Math-Net.Ru

Общероссийский математический портал

И. Д. Шкредов, О множествах больших тригонометрических сумм, *Изв. РАН. Сер. матем.*, 2008, том 72, выпуск 1, 161–182

DOI: <https://doi.org/10.4213/im1140>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.196.121.252

26 апреля 2023 г., 17:09:22

УДК 511.218+511.336

И. Д. Шкредов

О множествах больших тригонометрических сумм

Доказано существование нетривиальных решений уравнения $r_1 + r_2 = r_3 + r_4$, где r_1, r_2, r_3, r_4 принадлежат множеству R больших коэффициентов Фурье некоторого подмножества A из $\mathbb{Z}/N\mathbb{Z}$. Из этого утверждения следует, что множество R имеет сильные аддитивные свойства. Обсуждаются обобщения и приложения полученных результатов.

Библиография: 26 наименований.

§ 1. Введение

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

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

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

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

Пусть δ, α – действительные числа, $0 < \alpha \leq \delta \leq 1$, и пусть A – некоторое подмножество множества $\mathbb{Z}_N$ мощностью δN . Будем обозначать также через A характеристическую функцию этого множества. Рассмотрим множество $\mathcal{R}_\alpha$ больших тригонометрических сумм A :

$$\mathcal{R}_\alpha = \mathcal{R}_\alpha(A) = \{r \in \mathbb{Z}_N : |\hat{A}(r)| \geq \alpha N\}. \quad (3)$$

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 далее, а здесь 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 Парсеваля (2) вытекает оценка мощностью $\mathcal{R}_\alpha$, а именно $|\mathcal{R}_\alpha| \leq \delta/\alpha^2$. Существуют ли у множества $\mathcal{R}_\alpha$ еще какие-либо нетривиальные свойства? Ответ на этот вопрос оказывается положительным.

Через $\log$ обозначаем логарифм по основанию два.

В 2002 г. М.-Ч. Чанг доказала следующий результат [2].

Работа выполнена при финансовой поддержке РФФИ (грант № 06-01-00383), Программы Президента РФ (грант № 1726.2006.1) и INTAS (грант № 03-51-5-70).

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

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

где $\varepsilon_i \in \{-1, 0, 1\}$.

Развивая подход, предложенный в [3] (см. также [4]), Чанг получила приложение своего результата к доказательству теоремы Фреймана [5] о множествах с малой суммой. Напомним, что множество $Q \subseteq \mathbb{Z}$ называется d -мерной арифметической прогрессией, если

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

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

ТЕОРЕМА 2 (Г. А. Фрейман). Пусть $C > 0$ – некоторое число, $A \subseteq \mathbb{Z}$ – произвольное множество и $|A + A| \leq C|A|$. Тогда найдутся числа d и K , зависящие только от C , и d -мерная арифметическая прогрессия Q такие, что $|Q| \leq K|A|$ и $A \subseteq Q$.

Второе приложение теоремы 1 получил Б. Грин в статье [6] (см. также более ранние работы [7], [8] и недавнюю работу [9]). Сформулируем один из основных результатов статьи [6].

ТЕОРЕМА 3 (Б. Грин). Пусть A – произвольное подмножество множества $\mathbb{Z}_N$ мощностью δN . Тогда $A + A + A$ содержит арифметическую прогрессию, длина которой не меньше

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

В другой работе (см. [10]) Грин показал, что теорема Чанг является в некотором смысле точной. Пусть $E = \{e_1, \dots, e_{|E|}\} \subseteq \mathbb{Z}_N$ – произвольное множество. Обозначим через $\text{Span}(E)$ множество всех сумм вида $\sum_{i=1}^{|E|} \varepsilon_i e_i$, где $\varepsilon_i \in \{-1, 0, 1\}$.

ТЕОРЕМА 4 (Б. Грин). Пусть δ, α – действительные числа, $\delta \leq 1/8$, $0 < \alpha \leq \delta/32$. Пусть также

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

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

Вопрос о структуре множества $\mathcal{R}_\alpha$, когда параметр α близок к δ , изучался в работах [11]–[13] (см. также обзор [14]).

