha$ is defined*

Department of Number Theory, Faculty of Mechanics and Mathematics, Moscow State University, Leninskie gory, Moscow, 119992 Russia
e-mail: ishkredov@rambler.ru

by (3). *Let* $B \subseteq \mathcal{R}_\alpha\backslash\{0\}$ *be an arbitrary set. Then the number*

$$T_k(B) := \left|\{(r_1, r_2, \ldots, r_k, r_1', r_2', \ldots, r_k') \in B^{2k}: r_1 + r_2 + \ldots + r_k = r_1' + r_2' + \ldots + r_k'\}\right| \quad (5)$$

is at least $\dfrac{\delta\alpha^{2k}|B|^{2k}}{(2^{4k}\delta^{2k})}$.

Theorem 3 is proved in Section 2, where the case $k = 2$ is first treated in detail and, then, the proof of Theorem 3 is sketched in the general case. In Section 3, we apply the main result to several problems in combinatorial number theory and derive a strengthening of Theorem 1 (see Theorem 4). Additionally, we apply Theorem 3 to prove Freiman's theorem.

2. PROOF OF THE MAIN THEOREM

First, we explain the basic idea behind the proof of Theorem 3. Let N be a positive integer and $\hat{A}(r)$ be the Fourier coefficients of A. As was noted above, the Fourier coefficients of a set satisfy Parseval's identity. Do there exist any other nontrivial relations between the Fourier coefficients $\hat{A}(r)$ in addition to (2)? It is easy to see that this question is answered in the affirmative.

Let $f, g: \mathbb{Z}_N \to \mathbb{C}$ be arbitrary complex functions. By using the inversion formula

$$f(x) = \frac{1}{N}\sum_{r \in \mathbb{Z}_N} \hat{f}(r)e(rx), \quad (6)$$

it is easy to obtain the identity

$$\frac{1}{N}\sum_r \hat{f}(r)\overline{\hat{g}(r-u)} = \sum_x f(x)\overline{g(x)}e(-xu). \quad (7)$$

Now, if f is the characteristic function of a set $A \subset \mathbb{Z}_N$, then formula (7) can be rewritten as

$$\hat{f}(u) = \frac{1}{N}\sum_r \hat{f}(r)\overline{\hat{f}(r-u)}. \quad (8)$$

Clearly, (8) contains all the relations between the Fourier coefficients of A. For example, Parseval's identity (2) is derived if we set $u = 0$ in (8).

Let us prove Theorem 3. For a better demonstration of the main idea behind the proof, we prove Theorem 3 for the case $k = 2$ separately. Specifically, let $k = 2$ and B be an arbitrary subset of $\mathcal{R}_\alpha\backslash\{0\}$. We need the following result.

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

$$\mathcal{R}_{\alpha'}' = \{r \in \mathbb{Z}_N: \alpha' N \le |\hat{A}(r)| < 2\alpha' N\} \quad (9)$$

and B' *is an arbitrary subset of* $\mathcal{R}_{\alpha'}'\backslash\{0\}$. *Then* $T_2(B') \ge (\alpha')^4|B'|^4/(16\delta^3)$.

Proof. Let $f_{B'}(x) = \dfrac{1}{N}\sum_{r \in B'} \hat{A}(r)e(rx)$. It is easy to see that $\hat{f}_{B'}(r) = \hat{A}(r)B'(r)$. Consider the sum $\sigma = \sum_s \left|\sum_r \hat{f}_{B'}(r)\overline{\hat{A}(r-s)}\right|^2$. Applying formula (7) and Parseval's identity, we find

$$\sigma = N^2\sum_s \left|\sum_x f_{B'}(x)\overline{A(x)}e(-xs)\right|^2 = N^3\sum_x |f_{B'}(x)|^2 A(x)^2. \quad (10)$$

To estimate the sum $\sum_x |f_{B'}(x)|^2A(x)^2$ from below, we use Parseval's identity and the definition of $\mathcal{R}_{\alpha'}'$:

$$\left(\sum_x f_{B'}(x)A(x)\right)^2 = \left(\frac{1}{N}\sum_r \hat{f}_{B'}(r)\overline{\hat{A}(r)}\right)^2 = \left(\frac{1}{N}\sum_r |\hat{f}_{B'}(r)|^2\right)^2 \quad (11)$$

$$\ge (N\alpha'^2|B'|)^2 = \alpha'^4|B'|^2N^2. \quad (12)$$

On the other hand,

$$\left(\sum_x f_{B'}(x)A(x)\right)^2 \le \left(\sum_x |f_{B'}(x)|^2A(x)^2\right)\left(\sum_x A(x)^2\right) = \delta N\left(\sum_x |f_{B'}(x)|^2A(x)^2\right). \quad (13)$$

