О множествах больших тригонометрических сумм *

Шкредов И.Д.

Известия Академии наук, 72, N 1, 2008, 1–22.

Аннотация.

Пусть A — подмножество $\mathbb{Z}/N\mathbb{Z}$ и пусть R — множество больших коэффициентов Фурье множества A. Свойства множества R изучались в работах М.– Ч. Чанг и Б. Грина. В настоящей статье мы доказываем существование нетривиальных решений у уравнения $r_1 + r_2 = r_3 + r_4$, где $r_1, r_2, r_3, r_4 \in R$. Это утверждение говорит о том, что множество R имеет сильные аддитивные свойства. Также мы обсуждаем обобщения и приложения полученных результатов.

1. Введение.

Пусть N — натуральное число. Обозначим через $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ множество вычетов по модулю N. Пусть $f : \mathbb{Z}_N \to \mathbb{C}$ — произвольная функция. Преобразование Фурье функции f задается формулой

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

где $e(x) = e^{-2\pi i x/N}$. Для коэффициентов Фурье функции f справедливо равенство Парсеваля

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

Пусть δ, α — действительные числа, $0 < \alpha \le \delta \le 1$ и пусть A — некоторое подмножество $\mathbb{Z}_N$ мощности δN. Будем обозначать той же буквой A характеристическую функцию этого множества. Рассмотрим множество $\mathcal{R}_\alpha$ больших тригонометрических сумм A

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

Для многих задач комбинаторной теории чисел важно знать структуру множества $\mathcal{R}_\alpha$. Иными словами, какими свойствами обладает множество $\mathcal{R}_\alpha$? Ответ на этот вопрос очень важен, в чем мы убедимся ниже, а сейчас отметим лишь то, что данный вопрос задавал В.Т. Гауэрс в обзоре [1].

Перечислим простейшие свойства множества $\mathcal{R}_\alpha$. Из определения $\mathcal{R}_\alpha$ вытекает, что $0 \in \mathcal{R}_\alpha$ и $\mathcal{R}_\alpha = -\mathcal{R}_\alpha$ в том смысле, что если $r \in \mathcal{R}_\alpha$, то и $-r \in \mathcal{R}_\alpha$. Далее, из равенства

*Работа выполнена при финансовой поддержке РФФИ N 06-01-00383, гранта Президента РФ N 1726.2006.1, гранта НШ-691.2008.1 и INTAS (грант N 03–51–5-70).

Парсеваля (2) вытекает оценка на мощность $\mathcal{R}_\alpha$, а именно $|\mathcal{R}_\alpha| \le \delta/\alpha^2$. Существуют ли у множества $\mathcal{R}_\alpha$ еще какие–то нетривиальные свойства? Ответ на этот вопрос оказывается положительным.

Пусть log означает логарифм по основанию два. В 2002 году М.– Ч. Чанг доказала следующий результат [3].

Теорема 1.1 (Чанг) *Пусть δ, α — действительные числа, $0 < \alpha \le \delta \le 1$, A — произвольное подмножество $\mathbb{Z}_N$ мощности δN и множество $\mathcal{R}_\alpha$ определено равенством (3). Тогда найдется множество $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\} \subseteq \mathbb{Z}_N$, $|\Lambda| \le 2(\delta/\alpha)^2 \log(1/\delta)$ такое, что всякий элемент r множества $\mathcal{R}_\alpha$ представляется в виде*

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

где $\varepsilon_i \in \{-1, 0, 1\}$.

Развивая подход из [4] (см. также [5]) Чанг получила приложение своего результата к доказательству теоремы Фреймана [6] о множествах с маленькой суммой. Напомним, что множество $Q \subseteq \mathbb{Z}$ называется *d–мерной арифметической прогрессией*, если

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

где m_i — натуральные, а n_i — целые числа. Справедлива следующая теорема.

Теорема 1.2 (Фрейман) *Пусть $C > 0$ — некоторое число и $A \subseteq \mathbb{Z}$ — произвольное множество. Пусть также $|A + A| \le C|A|$. Тогда найдутся числа d и K, зависящие только от C и d–мерная арифметическая прогрессия Q такая, что $|Q| \le K|A|$ и $A \subseteq Q$.*

Второе приложение теоремы 1.1 получил Б. Грин в статье [7] (см. также более ранние работы [11, 12] и недавнюю работу [13]). Сформулируем один из основных результатов статьи [7].

Теорема 1.3 (Грин) *Пусть A — произвольное подмножество $\mathbb{Z}_N$ мощности δN. Тогда $A + A + A$ содержит арифметическую прогрессию, длина которой не меньше*

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

В другой работе (см. [8]) Грин показал, что в некотором смысле теорема Чанг является точной. Пусть $E = \{e_1, \dots, e_{|E|}\} \subseteq \mathbb{Z}_N$ — произвольное множество. Обозначим через $\mathrm{Span}(E)$ множество всех сумм вида $\sum_{i=1}^{|E|} \varepsilon_i e_i$, где $\varepsilon_i \in \{-1, 0, 1\}$.

Теорема 1.4 (Грин) *Пусть δ, α — действительные числа, $\delta \le 1/8$, $0 < \alpha \le \delta/32$. Пусть также*

$$\left(\frac{\delta}{\alpha}\right)^2 \log(1/\delta) \le \frac{\log N}{\log\log N}. \qquad (6)$$

Тогда найдется множество $A \subseteq \mathbb{Z}_N$, $|A| = [\delta N]$ такое, что множество $\mathcal{R}_\alpha$, определенное формулой (3), не содержится в $\mathrm{Span}(\Lambda)$ для любого множества Λ, $|\Lambda| \le 2^{-12}(\delta/\alpha)^2 \log(1/\delta)$.

Вопрос о структуре множества $\mathcal{R}_\alpha$ когда параметр α близок к δ изучался в работах [14, 15, 16], см. также обзор [17].

Мы видим, что результаты о строении множества $\mathcal{R}_\alpha$ являются важными для комбинаторной теории чисел. В настоящей статье мы доказываем следующую теорему.

Теорема 1.5 *Пусть δ, α — действительные числа, $0 < \alpha \le \delta$, A — произвольное подмножество $\mathbb{Z}_N$ мощности δN, $k \ge 2$ — четное и множество $\mathcal{R}_\alpha$ определено равенством (3). Пусть также $B \subseteq \mathcal{R}_\alpha \setminus \{0\}$ — произвольное множество. Тогда величина*

$$T_k(B) := |\{\ (r_1, \ldots, r_k, r'_1, \ldots, r'_k) \in B^{2k}\ :\ r_1 + \cdots + r_k = r'_1 + \cdots + r'_k\ \}| \tag{7}$$

не меньше, чем

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

Покажем, что утверждение теоремы 1.5 не тривиально, когда параметр δ стремится к нулю при N стремящемся к бесконечности (если δ не стремится к нулю при $N \to \infty$, то структура множества $\mathcal{R}_\alpha$ может быть произвольной, см. по этому поводу работы [18, 19, 20]). Рассмотрим простейший случай $k = 2$. Пусть мощность множества $\mathcal{R}_\alpha$ по–порядку равна δ/α^2. Тогда по теореме 1.5 количество решений уравнения

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

по–порядку не меньше, чем δ/α^4. Среди этих решений существует три серии тривиальных решений. Первая серия — $r_1 = r_3$, $r_2 = r_4$, вторая — $r_1 = r_4$, $r_2 = r_3$ и, наконец, третья серия — $r_1 = -r_2$, $r_3 = -r_4$. Следовательно, у уравнения (9) существует не более $3|\mathcal{R}_\alpha|^2$ тривиальных решений. Так как мощность множества $\mathcal{R}_\alpha$ не превосходит δ/α^2, то величина $3|\mathcal{R}_\alpha|^2$ меньше, чем $3\delta^2/\alpha^4$. Мы видим, что эта величина меньше, чем δ/α^4, когда δ стремится к нулю. Таким образом, теорема 1.5 утверждает, что у уравнения (9) существуют не тривиальные решения. В этом смысле теорема 1.5 показывает, что множество $\mathcal{R}_\alpha$ обладает некоторой аддитивной структурой.

Доказательству теоремы 1.5 посвящен параграф 2. В этом параграфе мы сначала подробно разбираем случай $k = 2$, а затем доказываем теорему 1.5 в общей ситуации.