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

ТЕОРЕМА 5. Пусть δ, α – действительные числа, $0 < \alpha \leq \delta$, A – произвольное подмножество множества $\mathbb{Z}_N$ мощностью δN , $k \geq 2$ – четное число и множество $\mathcal{R}_\alpha$ определено равенством (3). Пусть также $B \subseteq \mathcal{R}_\alpha \setminus \{0\}$ – произвольное множество. Тогда величина

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

не меньше

$$\frac{\delta \alpha^{2k}}{2^{4k} \delta^{2k}} |B|^{2k}. \quad (8)$$

Покажем, что утверждение теоремы 5 не тривиально, когда параметр δ стремится к нулю при N , стремящемся к бесконечности (если δ не стремится к нулю при $N \rightarrow \infty$, то структура множества $\mathcal{R}_\alpha$ может быть произвольной [15]–[17]). Рассмотрим простейший случай $k = 2$. Пусть мощность множества $\mathcal{R}_\alpha$ по порядку равна δ/α^2 . Тогда по теореме 5 количество решений уравнения

$$r_1 + r_2 = r_3 + r_4, \quad r_1, r_2, r_3, r_4 \in \mathcal{R}_\alpha \setminus \{0\}, \quad (9)$$

по порядку не меньше δ/α^4 . Среди этих решений существует три серии тривиальных решений. В первой серии $r_1 = r_3$, $r_2 = r_4$, во второй $r_1 = r_4$, $r_2 = r_3$ и, наконец, в третьей серии $r_1 = -r_2$, $r_3 = -r_4$. Следовательно, уравнение (9) имеет 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 5 утверждает, что уравнение (9) имеет нетривиальные решения. Отсюда следует, что множество $\mathcal{R}_\alpha$ обладает некоторой аддитивной структурой.

Доказательству теоремы 5 посвящен § 2, где мы сначала подробно разбираем случай $k = 2$, а затем доказываем теорему 5 в общей ситуации.

Обобщению теоремы 5 на системы линейных уравнений посвящен § 3. В нашем доказательстве мы используем свойства норм Гауэрса (см. [18]).

В § 4 мы получим несколько приложений нашего основного результата к задачам комбинаторной теории чисел. Мы покажем, как из теоремы 5 и неравенства В. Рудина [19] вытекает теорема М.-Ч. Чанг. Более того, мы докажем результат, усиливающий теорему 1 (см. теорему 8). Также нами будет получено приложение теоремы 5 к теореме 2.

В последующих работах по настоящей тематике автор планирует получить дальнейшие приложения результатов о больших тригонометрических суммах к задачам комбинаторной теории чисел.

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

§ 2. Доказательство основной теоремы 5

Приведем некоторые предварительные рассуждения. Пусть N – натуральное число и $\hat{A}(r)$ – преобразование Фурье характеристической функции A . Как сказано выше, для коэффициентов Фурье множества A справедливо равенство

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

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

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

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

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

$$|f(x)|^2 = f(x). \quad (12)$$

Подставляя формулу (11) в (12), получаем

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

Отсюда имеем

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

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

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

Таким образом, комплексная функция $f: \mathbb{Z}_N \rightarrow \mathbb{C}$ 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 следующее обобщение равенства (15). Пусть $f, g: \mathbb{Z}_N \rightarrow \mathbb{C}$ – произвольные комплексные функции. Тогда

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

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

Объясним основную идею доказательства теоремы 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 $|\hat{A}(r)| = \alpha N$, а если $r \notin \mathcal{R}_\alpha$, $r \neq 0$, то $\hat{A}(r) = 0$ (обоснованность подобного предположения будет обсуждаться ниже). Пусть $\delta \leq 1/4$ и u – произвольный ненулевой вычет из $\mathcal{R}_\alpha$. Тогда $|\hat{A}(u)| = \alpha N$. Применяя формулу (15) и неравенство треугольника, получаем

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

Отсюда имеем

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

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

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

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 5. Докажем эту теорему отдельно для случая $k = 2$, а затем – в общей ситуации. Итак, пусть $k = 2$ и B – произвольное подмножество множества $\mathcal{R}_\alpha \setminus \{0\}$. Обозначим через $[N]$ отрезок натурального ряда $\{1, 2, \dots, N\}$.

Нам понадобится следующая лемма.