Applying inequalities (12) and (13), we find that $\sigma^2 \ge \dfrac{\alpha'^8}{\delta^2}|B'|^4N^8$. Let us estimate σ^2 from above. We have

$$\sigma = \sum_s\sum_{r,r'} \hat{f}_{B'}(r)\overline{\hat{f}_{B'}(r')}\overline{\hat{A}(r-s)}\hat{A}(r'-s) = \sum_u \left(\sum_r \hat{f}_{B'}(r)\overline{\hat{f}_{B'}(r-u)}\right)\overline{\left(\sum_r \hat{A}(r)\overline{\hat{A}(r-u)}\right)}, \quad (14)$$

which yields

$$\sigma^2 \le \sum_u \left|\sum_r \hat{f}_{B'}(r)\overline{\hat{f}_{B'}(r-u)}\right|^2 \sum_u \left|\sum_r \hat{A}(r)\overline{\hat{A}(r-u)}\right|^2 = \sigma_1\sigma_2. \quad (15)$$

Applying formula (8) and Parseval's identity gives

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

Since $\hat{f}_{B'}(r) = \hat{A}(r)B'(r)$ and $B' \subseteq \mathcal{R}'_{\alpha'}\setminus\{0\}$, we have $|\hat{f}_{B'}(r)| \le 2\alpha' B'(r)N$, which implies $\sigma_1 \le 16(\alpha')^4 T_2(B')N^4$. Applying the estimates for σ_1 and σ_2 and the lower bound for σ^2, we obtain $T_2(B') \ge \dfrac{(\alpha')^4|B'|^4}{16\delta^3}$, which completes the proof of Lemma 1.

Let

$$B_i = \{r \in B: \alpha\cdot 2^{i-1}N \le |\hat{A}(r)| < \alpha\cdot 2^i N\}, \quad i \ge 1. \tag{16}$$

It is clear that $B = \bigsqcup_{i\ge 1} B_i$. Applying Lemma 1 to each B_i gives $T_2(B_i) \ge \dfrac{(\alpha\cdot 2^{i-1})^4|B_i|^4}{16\delta^3}$, $i \ge 1$. Therefore,

$$T_2(B) \ge \sum_i T_2(B_i) \ge \frac{\alpha^4}{\delta^3\cdot 2^8}\sum_i 2^{4i}|B_i|^4. \tag{17}$$

We have $|B| = \sum_i |B_i|$. Using the Cauchy–Schwarz inequality, we obtain

$$|B|^4 = \left(\sum_i |B_i|\cdot 2^i\cdot 2^{-i}\right)^4 \le \left(\sum_i 2^{4i}|B_i|^4\right)\left(\sum_i 2^{-4i/3}\right)^3 \le \sum_i 2^{4i}|B_i|^4. \tag{18}$$

Substituting (18) into (17) yields $T_2(B) \ge \dfrac{\alpha^4}{\delta^3\cdot 2^8}|B|^4$. Thus, we have proved Theorem 3 for $k = 2$. In the general situation where $k \ge 2$ is even, we prove the following analogue of Lemma 1.

Lemma 2. *Suppose that* δ *and* α' *are real numbers such that* $0 < \alpha' \le \delta$, *A is an arbitrary subset of* $\mathbb{Z}_N$ *of cardinality* δN, *and* $k \ge 2$ *is even. Let* $\mathcal{R}'_{\alpha'}$ *be defined by* (9) *and B' be an arbitrary subset of* $\mathcal{R}'_{\alpha'}\setminus\{0\}$.

Then $T_k(B') \ge \dfrac{\delta(\alpha')^{2k}|B'|^{2k}}{(2\delta)^{2k}}$.

The required estimate is derived by applying Lemma 2 and following a line of reasoning similar of that used in (16)–(18). The proof of Theorem 3 is completed.

3. APPLICATIONS TO PROBLEMS IN COMBINATORIAL NUMBER THEORY

In this section, we prove a strengthening of Chang's theorem. Note that the proof technique shares many points with that used in [13, 14].

Theorem 4. *Let N be a positive integer,* $(N, 6) = 1$, δ *and* α *be real numbers such that* $0 < \alpha \le \delta \le \dfrac{1}{16}$, *A be an arbitrary subset of* $\mathbb{Z}_N$ *of cardinality* δN, *and the set* $\mathcal{R}_\alpha$ *be defined by* (3).