Обобщению теоремы 1.5 на системы линейных уравнений посвящен §3. В нашем доказательстве мы используем свойства норм Гауэрса (см. [2]).

В параграфе 4 мы получим несколько приложений нашего основного результата к задачам комбинаторной теории чисел. Мы покажем как из теоремы 1.5 и неравенства В. Рудина [21] вытекает теорема М.–Ч. Чанг. Более того, мы докажем результат, усиливающий теорему 1.1 (см. теорему 4.3). Также нами будет получено приложение теоремы 1.5 к уже упомянавшейся теореме Фреймана 1.2.

В наших последующих работах по настоящей тематике, мы планируем получить дальнейшие приложения результатов о больших тригонометрических суммах к задачам комбинаторной теории чисел и, в частности, доказать усиление теоремы 1.3.

Автор выражает глубокую благодарность С. В. Конягину за две его идеи, позволившие усилить формулировку основного результата, а также Н. Г. Мощевитину за постоянное внимание к работе.

2. Доказательство основной теоремы.

Мы начнем этот параграф с объяснения основной идеи доказательства теоремы 1.5. Пусть N — натуральное число и $\widehat{A}(r)$ — преобразование Фурье характеристической функции A. Как мы уже говорили выше, для коэффициентов Фурье множества A справедливо равенство

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

Существуют ли еще какие–то нетривиальные соотношения между коэффициентами Фурье $\widehat{A}(r)$ кроме равенства (10)? Легко видеть, что ответ на этот вопрос положительный.

Рассмотрим чуть более общую ситуацию. Пусть $f : \mathbb{Z}_N \to \mathbb{C}$ — произвольная комплексная функция. Для коэффициентов Фурье функции $f(x)$ справедлива формула обращения

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

Функция $f(x)$ будет характеристической функцией некоторого множества из $\mathbb{Z}_N$ тогда и только тогда, когда для всех x из $\mathbb{Z}_N$ выполнено

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

Подставляя формулу (11) в (12), получаем

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

Отсюда

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

Равенство (14) выполнено при всех $x \in \mathbb{Z}_N$. Следовательно, справедлива формула

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

Таким образом, комплексная функция $f : \mathbb{Z}_N \to \mathbb{C}$ является характеристической тогда и только тогда, когда ее коэффициенты Фурье удовлетворяют равенству (15). Ясно, что для характеристической функции $A(x)$ множества A формула (15) также выполнена. Кроме того, (15) содержит все соотношения между коэффициентами Фурье множества A. Например, равенство Парсеваля (2) получается, если в формуле (15) положить $u = 0$.

В дальнейшем нам понадобится небольшое обобщение равенства (15). Пусть $f, g : \mathbb{Z}_N \to \mathbb{C}$ — произвольные комплексные функции. Тогда

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

Ясно, что из равенства (16) вытекает формула (15).

Приступим к объяснению основной идеи доказательства теоремы 1.5. Пусть $A \subseteq \mathbb{Z}_N$ — произвольное множество, $|A| = \delta N$ и $\mathcal{R}_\alpha$ — множество больших тригонометрических сумм, задаваемое формулой (3). Рассмотрим модельную ситуацию. Пусть для всех $r \in \mathcal{R}_\alpha \setminus \{0\}$ выполнено $|\widehat{A}(r)| = \alpha N$, а если $r \notin \mathcal{R}_\alpha$, $r \neq 0$, то $\widehat{A}(r) = 0$ (обоснованность подобного предположения будет обсуждатся ниже). Пусть $\delta \le 1/4$ и u — произвольный ненулевой вычет из $\mathcal{R}_\alpha$. Тогда $|\widehat{A}(u)| = \alpha N$. Применяя формулу (15) и неравенство треугольника, получаем

$$\alpha N = |\widehat{A}(u)| \le \frac{1}{N} \sum_r |\widehat{A}(r)| |\widehat{A}(r-u)| \le$$

$$\leq \frac{1}{N}\delta N|\widehat{A}(-u)| + \frac{1}{N}|\widehat{A}(u)|\delta N + \frac{1}{N}\sum_{r\neq 0, r\neq u} |\widehat{A}(r)||\widehat{A}(r-u)|\,. \tag{17}$$

Отсюда,

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

Для всех $r \neq 0$ имеем $|\widehat{A}(r)| = \alpha N \cdot \mathcal{R}_\alpha(r)$. Следовательно,

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

Из неравенства (18) вытекает, что для всех $u \in \mathcal{R}_\alpha \setminus \{0\}$ число решений уравнения $r_1 - r_2 = u$, где $r_1, r_2 \in \mathcal{R}_\alpha \setminus \{0\}$ не меньше, чем $1/(2\alpha)$. Следовательно, множество $\mathcal{R}_\alpha$ обладает нетривиальными аддитивными соотношениями.

Перейдем теперь к строгому доказательству теоремы 1.5. Чтобы лучше показать главную идею доказательства нашего основного результата мы докажем теорему 1.5 отдельно для случая $k = 2$, а затем и в общей ситуации. Итак, пусть $k = 2$ и B — произвольное подмножество $\mathcal{R}_\alpha \setminus \{0\}$. Обозначим через $[N]$ отрезок натурального ряда $\{1, 2, \ldots, N\}$.

Нам понадобится следующая лемма.

Лемма 2.1 *Пусть δ, α' — действительные числа, $0 < \alpha' \leq \delta$ и A — произвольное подмножество $\mathbb{Z}_N$ мощности δN. Пусть также*

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

и B' — произвольное подмножество $\mathcal{R}'_{\alpha'} \setminus \{0\}$. Тогда $T_2(B') \geq (\alpha')^4|B'|^4/(16\delta^3)$.

Доказательство. Пусть

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

Функция $f_{B'}(x)$, вообще говоря, является комлексной. Легко видеть, что $\widehat{f}_{B'}(r) = \widehat{A}(r)B'(r)$. Рассмотрим сумму

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

Применяя формулу (16) и равенство Парсеваля, находим

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

Оценим снизу сумму $\sum_x |f_{B'}(x)|^2 A(x)^2$. Используя равенство Парсеваля и определение множества $\mathcal{R}'_{\alpha'}$, получаем

$$\left(\sum_x f_{B'}(x)A(x)\right)^2 = \left(\frac{1}{N}\sum_r \widehat{f}_{B'}(r)\overline{\widehat{A}(r)}\right)^2 = \left(\frac{1}{N}\sum_r |\widehat{f}_{B'}(r)|^2\right)^2 \geq \tag{22}$$

$$\geq (N\alpha'^2|B'|)^2 = \alpha'^4|B'|^2N^2\,. \tag{23}$$

С другой стороны

$$\left(\sum_x f_{B'}(x)A(x)\right)^2 \le \left(\sum_x |f_{B'}(x)|^2 A(x)^2\right)\cdot\left(\sum_x A(x)^2\right) = \delta N\left(\sum_x |f_{B'}(x)|^2 A(x)^2\right). \tag{24}$$

Применяя неравенства (23) и (24), находим

$$\sigma^2 \ge \frac{\alpha'^8}{\delta^2}|B'|^4 N^8\,. \tag{25}$$

Оценим величину σ^2 сверху. Имеем

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

$$= \sum_u \left(\sum_r \widehat{f}_{B'}(r)\overline{\widehat{f}_{B'}(r-u)}\right)\cdot\overline{\left(\sum_r \widehat{A}(r)\overline{\widehat{A}(r-u)}\right)}\,. \tag{26}$$

Отсюда

$$\sigma^2 \le \sum_u \left|\sum_r \widehat{f}_{B'}(r)\overline{\widehat{f}_{B'}(r-u)}\right|^2 \cdot \sum_u \left|\sum_r \widehat{A}(r)\overline{\widehat{A}(r-u)}\right|^2 = \sigma_1\cdot\sigma_2\,. \tag{27}$$

Применяя формулу (15) и равенство Парсеваля, получаем

$$\sigma_2 = N^2 \sum_u |\widehat{A}(u)|^2 = \delta N^4\,. \tag{28}$$

Так как $\widehat{f}_{B'}(r) = \widehat{A}(r)B'(r)$ и $B' \subseteq \mathcal{R}'_{\alpha'}\setminus\{0\}$, то $|\widehat{f}_{B'}(r)| \le 2\alpha' B'(r)N$. Отсюда

$$\sigma_1 \le 16(\alpha')^4 T_2(B')N^4\,. \tag{29}$$

Подставляя оценки (28), (29) в неравенство (25), находим $T_2(B') \ge (\alpha')^4|B'|^4/(16\delta^3)$. Лемма 2.1 доказана.