ЛЕММА 1. Пусть δ, α' – действительные числа, $0 < \alpha' \leq \delta$, и A – произвольное подмножество множества $\mathbb{Z}_N$ мощностью δN . Пусть также

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

и B' – произвольное подмножество множества $\mathcal{R}'_{\alpha'} \setminus \{0\}$. Тогда

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

ДОКАЗАТЕЛЬСТВО. Пусть

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

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

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

Применяя формулу (16) и равенство Парсеваля, находим

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

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

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

С другой стороны,

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

Применяя неравенства (22) и (23), находим

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

Оценим величину σ^2 сверху. Имеем

$$\begin{aligned} \sigma &= \sum_s \sum_{r, r'} \hat{f}_{B'}(r) \overline{\hat{f}_{B'}(r')} \overline{\hat{A}(r-s)} \hat{A}(r'-s) \\ &= \sum_u \left(\sum_r \hat{f}_{B'}(r) \overline{\hat{f}_{B'}(r-u)} \right) \overline{\left(\sum_r \hat{A}(r) \hat{A}(r-u) \right)}. \end{aligned} \quad (25)$$

Отсюда получаем

$$\sigma^2 \leq \sum_u \left| \sum_r \hat{f}_{B'}(r) \overline{\hat{f}_{B'}(r-u)} \right|^2 \sum_u \left| \sum_r \hat{A}(r) \overline{\hat{A}(r-u)} \right|^2 = \sigma_1 \sigma_2. \quad (26)$$

Применяя формулу (15) и равенство Парсеваля, получаем

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

Поскольку $\hat{f}_{B'}(r) = \hat{A}(r) B'(r)$ и $B' \subseteq \mathcal{R}'_{\alpha'} \setminus \{0\}$, то $|\hat{f}_{B'}(r)| \leq 2\alpha' B'(r) N$. Отсюда имеем

$$\sigma_1 \leq 16(\alpha')^4 T_2(B') N^4. \quad (28)$$

Подставляя (27), (28) в неравенство (24), находим $T_2(B') \geq (\alpha')^4 |B'|^4 / (16\delta^3)$. Лемма доказана.

Пусть

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

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

$$T_2(B) \geq \sum_i T_2(B_i) \geq \frac{\alpha^4}{28\delta^3} \sum_i 2^{4i} |B_i|^4. \quad (29)$$

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

$$|B|^4 = \left(\sum_i 2^i 2^{-i} |B_i| \right)^4 \leq \left(\sum_i 2^{4i} |B_i|^4 \right) \left(\sum_i 2^{-4i/3} \right)^3 \leq \sum_i 2^{4i} |B_i|^4. \quad (30)$$

Подставляя оценку (30) в (29), получаем неравенство

$$T_2(B) \geq \frac{\alpha^4}{28\delta^3} |B|^4. \quad (31)$$

Рассмотрим теперь общий случай $k \geq 2$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 5. Докажем сначала аналог леммы 1.

ЛЕММА 2. Пусть δ, α' – действительные числа, $0 < \alpha' \leq \delta$, A – произвольное подмножество множества $\mathbb{Z}_N$ мощностью δN и $k \geq 2$ – четное число. Пусть также

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

и B' – произвольное подмножество множества $\mathcal{R}'_{\alpha'} \setminus \{0\}$. Тогда

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

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

$$\sigma = \left(\sum_x f_{B'}(x) A(x) \right)^k. \quad (33)$$

Оценивая σ снизу, как в лемме 1, находим

$$\sigma \geq ((\alpha')^2 |B'| N)^k. \quad (34)$$

Поскольку k – четное число, то оно имеет вид $k = 2k'$, $k' \in \mathbb{N}$. Применяя неравенство Гёльдера, получаем

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

Отсюда имеем

$$(\sigma')^2 = \left(\sum_x |f_{B'}(x)|^{2k'} A^2(x) \right)^2 \geq \delta^2 \frac{(\alpha')^{4k}}{\delta^{2k}} |B'|^{2k} N^2. \quad (36)$$

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

$$\begin{aligned} \sigma' &= \sum_x |f_{B'}(x)|^{2k'} A^2(x) \\ &= \frac{1}{N^{2k'+2}} \sum_x \sum_{r_1, \dots, r_{k'}, r'_1, \dots, r'_{k'}} \sum_{y, z} \hat{f}_{B'}(r_1) \dots \hat{f}_{B'}(r_{k'}) \overline{\hat{f}_{B'}(r'_1)} \dots \overline{\hat{f}_{B'}(r'_{k'})} \hat{A}(y) \overline{\hat{A}(z)} \\ &\quad \times e(x(r_1 + \dots + r_{k'} - r'_1 - \dots - r'_{k'})) e(x(y - z)) \\ &= \frac{1}{N^{2k'+1}} \sum_{u, y} \sum_{\substack{r_1, \dots, r_{k'}, r'_1, \dots, r'_{k'} \\ r_1 + \dots + r_{k'} = r'_1 + \dots + r'_{k'} - u}} \hat{f}_{B'}(r_1) \dots \hat{f}_{B'}(r_{k'}) \\ &\quad \times \overline{\hat{f}_{B'}(r'_1)} \dots \overline{\hat{f}_{B'}(r'_{k'})} \hat{A}(y) \overline{\hat{A}(y - u)} \\ &= \frac{1}{N^{2k'+1}} \sum_u \left(\sum_y \hat{A}(y) \overline{\hat{A}(y - u)} \right) \\ &\quad \times \left(\sum_{\substack{r_1, \dots, r_{k'}, r'_1, \dots, r'_{k'} \\ r_1 + \dots + r_{k'} = r'_1 + \dots + r'_{k'} - u}} \hat{f}_{B'}(r_1) \dots \hat{f}_{B'}(r_{k'}) \overline{\hat{f}_{B'}(r'_1)} \dots \overline{\hat{f}_{B'}(r'_{k'})} \right). \end{aligned} \quad (37)$$