Then there exists a set $\Lambda^* \subseteq \mathbb{Z}_N$ *with* $|\Lambda|^* \le \max\left(2^{30}\left(\dfrac{\delta}{\alpha}\right)^2\log_2\left(\dfrac{1}{\delta}\right),\ 4\exp\left(4\left(\log_2\log_2\left(\dfrac{1}{\delta}\right)\right)^2\right)\right)$ *such that, for any residue* $r \in \mathcal{R}_\alpha$, *there is a tuple* $\lambda_1^*, \lambda_2^*, \ldots, \lambda_M^*$ *consisting of at most* $8\log_2\left(\dfrac{1}{\delta}\right)$ *elements of* Λ^* *such that*

$$r = \sum_{i=1}^{M}\varepsilon_i\lambda_i^* \pmod N, \tag{19}$$

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

To prove Theorem 4, we need several auxiliary propositions and definitions.

Definition 1. Let k and s be positive integers. Consider the family $\Lambda(k, s)$ of subsets of $\mathbb{Z}_N$ that possess the following property. If a set $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_{|\Lambda|}\}$ belongs to $\Lambda(k, s)$, then the equality

$$\sum_{i=1}^{|\Lambda|}\lambda_i s_i = 0 \pmod N, \quad \lambda_i \in \Lambda, \quad s_i \in \mathbb{Z}, \quad |s_i| \le s, \quad \sum_{i=1}^{|\Lambda|}|s_i| \le 2k \tag{20}$$

implies that all s_i are equal to zero.

The definition of $\Lambda(k, 1)$ can be found in [15]. The following upper bound on T_k holds for an arbitrary set in $\Lambda(k, 3)$.

Statement 1. *Let k be a positive integer,* Λ *be an arbitrary subset of the family* $\Lambda(k, 3)$, *and* $\log_2|\Lambda| \ge \log_2^2 k$.

Then $T_k(\Lambda) \le 2^{20k}k^k|\Lambda|^k$.

Proof of Theorem 4. Let $k = 2\lceil \log_2\left(\frac{1}{\delta}\right)\rceil$. Let $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_{|\Lambda|}\}$ be a maximal subset of $\mathcal{R}_\alpha\backslash\{0\}$ that belongs to $\Lambda(k, 3)$. If $\mathcal{R}_\alpha = \{0\}$, there is nothing to prove. If $\mathcal{R}_\alpha\backslash\{0\}$ is not empty, then Λ is not empty as well. Let $\Lambda^* = \left(\bigcup_{j=1}^{s} j^{-1}\Lambda\right) \cup \{0\}$. Then $|\Lambda^*| \le 4|\Lambda|$ and $0 \in \Lambda^*$. We prove that, for any $x \in \mathcal{R}_\alpha\backslash\{0\}$, there exists $j \in \{1, 2, \ldots, s\}$ such that

$$xj = \sum_{i=1}^{|\Lambda|}\lambda_i s_i, \text{ где } s_i \in \mathbb{Z}, \ |s_i| \le s, \ \sum_{i=1}^{|\Lambda|}|s_i| \le 2k. \quad (21)$$

Since $i \in \{1, 2, \ldots, |\Lambda|\}$ for any $j \in \{1, 2, \ldots, s\}$ and any $j^{-1}\lambda_i \in \Lambda^*$, the required assertion follows from equality (21). Thus, let x be an arbitrary element of $\mathcal{R}_\alpha\backslash\Lambda$ such that $x \ne 0$. Consider all relations of the form $\sum_{i=1}^{|\Lambda|+1}\tilde{\lambda}_i s_i = 0$, where $\tilde{\lambda}_i \in \Lambda\bigsqcup\{x\}$ and $s_i \in \mathbb{Z}$ with $|s_i| \le s$ and $\sum_{i=1}^{|\Lambda|+1}|s_i| \le 2k$. If all these relations are trivial, i.e., if $s_i = 0$, $i \in \{1, 2, \ldots, |\Lambda| + 1\}$ for any such relation, then we obtain a contradiction with the maximality of Λ. Therefore, there exists a nontrivial relation of form (21) such that $s_1, s_2, \ldots, s_{|\Lambda|}, j$ are not all zero. Here, $j \in \{-s, -s + 1, \ldots, s\}$. If $j = 0$, we obtain a contradiction with the fact that Λ belongs to $\Lambda(k, 3)$. Consequently, we can assume that $j \in \{1, 2, \ldots, s\}$. Since $2k \le 8\log_2\left(\frac{1}{\delta}\right)$, we find that, for any element $x \in \mathcal{R}_\alpha$, there exist a tuple $\lambda_1^*, \lambda_2^*, \ldots, \lambda_M^*$ consisting of at most $8\log_2\left(\frac{1}{\delta}\right)$ elements of Λ^* such that equality (19) holds.