Пусть

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

Ясно, что $B = \bigsqcup_{i\ge 1} B_i$. Применяя лемму 2.1 к каждому B_i, получаем $T_2(B_i) \ge (\alpha 2^{i-1})^4|B_i|^4/(16\delta^3)$, $i\ge 1$. Отсюда

$$T_2(B) \ge \sum_i T_2(B_i) \ge \frac{\alpha^4}{\delta^3 2^8}\sum_i 2^{4i}|B_i|^4\,. \tag{30}$$

Имеем $|B| = \sum_i |B_i|$. Из неравенства Коши–Буняковского вытекает оценка

$$|B|^4 = \left(\sum_i |B_i|2^i 2^{-i}\right)^4 \le \left(\sum_i 2^{4i}|B_i|^4\right)\cdot\left(\sum_i 2^{-4i/3}\right)^3 \le \sum_i 2^{4i}|B_i|^4\,. \tag{31}$$

Подставляя оценку (31) в (30), получаем неравенство

$$T_2(B) \ge \frac{\alpha^4}{\delta^3 2^8}|B|^4\,. \tag{32}$$

Перейдем теперь к общему случаю $k \geq 2$.

Доказательство теоремы 1.5 Докажем сначала аналог леммы 2.1.

Лемма 2.2 *Пусть δ, α' — действительные числа, $0 < \alpha' \leq \delta$, A — произвольное подмножество $\mathbb{Z}_N$ мощности δN и $k \geq 2$ — четное. Пусть также*

$$\mathcal{R}'_{\alpha'} = \{ \ r \in \mathbb{Z}_N \ : \ \alpha' N \leq |\widehat{A}(r)| < 2\alpha' N \ \} . \tag{33}$$

и B' — произвольное подмножество $\mathcal{R}'_{\alpha'} \setminus \{0\}$. Тогда $T_k(B') \geq \delta(\alpha')^{2k}|B'|^{2k}/(2\delta)^{2k}$.

Доказательство. Пусть функция $f_{B'}(x)$ определена формулой

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

Рассмотрим сумму

$$\sigma = \left(\sum_x f_{B'}(x) A(x) \right)^k . \tag{34}$$

Оценивая σ снизу как в лемме 2.1, находим

$$\sigma \geq (\alpha'^2 |B'| N)^k . \tag{35}$$

Так как k — четное, то k имеет вид $k = 2k'$, $k' \in \mathbb{N}$. Применяя неравенство Гельдера, получаем

$$\sigma = \left(\sum_x f_{B'}(x) A(x) \right)^{2k'} \leq \left(\sum_x |f_{B'}(x)|^{2k'} A^2(x) \right) \left(\sum_x A(x) \right)^{k-1} =$$

$$= \left(\sum_x |f_{B'}(x)|^{2k'} A^2(x) \right) (\delta N)^{k-1} . \tag{36}$$

Отсюда

$$\sigma'^2 = \left(\sum_x |f_{B'}(x)|^{2k'} A^2(x) \right)^2 \geq \delta^2 \frac{\alpha'^{4k}}{\delta^{2k}} |B'|^{2k} N^2 . \tag{37}$$

С другой стороны, применяя формулу обращения (11), находим

$$\sigma' = \sum_x |f_{B'}(x)|^{2k'} A^2(x) =$$

$$= \frac{1}{N^{2k'+2}} \sum_x \sum_{r_1, \dots, r_{k'}, r'_1, \dots, r'_{k'}} \sum_{y,z} \widehat{f}_{B'}(r_1) \dots \widehat{f}_{B'}(r_{k'}) \overline{\widehat{f}_{B'}(r_1)} \dots \overline{\widehat{f}_{B'}(r_{k'})} \widehat{A}(y) \overline{\widehat{A}(z)}$$

$$\times e(x(r_1 + \dots + r_{k'} - r'_1 - \dots - r'_{k'})) e(x(y-z)) =$$

$$= \frac{1}{N^{2k'+1}} \sum_{u,y} \sum_{r_1, \dots, r_{k'}, r'_1, \dots, r'_{k'}, r_1 + \dots + r_{k'} = r'_1 + \dots + r'_{k'} - u} \widehat{f}_{B'}(r_1) \dots \widehat{f}_{B'}(r_{k'})$$

$$\times \overline{\widehat{f}_{B'}(r_1)} \dots \overline{\widehat{f}_{B'}(r_{k'})} \widehat{A}(y) \overline{\widehat{A}(y-u)} =$$

$$= \frac{1}{N^{2k'+1}} \sum_u \left(\sum_y \widehat{A}(y) \overline{\widehat{A}(y-u)} \right) \times$$

$$\times \left(\sum_{r_1,\dots,r_{k'},r'_1,\dots,r'_{k'},r_1+\dots+r_{k'}=r'_1+\dots+r'_{k'}-u} \widehat{f}_{B'}(r_1)\dots\widehat{f}_{B'}(r_{k'}) \overline{\widehat{f}_{B'}(r_1)} \dots \overline{\widehat{f}_{B'}(r_{k'})} \right) \tag{38}$$

Отсюда

$$\sigma'^2 \le \frac{1}{N^{4k'+2}} \sum_u \left| \sum_y \widehat{A}(y) \overline{\widehat{A}(y-u)} \right|^2 \times$$

$$\times \sum_u \left| \sum_{r_1,\dots,r_{k'},r'_1,\dots,r'_{k'},r_1+\dots+r_{k'}=r'_1+\dots+r'_{k'}-u} \widehat{f}_{B'}(r_1)\dots\widehat{f}_{B'}(r_{k'}) \overline{\widehat{f}_{B'}(r_1)} \dots \overline{\widehat{f}_{B'}(r_{k'})} \right|^2 =$$

$$= \frac{1}{N^{4k'+2}} \cdot \sigma_1 \cdot \sigma_2 \,. \tag{39}$$

Применяя формулу (15) и равенство Парсеваля, получаем

$$\sigma_1 = N^2 \sum_u |\widehat{A}(u)|^2 = \delta N^4 \,. \tag{40}$$

Так как $B' \subseteq \mathcal{R}'_{\alpha'} \setminus \{0\}$, то $|\widehat{f}_{B'}(r)| \le 2\alpha' B'(r) N$. Отсюда

$$\sigma_2 \le \left((2\alpha' N)^{2k'} \right)^2 \sum_u \left| \sum_{r_1,\dots,r_{k'},r'_1,\dots,r'_{k'},r_1+\dots+r_{k'}=r'_1+\dots+r'_{k'}-u} B'(r_1)\dots B'(r_{k'}) B'(r_1)\dots B'(r_{k'}) \right|^2$$

$$= (2\alpha' N)^{2k} \cdot T_k(B') \,. \tag{41}$$

Применяя равенства (39), (40) и неравенства (37), (41), находим

$$T_k(B') \ge \delta (\alpha')^{2k} |B'|^{2k} / (2\delta)^{2k} \,. \tag{42}$$

Лемма 2.2 доказана.

Пусть

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

Ясно, что $B = \bigsqcup_{i \ge 1} B_i$. Применяя лемму 2.2 к каждому B_i, получаем $T_k(B_i) \ge \delta(\alpha 2^{i-1})^{2k} |B_i|^{2k} / (2\delta)^{2k}$, $i \ge 1$. Отсюда

$$T_k(B) \ge \sum_i T_k(B_i) \ge \frac{\delta \alpha^{2k}}{2^{4k} \delta^{2k}} \sum_i 2^{2ki} |B_i|^{2k} \,. \tag{43}$$

Имеем $|B| = \sum_i |B_i|$. Применяя неравенство Гельдера, находим

$$|B|^{2k} = \left(\sum_i |B_i| 2^i 2^{-i} \right)^{2k} \le \left(\sum_i 2^{2ki} |B_i|^{2k} \right) \cdot \left(\sum_i 2^{-2ki/(2k-1)} \right)^{2k-1} \le \sum_i 2^{2ki} |B_i|^{2k} \,. \tag{44}$$

Подставляя оценку (44) в (43), получаем неравенство

$$T_k(B) \geq \frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}}|B|^{2k}\,. \tag{45}$$

Теорема 1.5 доказана.

3. Системы линейных уравнений с элементами из множества больших тригонометрических сумм.