Отсюда имеем

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

Применяя формулу (15) и равенство Парсеваля, получаем

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

Поскольку $B' \subseteq \mathcal{R}'_{\alpha'} \setminus \{0\}$, то $|\hat{f}_{B'}(r)| \leq 2\alpha' B'(r)N$. Отсюда имеем

$$\begin{aligned} \sigma_2 &\leq ((2\alpha' N)^{2k'})^2 \sum_u \left| \sum_{\substack{r_1, \dots, r_{k'}, r'_1, \dots, r'_{k'} \\ r_1 + \dots + r_{k'} = r'_1 + \dots + r'_{k'} - u}} B'(r_1) \dots B'(r_{k'}) B'(r'_1) \dots B'(r'_{k'}) \right|^2 \\ &= (2\alpha' N)^{2k} T_k(B'). \end{aligned} \quad (40)$$

Применяя равенства (38), (39) и неравенства (36), (40), находим

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

Лемма доказана.

Пусть

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

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

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

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

$$\begin{aligned} |B|^{2k} &= \left(\sum_i 2^i 2^{-i} |B_i| \right)^{2k} \leq \left(\sum_i 2^{2ki} |B_i|^{2k} \right) \left(\sum_i 2^{-2ki/(2k-1)} \right)^{2k-1} \\ &\leq \sum_i 2^{2ki} |B_i|^{2k}. \end{aligned} \quad (43)$$

Подставляя оценку (43) в (42), получаем неравенство

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

Теорема 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 размером $2^{d+1}k \times (d+1)$, в которой элементы a_{ij} определяются по формуле

$$a_{ij} = \begin{cases} 1, & \text{если в двоичном разложении } (j-1) \text{ на } (i-1)\text{-м месте стоит } 1 \\ & \text{и } 1 \leq j \leq 2^d k, \\ -1, & \text{если в двоичном разложении } (j-1) \text{ на } (i-1)\text{-м месте стоит } 1 \\ & \text{и } 2^d k < j \leq 2^{d+1} k, \\ 0 & \text{в противном случае.} \end{cases} \quad (45)$$

Напомним, 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 6. Пусть δ, α – действительные числа, $0 < \alpha \leq \delta$, A – произвольное подмножество множества $\mathbb{Z}_N$ мощностью δN , k – натуральное число, $d \geq 0$ – целое и множество $\mathcal{R}_\alpha$ определено равенством (3). Пусть $B \subseteq \mathcal{R}_\alpha \setminus \{0\}$ – произвольное множество. Рассмотрим систему уравнений

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

где элементы a_{ij} матрицы A определены формулой (45) и все $r_j \in B$. Тогда число решений системы (46) не меньше

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

Ясно, что теорема 6 является обобщением теоремы 5. Чтобы это увидеть, достаточно положить в теореме 6 число d равным нулю.

Для доказательства теоремы 6 нам понадобятся свойства норм Гауэрса (см. [18]).

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

ОПРЕДЕЛЕНИЕ 1. Пусть $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ – произвольная функция. Равномерной нормой Гауэрса (или просто нормой Гауэрса) функции f называется величина

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

Нам понадобится следующая лемма (см. [18]).

ЛЕММА 3 (неравенство монотонности для норм Гауэрса). Пусть $f : \mathbb{Z}_N \rightarrow \mathbb{C}$ – произвольная функция и d – натуральное число. Тогда

$$\|f\|_{U^d} \leq \|f\|_{U^{d+1}}. \quad (49)$$

Дальнейшие свойства норм Гауэрса могут быть найдены в [18].

Докажем следующую лемму.