It remains to prove the estimate for the cardinality of Λ^*. If $\log_2|\Lambda| \le (\log_2 k)^2$, then $|\Lambda| \le \exp\left(4\left(\log_2\log_2\left(\frac{1}{\delta}\right)\right)^2\right)$. Consequently, $|\Lambda^*| \le 4\exp\left(4\left(\log_2\log_2\left(\frac{1}{\delta}\right)\right)^2\right)$.

If $\log_2|\Lambda| \ge (\log_2 k)^2$, then Statement 1 gives $T_k(\Lambda) \le 2^{20k}k^k|\Lambda|^k$. On the other hand, applying Theorem 3, we obtain $T_k \ge \frac{\delta\alpha^{2k}|\Lambda|^{2k}}{(2^{4k}\delta^{2k})}$, which yields $|\Lambda| \le 2^{27}\left(\frac{\delta}{\alpha}\right)^2\log_2\left(\frac{1}{\delta}\right)$ and, consequently, $|\Lambda^*| \le 2^{30}\left(\frac{\delta}{\alpha}\right)^2\log_2\left(\frac{1}{\delta}\right)$.

In any case, $|\Lambda^*| \le \max(2^{30}(\delta/\alpha)^2\log_2(1/\delta), 4\exp\left(4\left(\log_2\log_2\left(\frac{1}{\delta}\right)\right)^2\right)$. This completes the proof of the theorem.

Suppose that K is an arbitrary subset of $\mathbb{Z}_N$ and $\varepsilon \in (0, 1)$ is any real number. The Bohr set $B(K, \varepsilon)$ is defined as

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

The following assertion was used in [2] to prove Freiman's theorem.

Proposition 1. *Let N be a positive integer, $\delta \in (0, 1)$ be a real number, and A be an arbitrary subset of $\mathbb{Z}_N$ with $|A| = \delta N$.*

Then $2A - 2A$ contains a Bohr set $B(K, \varepsilon)$, where $|K| \le 8\delta^{-1}\log_2(1/\delta)$ and $\varepsilon = \frac{\delta}{(2^8\log_2(1/\delta))}$.

Applying Theorem 4 and using the approach of [2], we prove a slight strengthening of Proposition 1.

Proposition 2. *Let N be a positive integer, $(N, 6) = 1$, $0 < \delta \le 2^{-128}$ be a real number, and A be an arbitrary subset of $\mathbb{Z}_N$ with $|A| = \delta N$.*

Then $2A - 2A$ contains a Bohr set $B(K, \varepsilon)$, where $|K| \le 2^{33}\frac{1}{\delta}\log_2(1/\delta)$ and $\varepsilon = \frac{1}{(2^8\log_2(1/\delta))}$.

ACKNOWLEDGMENTS

The author is deeply grateful to Professor S.V. Konyagin for his idea that made it possible to strengthen the main result and to Professor N.G. Moshchevitin for his constant interest in this study.

This work was supported by the Russian Foundation for Basic Research (project no. 06-01-00383), a grant from the President of the Russian Federation (1726.2006.1), and INTAS (project no. 03-51-5-70).

REFERENCES

1. W. T. Gowers, Geom. Funct. Anal. Special Volume, Part 1, 79–117 (1999).

2. M.-C. Chang, Duke Math. J. **113**, 399–419 (2002).
3. I. Ruzsa, Acta Math. Hung. **65**, 379–388 (1994).
4. Y. Bilu, Astérisque **258**, 77–108 (1999).
5. G. A. Freiman, *Foundations of a Structural Theory of Set Addition* (Kazan. Gos. Ped. Inst., Kazan, 1966; Am. Math. Soc., Providence, R.I., 1973).
6. B. Green, Geom. Funct. Anal. **12**, 584–597 (2002).
7. B. Green, Combin. Probab. Comp. **12** (2), 127–138 (2003).
8. J. Bourgain, *A Tribute of Paul Erdös* (Cambridge Univ. Press, Cambridge, 1990), pp. 105–109.
9. G. A. Freiman, H. Halberstam, and I. Ruzsa, J. London Math. Soc. **46** (2), 193–201 (1992).
10. A. A. Yudin, in *Number Theory* (Kalinin. Gos. Univ., Moscow, 1973), pp. 163–174 [in Russian].
11. A. Besser, Astérisque **258**, 35–76 (1999).
12. V. F. Lev, Duke Math. J. **107**, 239–263 (2001).
13. Yu. V. Linnik, Mat. Sb. **12** (1), 28–39 (1943).
14. Yu. V. Nesterenko, Tr. Mosk. Mat. O–va **48**, 97–105 (1985).
15. B. Bajnok and I. Ruzsa, Integers: Electr. J. Comb. Number Theory **3** (A02) (2003).