Пусть k — натуральное число, $d \geq 0$ — целое. Пусть $A = (a_{ij})$ — матрица $(2^{d+1}k \times (d+1))$, где элементы (a_{ij}) матрицы A определяются по формуле

$$a_{ij} = \begin{cases} 1, & \text{если в двоичном разложении } (j-1) \text{ на } (i-1)\text{-ом месте стоит } 1 \\ & \text{и } 1 \leq j \leq 2^d k\,, \\ -1, & \text{если в двоичном разложении } (j-1) \text{ на } (i-1)\text{-ом месте стоит } 1 \\ & \text{и } 2^d k < j \leq 2^{d+1}k\,, \\ 0, & \text{иначе.} \end{cases}$$

Напоминаем, что двоичное разложение натурального числа n определяется по правилу $n = \sum n_l \cdot 2^{l-1}$, где $l \geq 1$ и $n_l \in \{0,1\}$.

Приведем пример матрицы A. Пусть $k = 2$ и $d = 2$. Тогда

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

Настоящий параграф посвящен доказательству следующей теоремы.

Теорема 3.1 *Пусть δ, α — действительные числа, $0 < \alpha \leq \delta$, A — произвольное подмножество $\mathbb{Z}_N$ мощности δN, k — натуральное число, $d \geq 0$ — целое и множество $\mathcal{R}_\alpha$ определено равенством (3). Пусть также $B \subseteq \mathcal{R}_\alpha \setminus \{0\}$ — произвольное множество. Рассмотрим систему уравнений*

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

где элементы (a_{ij}) матрицы $A = (a_{ij})$, определены формулой выше и все $r_j \in B$. Тогда число решений системы (46) не меньше, чем

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

Ясно, что теорема 3.1 является обобщением теоремы 1.5. Чтобы это увидеть достаточно положить в теореме 3.1 число d равным нулю.

Для доказательства теоремы 3.1 нам понадобятся свойства норм Гауэрса (см. [2]).

Пусть $d \geq 0$ — целое число и $\{0,1\}^d = \{\omega = (\omega_1, \ldots, \omega_d) \ : \ \omega_j \in \{0,1\}, j = 1, 2, \ldots, d\}$ — обычный d—мерный куб. Для $\omega \in \{0,1\}^d$ пусть $|\omega|$ равно $\omega_1 + \cdots + \omega_d$. Если $h = (h_1, \ldots, h_d) \in \mathbb{Z}_N^d$, то $\omega \cdot h := \omega_1 h_1 + \ldots \omega_d h_d$. Пусть также $\mathcal{C}$ означает оператор комлексного сопряжения. Если n — натуральное число, то $\mathcal{C}^n$ означает применение оператора комлексного сопряжения n раз. Пусть также $\|\omega\| = \sum_{i=1}^d \omega_i \cdot 2^{i-1} + 1$. Для всякого

$\omega \in \{0,1\}^d$ определим отображение из $\mathbb{Z}_N^{2^d}$ в $\mathbb{Z}_N$, которое обозначим той же буквой ω, по правилу : если $\vec{r} \in \mathbb{Z}_N^{2^d}$, то $\omega(\vec{r})$ есть $\|\omega\|$–ая компонента вектора $\vec{r}$.

Определение 3.2 Пусть $f : \mathbb{Z}_N \to \mathbb{C}$ — произвольная функция. *Равномерной нормой Гауэрса* (или просто нормой Гауэрса) функции f называется величина

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

Нам понадобится следующая лемма (см. [2]).

Лемма 3.3 (неравенство монотонности для норм Гауэрса) *Пусть $f : \mathbb{Z}_N \to \mathbb{C}$ — произвольная функция и d — натуральное число. Тогда*

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

Дальнейшие свойства норм Гауэрса могут быть найдены в [2].

Докажем лемму.

Лемма 3.4 *Пусть δ, α' — действительные числа, $0 < \alpha' \le \delta$, A — произвольное подмножество $\mathbb{Z}_N$ мощности δN, k — натуральное число и $d \ge 0$ — целое. Пусть также*

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

и B' — произвольное подмножество $\mathcal{R}'_{\alpha'} \setminus \{0\}$. Тогда число решений системы (46) с $r_j \in B'$ не меньше, чем

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

Доказательство. Пусть функция $f(x)$ определена формулой

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

Применяя неравенство Гельдера, находим

$$\left| \sum_x f(x) A(x) \right|^{2k} \le \sum_x |f(x)|^{2k} \cdot \left(\sum_x A(x) \right)^{2k-1} = \sum_x |f(x)|^{2k} \cdot (\delta N)^{2k-1} . \tag{52}$$

С другой стороны, используя равенство Парсеваля и определение множества $\mathcal{R}'_{\alpha'}$, получаем

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

Рассмотрим сумму

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

Из (52) и (53), вытекает неравенство

$$\sigma \ge \frac{\delta \alpha'^{4k}}{\delta^{2k}} |B'|^{2k} \tag{55}$$

Применяя лемму 3.3, находим

$$\sigma^{2^d} \le \frac{1}{N^{d+1}} \sum_{x\in\mathbb{Z}_N} \sum_{h\in\mathbb{Z}_N^d} \prod_{\omega\in\{0,1\}^d} |f(x+\omega\cdot h)|^{2k} = \frac{1}{N^{d+1}} \sum_{x\in\mathbb{Z}_N} \sum_{h\in\mathbb{Z}_N^d} \left| \prod_{\omega\in\{0,1\}^d} f(x+\omega\cdot h) \right|^{2k} \quad (56)$$

Используя формулу обращения (11), получаем

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

Отсюда,

$$\sigma^{2^d} = \frac{1}{N^{k2^{d+1}+d+1}} \sum_{x\in\mathbb{Z}_N} \sum_{h\in\mathbb{Z}_N^d} \sum_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}\in\mathbb{Z}_N^{2^d}} \prod_{i=1}^{k} \prod_{\omega^{(i)}\in\{0,1\}^d} \widehat{f}(\omega^{(i)}(r^{(i)}))e(\omega^{(i)}(r^{(i)})(x+\omega^{(i)}\cdot h))$$

$$\times \prod_{i=k+1}^{2k} \prod_{\omega^{(i)}\in\{0,1\}^d} \overline{\widehat{f}(\omega^{(i)}(r^{(i)}))} e(-\omega^{(i)}(r^{(i)})(x+\omega^{(i)}\cdot h)) \quad (58)$$

Обозначим через $\sum$ систему уравнений

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

Тогда

$$\sigma^{2^d} = \frac{1}{N^{k2^{d+1}+d+1}} \sum_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}\in\mathbb{Z}_N^{2^d}} \prod_{i=1}^{k} \prod_{\omega^{(i)}\in\{0,1\}^d} \widehat{f}(\omega^{(i)}(r^{(i)}))$$

$$\times \prod_{i'=k+1}^{2k} \prod_{\omega^{(i')}\in\{0,1\}^d} \overline{\widehat{f}(\omega^{(i')}(r^{(i')}))} \sum_{x\in\mathbb{Z}_N} \sum_{h\in\mathbb{Z}_N^d} e(\omega^{(i)}(r^{(i)})(x+\omega^{(i)}\cdot h) - \omega^{(i')}(r^{(i')})(x+\omega^{(i')}\cdot h))$$

$$= \frac{1}{N^{k2^{d+1}}} \sum_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}\in\sum} \prod_{i=1}^{k} \prod_{\omega^{(i)}\in\{0,1\}^d} \widehat{f}(\omega^{(i)}(r^{(i)})) \prod_{i=k+1}^{2k} \prod_{\omega^{(i)}\in\{0,1\}^d} \overline{\widehat{f}(\omega^{(i)}(r^{(i)}))} \quad (59)$$

Суммирование в формуле (59) проходит по векторам $r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}$, удовлетворяющим системе уравнений $\sum$. Нетрудно убедиться, что эта система совпадает с системой уравнений (46).