ЛЕММА 4. Пусть δ, α' – действительные числа, $0 < \alpha' \leq \delta$, A – произвольное подмножество множества $\mathbb{Z}_N$ мощностью δN , k – натуральное число и $d \geq 0$ – целое. Пусть также

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

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

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

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

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

Применяя неравенство Гёльдера, находим

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

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

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

Рассмотрим сумму

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

Из соотношений (52) и (53) вытекает неравенство

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

Применяя лемму 3, находим

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

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 имеем

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

Обозначим через Σ систему уравнений

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

Тогда

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

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

Поскольку $\hat{f}_{B'}(r) = \hat{A}(r)B'(r)$ и $B' \subseteq \mathcal{R}'_{\alpha'} \setminus \{0\}$, то $|\hat{f}_{B'}(r)| \leq 2\alpha'B'(r)N$. Отсюда имеем

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

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

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

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

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

Лемма доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 6. Пусть

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

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

Пусть E – некоторое множество. Обозначим через $S_{k,d}(E)$ число решений системы уравнений (46) с $r_i \in E$. Применяя лемму 4 к каждому B_i , получаем

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

где $i \geq 1$. Отсюда имеем

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

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

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

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

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

Теорема доказана.

§ 4. Приложения к задачам комбинаторной теории чисел

В доказательстве теоремы 1 Чанг использовала теорему Рудина [19] (см. также [20]) о диссоциативных подмножествах множества $\mathbb{Z}_N$. Множество $\mathcal{D} = \{d_1, \dots, d_{|\mathcal{D}|}\} \subseteq \mathbb{Z}_N$ называется *диссоциативным*, если из сравнения

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

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

ТЕОРЕМА 7 (В. 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*

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

Доказательства теоремы 7 и теоремы Чанг могут быть также найдены в [9], [21]. Мы покажем, как из теоремы Рудина и теоремы 5 вытекает аналог теоремы 1, отличающийся от теоремы Чанг только лишь чуть более слабой оценкой мощности множества Λ .

ПРЕДЛОЖЕНИЕ 1. *Пусть δ, α – действительные числа, $0 < \alpha \leq \delta \leq 1$, A – произвольное подмножество множества $\mathbb{Z}_N$ мощностью 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*

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

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. Так как $\mathcal{D}$ – диссоциативное множество, то $0 \notin \mathcal{D}$. Применяя теорему 5, получаем оценку

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

С другой стороны,

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

где C – абсолютная константа из теоремы 7. 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 из $\mathcal{R}_\alpha$, то любой элемент r множества $\mathcal{R}_\alpha$ представляется в виде $r \equiv \sum_{i=1}^{|\mathcal{D}|} \varepsilon_i d_i \pmod{N}$, 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 доказано.

В этой статье мы докажем результат, усиливающий теорему Чанг. Наш метод доказательства и методы, используемые в работах [22]–[24], имеют много общего.

ТЕОРЕМА 8. Пусть N – натуральное число, $(N, 2) = 1$, δ, α – действительные числа, $0 < \alpha \leq \delta \leq 1/16$, A – произвольное подмножество множества $\mathbb{Z}_N$ мощностью δN и множество $\mathcal{R}_\alpha$ определено равенством (3). Тогда существует множество $\Lambda^* \subseteq \mathbb{Z}_N$,

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

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

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

где $\varepsilon_i \in \{-1, 0, 1\}$.

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

$$|\tilde{\Lambda}| \leq 2^{12}(\delta/\alpha)^2 \log(1/\delta) \log \log(1/\delta), \quad (72)$$

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

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

где $\varepsilon_i \in \{-1, 0, 1\}$.

ЗАМЕЧАНИЕ 1. В отличие от теоремы 1 в теореме 8 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 1. Пусть N – натуральное число, $(N, 6) = 1$, δ, α – действительные числа, $0 < \alpha \leq \delta \log^{1/2}(1/\delta)$ и множество $\mathcal{R}_\alpha$ определено равенством (3). Тогда существует множество $\Lambda^* \subseteq \mathbb{Z}_N$, $|\Lambda^*| \leq 2^{12}(\delta/\alpha)^2 \log(1/\delta)$, 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 $r \equiv \sum_{i=1}^M \varepsilon_i \lambda_i^* \pmod{N}$, где $\varepsilon_i \in \{-1, 0, 1\}$.

Для доказательства теоремы 8 нам понадобятся несколько вспомогательных утверждений и определений.

ОПРЕДЕЛЕНИЕ 2. 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 сравнения

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

вытекает, что все s_i равны нулю.

Определение семейства $\Lambda(k, 1)$ можно найти в статье [25].

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 оценка сверху величины T_k .

УТВЕРЖДЕНИЕ 1. Пусть k, s – натуральные числа, Λ – произвольное множество из семейства $\Lambda(k, s)$ и справедливо неравенство $|\Lambda| \geq k$. Тогда

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

ПРИМЕР 1. Пусть $\log |\Lambda| \geq \log^2 k$ и Λ – произвольное множество из семейства $\Lambda(k, 3)$. Применяя неравенство (75), получаем $T_k(\Lambda) \leq 2^{20k} k^k |\Lambda|^k$. Легко видеть, что эта оценка является неупрощаемой по порядку в том смысле, что для всякого множества Λ и для любого натурального k такого, что $\log |\Lambda| \geq \log^2 k$, всегда выполнено $T_k(\Lambda) \geq \binom{|\Lambda|}{k} (k!)^2 \gg e^{-k} k^k |\Lambda|^k$.

ДОКАЗАТЕЛЬСТВО УТВЕРЖДЕНИЯ 1. 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, что набор $s_1, \dots, s_l$ упорядочен по убыванию: $s_1 \geq s_2 \geq \dots \geq s_l \geq 1$.

Пусть $E(s_1, \dots, s_l)(x) = \{(\lambda_1, \dots, \lambda_k) : \text{среди } \lambda_1, \dots, \lambda_k \text{ существует ровно } s_1 \text{ одинаковых } \tilde{\lambda}_1, s_2 \text{ одинаковых } \tilde{\lambda}_2, \dots \text{ и } s_l \text{ одинаковых } \tilde{\lambda}_l \text{ таких, что } s_1 \tilde{\lambda}_1 + \dots + s_l \tilde{\lambda}_l = x, \text{ и все } \tilde{\lambda}_i \text{ различные}\}$. Будем обозначать для краткости множество $E(s_1, \dots, s_l)(x)$ через $E(\vec{s})(x)$. Напомним, 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 проводится по всем векторам, для которых $\sum_{i=1}^l s_i = k$. Отсюда имеем

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

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

$$l \leq k - s|B|. \quad (77)$$

Действительно,

$$k = \sum_{i \in G} s_i + \sum_{i \in B} s'_i \geq |G| + (s+1)|B| = l + s|B|. \quad (78)$$

Из неравенства (78) вытекает неравенство (77).

Докажем следующую лемму.

ЛЕММА 5. Для любого $\vec{s}$, $\sum_{i=1}^l s_i = k$, и любого $x \in \mathbb{Z}_N$ выполнено

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

ДОКАЗАТЕЛЬСТВО. 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 получаем

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

Кроме того, $\Lambda \cap (-\Lambda) = \emptyset$. Следовательно,

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

где $s'_i \in \mathbb{Z}$, $|s'_i| \leq s$, $\sum_i |s'_i| \leq 2k$ и $\lambda_i^0 \in \Lambda$ 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 $\tilde{\lambda}_2, \dots$ и 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 доказана.

Вернемся к доказательству утверждения. Оценим сумму σ . Пусть b – целое неотрицательное число, и пусть

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

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

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

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

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

Применяя лемму 5, находим $|E(\vec{s})(x)| \leq P_k(\vec{s})|\Lambda|^{|\vec{s}|}$. Отсюда и из неравенства (82) получаем

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

Рассмотрим сумму

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

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,

$$\begin{aligned} \sum_{x \in \mathbb{Z}_N} \sum_{\vec{s}: |B(\vec{s})|=b} |E(\vec{s})(x)| &\leq \binom{|\Lambda|}{k - sb} (k - sb)^k \\ &\leq \frac{|\Lambda|^{k-sb}}{(k - sb)!} (k - sb)^k \leq e^k k^{sb} |\Lambda|^{k-sb}. \end{aligned} \quad (85)$$

Отсюда и из (83) находим

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

Значит,

$$\begin{aligned} \sigma &\leq 2 \left(\left[\frac{(k-1)}{s} \right] + 1 \right)^2 e^k k^k |\Lambda|^k \sum_{b=0}^{\left[\frac{(k-1)}{s} \right]} \left(\frac{k^s}{|\Lambda|^{s-1}} \right)^b \\ &= 2 \left(\left[\frac{(k-1)}{s} \right] + 1 \right)^2 e^k k^k |\Lambda|^k \sigma^*. \end{aligned} \quad (87)$$