Так как $\widehat{f}_{B'}(r) = \widehat{A}(r)B'(r)$ и $B' \subseteq \mathcal{R}'_{\alpha'} \setminus \{0\}$, то $|\widehat{f}_{B'}(r)| \le 2\alpha' B'(r)N$. Отсюда

$$\sigma^{2^d} \le (2^{2k}(\alpha')^{2k})^{2^d} N^{k2^{d+1}} \tag{60}$$

Применяя неравенства (55), (56) и (60), окончательно находим

$$\sum^{*}_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)} \in \sum} 1 \ge \left(\frac{\delta(\alpha')^{4k}}{\delta^{2k}} |B'|^{2k} \right)^{2^d} \frac{1}{(2^{2k}(\alpha')^{2k})^{2^d}} = \left(\frac{\delta\alpha'^{2k}}{2^{2k}\delta^{2k}} |B'|^{2k} \right)^{2^d} . \tag{61}$$

Суммирование в (61) проходит по векторам $r^{(i)}$, $i \in 1, 2, \dots, 2k$ все компоненты которых принадлежат множеству B'. Иными словами, число решений системы (46) с $r_i \in B'$ не меньше, чем

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

Лемма 3.4 доказана.

Приступим к непосредственному доказательству теоремы 3.1.

Пусть

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

Ясно, что $B = \bigsqcup_{i \ge 1} B_i$.

Пусть E — некоторое множество. Обозначим через $S_{k,d}(E)$ число решений системы уравнений (46) с $r_i \in E$. Применяя лемму 3.4 к каждому B_i, получаем

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

где $i \ge 1$. Отсюда

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

Имеем $|B| = \sum_i |B_i|$. Применяя неравенство Гельдера, находим

$$|B|^{k2^{d+1}} = \left(\sum_i |B_i| 2^i 2^{-i} \right)^{k2^{d+1}} \le \left(\sum_i \left(2^{2ki} |B_i|^{2k} \right)^{2^d} \right) \cdot \left(\sum_i 2^{-(k2^{d+1} i)/(k2^{d+1}-1)} \right)^{k2^{d+1}-1} \le$$

$$\le \sum_i \left(2^{2ki} |B_i|^{2k} \right)^{2^d} . \tag{63}$$

Подставляя оценку (63) в (62), получаем требуемое неравенство

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

Теорема 3.1 доказана.

4. Приложения к задачам комбинаторной теории чисел.

В доказательстве теоремы 1.1 Чанг использовала теорему Рудина [21] (см. также [22]) о диссоциативных подмножествах $\mathbb{Z}_N$. Множество $\mathcal{D} = \{d_1, \dots, d_{|\mathcal{D}|}\} \subseteq \mathbb{Z}_N$ называется *диссоциативным*, если из равенства

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

где $\varepsilon_i \in \{-1, 0, 1\}$ вытекает, что все ε_i равны нулю.

Теорема 4.1 (Рудин) *Существует абсолютная константа $C > 0$ такая, что для произвольного диссоциативного множества $\mathcal{D} \subseteq \mathbb{Z}_N$, произвольных комплексных чисел $a_n \in \mathbb{C}$ и всех натуральных чисел $p \geq 2$ выполнено неравенство*

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

Доказательства теоремы 4.1 и теоремы Чанг могут быть также найдены в [9, 10]. Мы покажем как из теоремы Рудина и теоремы 1.5 вытекает аналог теоремы 1.1, отличающийся от теоремы Чанг только лишь чуть более слабой оценкой на мощность множества Λ.

Предложение 4.2 *Пусть δ, α — действительные числа, $0 < \alpha \leq \delta \leq 1$, A — произвольное подмножество $\mathbb{Z}_N$ мощности δN и множество $\mathcal{R}_\alpha$ определено равенством (3). Тогда найдется множество $\mathcal{D} = \{d_1, \dots, d_{|\mathcal{D}|}\} \subseteq \mathbb{Z}_N$, $|\mathcal{D}| \leq 2^8 C^2 (\delta/\alpha)^2 \log(1/\delta)$ такое, что всякий элемент r множества $\mathcal{R}_\alpha$ представляется в виде*

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

где $\varepsilon_i \in \{-1, 0, 1\}$, а C — абсолютная константа из неравенства Рудина (66).

Доказательство. Пусть $k = 2\lceil \log(1/\delta) \rceil$ и пусть $\mathcal{D} \subseteq \mathcal{R}_\alpha$ — *максимальное* диссоциативное подмножество $\mathcal{R}_\alpha$. Так как $\mathcal{D}$ — диссоциативное множество, то $0 \notin \mathcal{D}$. Применяя теорему 1.5, получаем оценку

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

С другой стороны

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

где C — абсолютная константа из теоремы 4.1. Действительно, пусть числа a_n в формуле (66) равны $\mathcal{D}(n)$, а $p = 2k$. Тогда левая часть в неравенстве (66) есть $T_k(\mathcal{D})$, а правая равна $C^{2k} 2^k k^k |\mathcal{D}|^k$. Имеем $k = 2\lceil \log 1/\delta \rceil$. Применяя неравенства (68) и (69), находим $|\mathcal{D}| \leq 2^8 C^2 (\delta/\alpha)^2 (\log 1/\delta)$. Так как $\mathcal{D}$ максимальное диссоциативное подмножество $\mathcal{R}_\alpha$, то любой элемент r множества $\mathcal{R}_\alpha$ представляется в виде $r = \sum_{i=1}^{|\mathcal{D}|} \varepsilon_i d_i \pmod N$, где $d_i \in \mathcal{D}$ и $\varepsilon_i \in \{-1, 0, 1\}$. Заметим, что оценка $|\mathcal{D}| \leq 2^8 C^2 (\delta/\alpha)^2 \log(1/\delta)$ отличается от аналогичной оценки в теореме Чанг лишь в константу раз. Предложение 4.2 доказано.

В этой статье мы докажем результат, усиливающий теорему Чанг. Наш метод доказательства и работы [23, 24, 25] имеют много общих моментов.

Теорема 4.3 *Пусть N — натуральное число, $(N,2)=1$, δ,α — действительные числа, $0<\alpha\le\delta\le 1/16$, A — произвольное подмножество $\mathbb{Z}_N$ мощности δN и множество $\mathcal{R}_\alpha$ определено равенством (3). Тогда существует множество $\Lambda^*\subseteq\mathbb{Z}_N$,*

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

такое, что для любого вычета $r\in\mathcal{R}_\alpha$ существует набор $\lambda^*_1,\dots,\lambda^*_M$ из не более, чем $8\log(1/\delta)$ элементов Λ^* такой, что

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

где $\varepsilon_i\in\{-1,0,1\}$.

Кроме того, если число N — простое, то найдется множество $\tilde\Lambda\subseteq\mathbb{Z}_N$,

$$|\tilde\Lambda| \le 2^{12}(\delta/\alpha)^2\log(1/\delta)\log\log(1/\delta) \tag{72}$$

такое, что для любого вычета $r\in\mathcal{R}_\alpha$ существует набор $\tilde\lambda_1,\dots,\tilde\lambda_M$ из не более, чем $8\log(1/\delta)$ элементов $\tilde\Lambda$ такой, что

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

где $\varepsilon_i\in\{-1,0,1\}$.

Замечание 4.4 В отличие от теоремы 1.1 в теореме 4.3 вычеты $\lambda^*_1,\dots,\lambda^*_M\in\Lambda^*$ в равенстве (71) и, аналогично, вычеты $\tilde\lambda_1,\dots,\tilde\lambda_M\in\tilde\Lambda$ в равенстве (73) не обязательно различные.

Следствие 4.5 *Пусть N — натуральное число, $(N,6)=1$, δ,α — действительные числа, $0<\alpha\le\delta\cdot\log^{1/2}(1/\delta)$ и множество $\mathcal{R}_\alpha$ определено равенством (3). Тогда существует множество $\Lambda^*\subseteq\mathbb{Z}_N$, $|\Lambda^*|\le 2^{12}(\delta/\alpha)^2\log(1/\delta)$ такое, что для любого вычета $r\in\mathcal{R}_\alpha$ существует набор $\lambda^*_1,\dots,\lambda^*_M$ из не более, чем $8\log(1/\delta)$ элементов Λ^* такой, что $r=\sum_{i=1}^{M}\varepsilon_i\lambda^*_i \pmod N$, где $\varepsilon_i\in\{-1,0,1\}$.*

Для доказательства теоремы 4.3 нам понадобятся несколько вспомогательных утверждений и определений.

Определение 4.6 Пусть k,s — натуральные числа. Рассмотрим семейство множеств $\Lambda(k,s)$ из $\mathbb{Z}_N$, обладающих следующим свойством. Если множество $\Lambda=\{\lambda_1,\dots,\lambda_{|\Lambda|}\}$ принадлежит семейству $\Lambda(k,s)$, то из равенства

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

вытекает, что все s_i равны нулю.

Определение класса $\Lambda(k,1)$ можно найти в статье [26].

Заметим, что для всех $\Lambda\in\Lambda(k,s)$ выполнено $0\notin\Lambda$ и $\Lambda\cap-\Lambda=\emptyset$. Всюду ниже мы не будем специально оговаривать, что равенство двух элементов из $\mathbb{Z}_N$ понимается в смысле равенства по модулю N. Для множеств семейства $\Lambda(k,s)$ справедлива следующая верхняя оценка на величину T_k.

Утверждение 4.7 *Пусть k, s — натуральные числа, Λ — произвольное множество из семейства $\Lambda(k,s)$ и справедливо неравенство $|\Lambda| \ge k$. Тогда*

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

Пример 4.8 Пусть $\log|\Lambda| \ge \log^2 k$ и Λ — произвольное множество из класса $\Lambda(k,3)$. Применяя неравенство (75), получаем $T_k(\Lambda) \le 2^{20k} k^k |\Lambda|^k$. Легко видеть, что эта оценка является неулучшаемой по порядку в том смысле, что для *всякого* множества Λ и для любого натурального k такого, что $\log|\Lambda| \ge \log^2 k$ всегда выполнено $T_k(\Lambda) \ge \binom{|\Lambda|}{k}(k!)^2 \gg e^{-k} k^k |\Lambda|^k$.

Доказательство утверждения 4.7. Пусть $x \in \mathbb{Z}_N$ — произвольный вычет и величина $N_k(x)$ равна числу векторов $(\lambda_1, \dots, \lambda_k)$ таких, что все λ_i принадлежат Λ и $\lambda_1 + \dots + \lambda_k = x$. Тогда $T_k(\Lambda) = \sum_{x \in \mathbb{Z}_N} N_k^2(x)$. Пусть $s_1, \dots, s_l$ — натуральные числа такие, что $s_1 + \dots + s_l = k$. Можно считать, для определенности, набор $s_1, \dots, s_l$ упорядоченным по убыванию $s_1 \ge s_2 \ge \dots \ge s_l \ge 1$. Пусть

$$E(s_1, \dots, s_l)(x) = \{ (\lambda_1, \dots, \lambda_k) \ : \ \text{среди } \lambda_1, \dots, \lambda_k \text{ существует ровно } s_1 \text{ одинаковых } \tilde{\lambda}_1 \,,$$

$$s_2 \text{ одинаковых } \tilde{\lambda}_2 \,, \dots, s_l \text{ одинаковых } \tilde{\lambda}_l \text{ таких, что } s_1\tilde{\lambda}_1 + \dots + s_l\tilde{\lambda}_l = x \text{ и все } \tilde{\lambda}_i \text{ — различные} \}$$

Будем обозначать, для краткости, множество $E(s_1, \dots, s_l)(x)$, через $E(\vec{s})(x)$. Напоминаем, что числа $s_1, \dots, s_l$ в определении множеств $E(\vec{s})(x) = E(s_1, \dots, s_l)(x)$ обладают тем свойством, что $\sum_{i=1}^l s_i = k$. Тогда

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

где суммирование проходит по всем векторам со свойством $\sum_{i=1}^l s_i = k$. Отсюда

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

Пусть $\vec{s} = (s_1, \dots, s_l)$ и $G = G(\vec{s}) = \{ i \ : \ s_i \le s \}$, $B = B(\vec{s}) = \{ i \ : \ s_i > s \}$. Тогда $|G(\vec{s})| + |B(\vec{s})| = l(\vec{s}) = l$. Справедливо неравенство

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

Действительно,

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

Из неравенства (78) вытекает неравенство (77).

Докажем следующую лемму.

Лемма 4.9 *Для любого $\vec{s}$, $\sum_{i=1}^l s_i = k$ и любого $x \in \mathbb{Z}_N$ выполнено*

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

Доказательство леммы 4.9. Пусть $(\lambda_1, \dots, \lambda_k)$ — произвольный набор из $E(\vec{s})(x)$. Тогда $\sum_{i=1}^k \lambda_i = \sum_{i=1}^l s_i \tilde{\lambda}_i = x$, где $\tilde{\lambda}_i \in \{\lambda_1, \dots, \lambda_k\}$ — различные. Рассмотрим другой набор $(\lambda'_1,\dots,\lambda'_k)$ из $E(\vec{s})(x)$, $\sum_{i=1}^k \lambda'_i = \sum_{i=1}^l s_i\tilde{\lambda}'_i = x$, где $\tilde{\lambda}'_i \in \{\lambda'_1,\dots,\lambda'_k\}$ — различные. Предположим, что для всех $i \in B(\vec{s})$ выполнено $\tilde{\lambda}_i = \tilde{\lambda}'_i$. Докажем, что тогда для всех $i \in G(\vec{s})$ выполняется равенство $\tilde{\lambda}_i = \tilde{\lambda}'_i$. Имеем $\sum_{i=1}^l s_i\tilde{\lambda}_i = x = \sum_{i=1}^l s_i\tilde{\lambda}'_i$. Отсюда $\sum_{i\in G} s_i\tilde{\lambda}_i = \sum_{i\in G} s_i\tilde{\lambda}'_i$. Кроме того, $\Lambda \cap -\Lambda = \emptyset$. Следовательно, $\sum_{i\in G} s_i\tilde{\lambda}_i - \sum_{i\in G} s_i\tilde{\lambda}'_i = \sum_i s'_i\lambda^0_i = 0$, где $s'_i \in \mathbb{Z}$, $|s'_i| \le s$, $\sum_i |s'_i| \le 2k$ и $\lambda^0_i \in \Lambda$ — различные. Из определения семейства $\Lambda(k,s)$ вытекает, что все s'_i равны нулю. Отсюда для всех $i \in G(\vec{s})$ выполнено $\tilde{\lambda}_i = \tilde{\lambda}'_i$. Значит, набор $(\lambda'_1,\dots,\lambda'_k)$ является перестановкой набора $(\lambda_1,\dots,\lambda_k)$. По определению множества $E(\vec{s})(x)$ среди вычетов $\lambda_1,\dots,\lambda_k$ существуют ровно s_1 одинаковых $\tilde{\lambda}_1$, s_2 одинаковых $\tilde{\lambda}_2,\dots,s_l$ одинаковых $\tilde{\lambda}_l$ таких, что $s_1\tilde{\lambda}_1+\dots+s_l\tilde{\lambda}_l = x$ причем все $\tilde{\lambda}_i$ — различны. Следовательно, число перестановок одного набора $(\lambda_1,\dots,\lambda_k)$ равно $k!/(s_1!\dots s_l!)$. Таким образом, при фиксированных $\tilde{\lambda}_i$, $i\in B$ мы имеем не более $k!/(s_1!\dots s_l!)$ наборов $(\lambda_1,\dots,\lambda_k)$, принадлежащих $E(\vec{s})(x)$. Отсюда мощность $E(\vec{s})(x)$ не превосходит $|\Lambda|^{|B(\vec{s})|}k!/(s_1!\dots s_l!)$. Лемма 4.9 доказана.

Вернемся к доказательству утверждения 4.7.