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

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

Утверждение доказано.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 8. Пусть $k = 2\lceil \log(1/\delta) \rceil$, $s = 2$ и $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ – максимальное подмножество множества $\mathcal{R}_\alpha \setminus \{0\}$, принадлежащее семейству $\Lambda(k, s)$. Если $\mathcal{R}_\alpha = \{0\}$, то доказательство очевидно. Если $\mathcal{R}_\alpha \setminus \{0\}$ не пусто, то и Λ не пусто. Пусть $\Lambda^* = \left(\bigcup_{j=1}^s j^{-1}\Lambda \right) \cup \{0\}$. Тогда $|\Lambda^*| \leq 4|\Lambda|$ и $0 \in \Lambda^*$. Докажем, что для любого $x \in \mathcal{R}_\alpha \setminus \{0\}$ найдется $j \in [s]$ такое, что

$$xj = \sum_{i=1}^{|\Lambda|} \lambda_i s_i, \quad s_i \in \mathbb{Z}, \quad |s_i| \leq s, \quad \sum_{i=1}^{|\Lambda|} |s_i| \leq 2k. \quad (89)$$

Поскольку 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 $\mathcal{R}_\alpha \setminus \Lambda$, $x \neq 0$. Рассмотрим все соотношения вида $\sum_{i=1}^{|\Lambda|+1} \tilde{\lambda}_i s_i = 0$, где $\tilde{\lambda}_i \in \Lambda \setminus \{x\}$ и $s_i \in \mathbb{Z}$, $|s_i| \leq s$, $\sum_{i=1}^{|\Lambda|+1} |s_i| \leq 2k$. Если все такие соотношения тривиальны, т.е. 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 семейству $\Lambda(k, s)$. Следовательно, можно считать, что $j \in [s]$. Так как $2k \leq 8 \log(1/\delta)$, то мы получаем, что для любого элемента $x \in \mathcal{R}_\alpha$ существует множество $\{\lambda_1^*, \dots, \lambda_M^*\} \subset \Lambda^*$, $M \leq 8 \log(1/\delta)$, такое, что выполнено равенство (71).

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

Если $|\Lambda| \leq k^2$, то $|\Lambda| \leq 2^4 \log^2(1/\delta)$ и, следовательно, $|\Lambda^*| \leq 2^6 \log^2(1/\delta)$. Если $|\Lambda| > k^2$, то по утверждению 1 имеем $T_k(\Lambda) \leq 2^{3k} k^k |\Lambda|^k$. С другой стороны, применяя теорему 5, получаем $T_k(\Lambda) \geq \delta \alpha^{2k} |\Lambda|^{2k} / (2^{4k} \delta^{2k})$. Отсюда $|\Lambda| \leq 2^{10}(\delta/\alpha)^2 \log(1/\delta)$ и, следовательно, $|\Lambda^*| \leq 2^{12}(\delta/\alpha)^2 \log(1/\delta)$.

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

Теперь докажем существование множества $\tilde{\Lambda}$. Пусть $s = \lceil \log \log(1/\delta) \rceil$ и Λ_1 – максимальное подмножество множества $\mathcal{R}_\alpha \setminus \{0\}$, принадлежащее семейству $\Lambda(k, s)$, $k = 2 \lceil \log(1/\delta) \rceil$. Пусть $\tilde{\Lambda} = \bigcup_{j=1}^s j^{-1} \Lambda_1$. Тогда $|\tilde{\Lambda}| \leq s |\Lambda_1|$. Применяя рассуждения, аналогичные приведенным выше, легко показать, что для любого вычета $r \in \mathcal{R}_\alpha$ существует множество $\{\tilde{\lambda}_1, \dots, \tilde{\lambda}_M\} \subset \tilde{\Lambda}$, $M \leq 8 \log(1/\delta)$ такое, что выполнено равенство (73).

Докажем неравенство (72). Если $|\Lambda_1| \leq k^{s/(s-1)}$, то $|\Lambda_1| \leq 2^{10} \log(1/\delta)$ и $|\tilde{\Lambda}| \leq s |\Lambda_1| \leq 2^{12} \log(1/\delta) \log \log(1/\delta)$. Мы видим, что в этом случае неравенство (72) доказано. Пусть теперь $|\Lambda_1| > k^{s/(s-1)}$. Применяя утверждение 1, находим $T_k(\Lambda_1) \leq 2^{3k} k^k |\Lambda_1|^k$. С другой стороны, из теоремы 5 вытекает, что $T_k(\Lambda_1) \geq \delta \alpha^{2k} |\Lambda_1|^{2k} / (2^{4k} \delta^{2k})$. Отсюда имеем $|\Lambda_1| \leq 2^{10}(\delta/\alpha)^2 \log(1/\delta)$ и, следовательно, $|\tilde{\Lambda}| \leq 2^{12}(\delta/\alpha)^2 \log(1/\delta) \log \log(1/\delta)$. Теорема доказана.