Оценим сумму σ. Пусть b — целое неотрицательное число и пусть

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

Из неравенства (77) вытекает, что для всякого $\vec{s}$ выполнено $|B(\vec{s})| \le [k/s]$. Отсюда **и неравенства Коши–Буняковского получаем** $\sigma \le ([(\mathbf{k}-\mathbf{1})/\mathbf{s}]+\mathbf{1})^{\mathbf{2}} \sum_{b=0}^{[k/s]} \sigma_b$. Зафиксируем b и оценим сумму σ_b. Имеем

$$\sigma_b \le \left(\sum_{x\in\mathbb{Z}_N}\sum_{\vec{s}:|B(\vec{s})|=b} |E(\vec{s})(x)|\right)\cdot\left(\max_{x\in\mathbb{Z}_N}\sum_{\vec{s}:|B(\vec{s})|=b} |E(\vec{s})(x)|\right) . \tag{81}$$

Пусть $P_k(\vec{s}) = k!/(s_1!\dots s_l!)$. Тогда

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

Применяя лемму 4.9, находим $|E(\vec{s})(x)| \le P_k(\vec{s})|\Lambda|^{|B(\vec{s})|}$. Отсюда и неравенства (82), получаем

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

Рассмотрим сумму

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

Из неравенства (77) вытекает, что данная сумма оценивается сверху числом наборов $(\lambda_1,\dots,\lambda_k)\in\Lambda^k$ таких, что среди $\lambda_1,\dots,\lambda_k$ имеется не более $k-sb$ различных. Следовательно,

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

Отсюда и (83), находим

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

Значит,

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

Оценим сумму σ^*. Если $k^s \le |\Lambda|^{s-1}$, то легко видеть, что $\sigma^* \le [(\mathbf{k-1})/\mathbf{s}]+\mathbf{1}$. Если же $k^s > |\Lambda|^{s-1}$, то $\sigma^* \le ([(\mathbf{k-1})/\mathbf{s}]+\mathbf{1})(k/|\Lambda|)^k |\Lambda|^{k/s} \cdot |\mathbf{\Lambda}|^{\mathbf{1-1/s}}/\mathbf{k}$. В любом случае $\sigma^* \le ([(\mathbf{k-1})/\mathbf{s}]+\mathbf{1}) \max\{1, (k/|\Lambda|)^k |\Lambda|^{k/s} \cdot |\mathbf{\Lambda}|^{\mathbf{1-1/s}}/\mathbf{k}\}$. Следовательно,

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

Утверждение 4.7 доказано.

Приступим к непосредственному доказательству теоремы 4.3.

Доказательство. Пусть $k = 2\lceil \log(1/\delta) \rceil$. Пусть также $s = 2$ и пусть $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ — максимальное подмножество $\mathcal{R}_\alpha \setminus \{0\}$, принадлежащее семейству $\Lambda(k,s)$. Если $\mathcal{R}_\alpha = \{0\}$, то доказывать нечего. Если $\mathcal{R}_\alpha \setminus \{0\}$ не пусто, то тогда и Λ не пусто. Пусть $\Lambda^* = (\bigcup_{j=1}^s j^{-1}\Lambda) \bigsqcup \{0\}$. Тогда $|\Lambda^*| \le 4|\Lambda|$ и $0 \in \Lambda^*$. Докажем, что для любого $x \in \mathcal{R}_\alpha \setminus \{0\}$ найдется $j \in [s]$ такое, что

$$xj = \sum_{i=1}^{|\Lambda|} \lambda_i s_i \,, \quad \text{где } s_i \in \mathbb{Z} \,, \quad |s_i| \le s \,, \quad \sum_{i=1}^{|\Lambda|} |s_i| \le 2k \,. \tag{89}$$

Так как для любых $i \in [|\Lambda|]$, $j \in [s]$ выполнено $j^{-1}\lambda_i \in \Lambda^*$, то из равенства (89) будет вытекать нужное нам утверждение. Итак, пусть x — произвольный элемент из $\mathcal{R}_\alpha \setminus \Lambda$, $x \ne 0$. Рассмотрим все соотношения вида $\sum_{i=1}^{|\Lambda|+1} \tilde{\lambda}_i s_i = 0$, где $\tilde{\lambda}_i \in \Lambda \bigsqcup \{x\}$ и $s_i \in \mathbb{Z}$, $|s_i| \le s$, $\sum_{i=1}^{|\Lambda|+1} |s_i| \le 2k$. Если все такие соотношения тривиальны, то есть если для любого такого соотношения выполнено $s_i = 0$, $i \in [|\Lambda|+1]$, то мы получаем противоречие с максимальностью Λ. Значит, существует нетривиальное соотношение вида (89) такое, что не все числа $j, s_1, \dots, s_{|\Lambda|}$ равны нулю. При этом $j \in [-s, \dots, s]$. Если $j = 0$, то получаем противоречие с тем, что Λ принадлежит классу $\Lambda(k,s)$. Следовательно, можно считать, что $j \in [s]$. Так как $2k \le 8\log(1/\delta)$, то мы получаем, что для любого элемента $x \in \mathcal{R}_\alpha$ существуют набор $\lambda_1^*, \dots, \lambda_M^*$ из не более, чем $8\log(1/\delta)$ элементов Λ^* такой, что выполнено равенство (71).

Получим оценку $|\Lambda^*| \le \max(\, 2^{12}(\delta/\alpha)^2 \log(1/\delta),\, 2^6 \log^2(1/\delta)\,)$.

Если $|\Lambda| \le k^2$, то $|\Lambda| \le 2^4 \log^2(1/\delta)$ и, следовательно, $|\Lambda^*| \le 2^6 \log^2(1/\delta)$. Если же $|\Lambda| > k^2$, то по утверждению 4.7 имеем $T_k(\Lambda) \le 2^{3k} k^k |\Lambda|^k$. С другой стороны, применяя теорему 1.5, получаем $T_k(\Lambda) \ge \delta \alpha^{2k} |\Lambda|^{2k} / (2^{4k} \delta^{2k})$. Отсюда $|\Lambda| \le 2^{10}(\delta/\alpha)^2 \log(1/\delta)$ и, следовательно, $|\Lambda^*| \le 2^{12}(\delta/\alpha)^2 \log(1/\delta)$.

В любом случае $|\Lambda^*| \le \max(\, 2^{12}(\delta/\alpha)^2 \log(1/\delta),\, 2^6 \log^2(1/\delta)\,)$.

Теперь докажем существование множества $\tilde{\Lambda}$. Пусть $s = [\log\log(1/\delta)]$ и Λ_1 — максимальное подмножество $\mathcal{R}_\alpha \setminus \{0\}$, принадлежащее семейству $\Lambda(k,s)$, $k = 2\lceil \log(1/\delta) \rceil$. Пусть $\tilde{\Lambda} = \bigcup_{j=1}^s j^{-1}\Lambda_1$. Тогда $|\tilde{\Lambda}| \le s|\Lambda_1|$. Применяя рассуждения, аналогичные приведенным выше, легко показать, что для любого вычета $r \in \mathcal{R}_\alpha$ существует набор $\tilde\lambda_1, \dots, \tilde\lambda_M$ из не более, чем $8\log(1/\delta)$ элементов $\tilde\Lambda$ такой, что выполнено равенство (73).

Докажем неравенство (72). Если $|\Lambda_1| \le k^{s/(s-1)}$, то $|\Lambda_1| \le 2^{10}\log(1/\delta)$ и $|\tilde\Lambda| \le s|\Lambda_1| \le 2^{12}\log(1/\delta)\log\log(1/\delta)$. Мы видим, что в этом случае неравенство (72) доказано. Пусть теперь $|\Lambda_1| > k^{s/(s-1)}$. Применяя утверждение 4.7, находим $T_k(\Lambda_1) \le 2^{3k}k^k|\Lambda_1|^k$. С другой стороны из теоремы 1.5 вытекает, что $T_k(\Lambda_1) \ge \delta\alpha^{2k}|\Lambda_1|^{2k}/(2^{4k}\delta^{2k})$. Отсюда $|\Lambda_1| \le 2^{10}(\delta/\alpha)^2\log(1/\delta)$ и, следовательно, $|\tilde\Lambda| \le 2^{12}(\delta/\alpha)^2\log(1/\delta)\log\log(1/\delta)$. Теорема доказана.

Получим теперь приложение доказанных теорем 1.5 и 4.3 к задачам комбинаторной теории чисел.

Пусть K — произвольное подмножество $\mathbb{Z}_N$ и $\varepsilon \in (0,1)$ — любое действительное число. *Множеством Бора* $B(K,\varepsilon)$ называется множество

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

где $\|\cdot\|$ — означает целую часть действительного числа. О свойствах множеств Бора см. статью [27]. В частности, в этой статье было получено неравенство

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

При доказательстве количественного варианта теоремы Фреймана в работе [3] (см. также [10]) Чанг использовала следующее предложение.

Предложение 4.10 *Пусть N — натуральное число, $\delta \in (0,1)$ — действительное число и A — произвольное подмножество $\mathbb{Z}_N$, $|A| = \delta N$. Тогда $2A-2A$ содержит множество Бора $B(K,\varepsilon)$, где $|K| \le 8\delta^{-1}\log(1/\delta)$ и $\varepsilon = \delta/(2^8\log(1/\delta))$.*

Мы докажем небольшое усиление предложения 4.10.

Предложение 4.11 *Пусть N — натуральное число, $(N,2) = 1$, $0 < \delta \le 2^{-256}$ — действительное число и A — произвольное подмножество $\mathbb{Z}_N$, $|A| = \delta N$. Тогда $2A-2A$ содержит множество Бора $B(K,\varepsilon)$, где $|K| \le 2^{15}\delta^{-1}\log(1/\delta)$ и $\varepsilon = 1/(2^8\log(1/\delta))$.*

Применяя формулу (90) получаем, что размер множества Бора $B(K,\varepsilon)$ в предложении 4.10 не меньше $(1/2)\cdot 2^{-8\delta^{-1}(\log 1/\delta)^2}N$. В предложении 4.11 мощность множества Бора не меньше $(1/2)\cdot 2^{-2^{20}\delta^{-1}(\log 1/\delta)(\log\log 1/\delta)}N$.

Для доказательства предложения 4.11 нам понадобится следующее определение.

Определение 4.12 Пусть $f, g : \mathbb{Z}_N \to \mathbb{C}$ — произвольные функции. *Сверткой* функций f и g назовем функцию $(f*g)(x)$, которая определяется формулой

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

Легко видеть, что

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

Доказательство предолжения 4.11. Пусть $\alpha = \delta^{3/2}/2\sqrt{2}$. Применяя следствие 4.5 к $\mathcal{R}_\alpha(A)$, находим множество $\Lambda^* \subseteq \mathbb{Z}_N$, $|\Lambda^*| \le 2^{15}\delta^{-1}\log(1/\delta)$ такое, что для любого вычета $r \in \mathcal{R}_\alpha$ существует набор $\lambda_1^*, \dots, \lambda_M^*$ из не более, чем $8\log(1/\delta)$ элементов Λ^* такой, что выполнено равенство (71). Пусть $\mathcal{R}_\alpha^* = \mathcal{R}_\alpha \setminus \{0\}$. Рассмотрим множество Бора $B_1 = B(\mathcal{R}_\alpha^*, 1/20)$. Для всех $x \in B_1$ и всех $r \in \mathcal{R}_\alpha^*$ выполнено

$$|1 - e(rx)| = 2|\sin(\pi rx/N)| \le \frac{2\pi}{20} < \frac{1}{2}\,. \tag{93}$$

Легко видеть, что выражение $(A * A * A * A)(x)$ равно числу четверок $(a_1, a_2, a_3, a_4) \in A^4$, удовлетворяющих равенству $a_1 + a_2 - a_3 - a_4 = x$. Отсюда, $(A * A * A * A)(x) > 0$ тогда и только тогда, когда $x \in 2A - 2A$. Применяя формулы (11) и (92), получаем, что x принадлежит $2A - 2A$ тогда и только тогда, когда $\sum_r |\widehat{A}(r)|^4 e(rx) > 0$. Пусть $x \in B_1$. Тогда

$$\sum_r |\widehat{A}(r)|^4 e(rx) = \sum_r |\widehat{A}(r)|^4 - \sum_r |\widehat{A}(r)|^4 (1 - e(rx)) > \frac{1}{2} \sum_r |\widehat{A}(r)|^4 - 2 \sum_{r \notin R, r \neq 0} |\widehat{A}(r)|^4 \geq$$

$$\geq \frac{1}{2} \delta^4 N^4 - 2 \max_{r \notin R, r \neq 0} |\widehat{A}(r)|^2 \sum_r |\widehat{A}(r)|^2 \geq \frac{1}{2} \delta^4 N^4 - 2 \frac{\delta^3 N^2}{8} \delta N^2 = \frac{\delta^4 N^4}{4} > 0 \,. \tag{94}$$

(при выводе формулы (94) мы использовали равенство Парсеваля (2)). Из неравенства (94) вытекает, что множество Бора B_1 принадлежит $2A - 2A$. Рассмотрим другое множество Бора $B_2 = B(\Lambda^*, 1/(2^8 \log(1/\delta))$ и докажем включение $B_2 \subseteq B_1$. Так как для любого вычета $r \in \mathcal{R}^*_\alpha$ существует набор $\lambda^*_1, \ldots, \lambda^*_M$ из не более, чем $8 \log(1/\delta)$ элементов Λ^* такой, что выполнено равенство (71), то для всех $x \in B_2$ справедливо неравенство

$$\left\| \frac{rx}{N} \right\| \leq \sum_{i=1}^{M} \left\| \frac{\lambda^*_i x}{N} \right\| \leq 8 \log(1/\delta) \cdot \frac{1}{2^8 \log(1/\delta)} < \frac{1}{20} \,. \tag{95}$$

Таким образом, всякий $x \in B_2$ принадлежит B_1. Мы получили множество Бора $B_2 \subseteq 2A - 2A$, удовлетворяющее всем требуемым свойствам. Предложение 4.11 доказано.

Список литературы

[1] *Gowers W. T.* Rough structure and classification // Geom. Funct. Anal., Special Volume - GAFA2000 "Visions in Mathematics", Tel Aviv, (1999) Part I, 79–117.

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

[3] *Chang M.–C.,* A polynomial bound in Freiman's theorem // Duke Math. J. **113** (2002) no. 3, 399–419.

[4] *Ruzsa I.* Generalized arithmetic progressions and sumsets // Acta Math. Hungar., **65** (1994), 379–388.

[5] *Bilu Y.* Structure of sets with small sumset // Structure Theory of Sets Addition, Astérisque, Soc. Math. France, Montrouge, **258** (1999), 77–108.

[6] *Фрейман Г. А.* Основания структурной теории сложения множеств / Казанский гос. пед. инст., Казань, 1966.

[7] *Green B.* Arithmetic Progressions in Sumsets // Geom. Funct. Anal., **12** (2002) no. 3, 584–597.

[8] *Green B.* Some constructions in the inverse spectral theory of cyclic groups // Comb. Prob. Comp. **12** (2003) no. 2, 127–138.

[9] *Green B.* Spectral structure of sets of integers // Fourier analysis and convexity (survey article, Milan 2001), Appl. Numer. Harmon. Anal., Birkhauser Boston, Boston, MA (2004), 83–96.

[10] *Green B.* Structure Theory of Set Addition // ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis, Edinburgh March 25 — April 5 2002.

[11] *Bourgain J.* On Aritmetic Progressions in Sums of Sets of Integers // A Tribute of Paul Erdös, Cambridge University Press, Cambridge (1990), 105–109.

[12] *Freiman G. A., Halberstam H., Ruzsa I.* Integer Sumsets Containing Long Arithmetic Progressions // J. London Math. Soc. **46** (1992) no. 2, 193–201.

[13] *Croot E., Ruzsa I., Tomasz S.* Arithmetic progressions in sparse sumsets // представлено в печать.

[14] *Юдин А. А.* // Теория чисел (под ред. Г.А. Фреймана, А.М. Рубинова, Е.В. Новоселова), Калининский гос. унив., Москва (1973), 163–174.

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

[16] *Lev V. F.* Linear Equations over $\mathbb{F}_p$ and Moments of Exponential Sums // Duke Mathematical Journal **107** (2001), 239–263.

[17] *Konyagin S. V., Lev V. F.* On the distribution of exponential sums // Integers: Electronic Journal of Combinatorial Number Theory **0** # A01, (2000).

[18] *de Leeuw K., Katznelson Y., Kahane J. P.* Sur les coefficients de Fourier des fonctions continues // C. R. Acad. Sci. Paris Sér. A–B **285** (1977) no. 16, A1001–A1003.

[19] *Назаров Ф. Л.* Ударное решение задачи о коэффициентах // Алгебра и анализ **9** (1997) вып. 2, 272–287.

[20] *Ball K.* Convex geometry and functional analysis // Handbook of the geometry of Banach spaces, vol. I, North–Holland, Amsterdam (2001), 161–194.

[21] *Rudin W.* Fourier analysis on groups / Wiley 1990 (репринт издания 1962 года).

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

[23] *Виноградов И. М.* Метод тригонометрических сумм в теории чисел / М.: Наука, 1971.

[24] *Линник Ю. В.* О суммах Вейля // Матем. сб. **12** (1943) вып. I, 28–39.

[25] *Нестеренко Ю. В.* К теореме о среднем И.М. Виноградова // Труды Московского Математического общества **48** (1985), 97–105.

[26] *Bajnok B., Ruzsa I.* The independence number of a subset of an abelian group // Integers: Electronic Journal of Combinatorial Number Theory **3** # A02, 2003.

[27] *Bourgain J.* On triples in arithmetic progression // Geom. Funct. Anal. **9** (1999), 968–984.