Получим теперь приложение доказанных теорем 5 и 8 к задачам комбинаторной теории чисел.

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

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

где $\| \cdot \|$ – целая часть действительного числа (о свойствах множеств Бора см. [26]). В частности, в этой статье было получено неравенство

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

При доказательстве количественного варианта теоремы Фреймана в работе [2] (см. также [9]) Чанг использовала следующее предложение.

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

Мы докажем небольшое усиление предложения 2.

ПРЕДЛОЖЕНИЕ 3. Пусть N – натуральное число, $(N, 2) = 1$, $0 < \delta \leq 2^{-256}$ – действительное число и A – произвольное подмножество множества $\mathbb{Z}_N$, $|A| = \delta N$. Тогда $2A - 2A$ содержит множество Бора $B(K, \varepsilon)$, где $|K| \leq 2^{15} \delta^{-1} \log(1/\delta)$ и $\varepsilon = 1/(2^8 \log(1/\delta))$.

Применяя формулу (90), получаем, что размер множества Бора $B(K, \varepsilon)$ в предложении 2 не меньше $(1/2) \cdot 2^{-8\delta^{-1}(\log(1/\delta))^2 N}$. В предложении 3 мощность множества Бора не меньше $(1/2) \cdot 2^{-2^{20} \delta^{-1} \log(1/\delta) \log \log(1/\delta) N}$.

Для доказательства предложения 3 нам понадобится следующее определение.

ОПРЕДЕЛЕНИЕ 3. Пусть $f, g: \mathbb{Z}_N \rightarrow \mathbb{C}$ – произвольные функции. Сверткой функций f и g назовем функцию

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

Легко видеть, что

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

ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 3. Пусть $\alpha = \delta^{3/2}/(2\sqrt{2})$. Применяя следствие 1 к $\mathcal{R}_\alpha(A)$, находим множество $\Lambda^* \subseteq \mathbb{Z}_N$, $|\Lambda^*| \leq 2^{15} \delta^{-1} \log(1/\delta)$, 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

$$|1 - e(rx)| = 2 \left| \sin\left(\frac{\pi rx}{N}\right) \right| \leq \frac{2\pi}{20} < \frac{1}{2}. \quad (93)$$

Легко видеть, что выражение $(A * A * A * A)(x)$ равно количеству 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

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

(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 $\lambda_1^*, \dots, \lambda_M^*$ из не более чем $8 \log(1/\delta)$ элементов Λ^* такой, что выполнено равенство (71), то для всех $x \in B_2$ справедливо неравенство

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

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

Список литературы

1. W. T. Gowers, “Rough structure and classification”, *Visions in mathematics—Towards 2000*, GAFA 2000. Proceedings of a meeting (Tel Aviv, Israel, August 25–September 3, 1999), Geom. Funct. Anal., Special Volume, Part I, eds. N. Alon et al., Birkhäuser, Basel, 2000, 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 sets addition*, Astérisque, **258**, eds. J.-M. Deshouillers et al., Soc. Math. France, Paris, 1999, 77–108.
5. Г. А. Фрейман, *Начала структурной теории сложения множеств*, Казан. гос. пед. инст., Казань, 1966; англ. пер.: G. A. Freiman, *Foundations of a structural theory of set addition*, Transl. Math. Monogr., **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 of Paul Erdős*, Cambridge Univ. Press, Cambridge, 1990, 105–109.
8. G. A. Freiman, H. Halberstam, I. Z. Ruzsa, “Integer sum sets containing long arithmetic progressions”, *J. London Math. Soc. II*, **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. А. А. Юдин, “О мере больших значений тригонометрических сумм”, *Теория чисел*, ред. Г. А. Фрейман, А. М. Рубинов, Е. В. Новоселов, Калининский гос. ун-т, Калинин, 1973, 163–174.
12. A. Besser, “Sets of integers with large trigonometric sums”, *Structure theory of set addition*, Astérisque, **258**, eds. J.-M. Deshouillers et al., Soc. Math. France, Paris, 1999, 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, V. F. Lev, “On the distribution of exponential sums”, *Integers*, **0** (2000), A1.
15. K. de Leeuw, Y. Katznelson, J.-P. Kahane, “Sur les coefficients de Fourier des fonctions continues”, *C. R. Acad. Sci. Paris Sér. A*, **285**:16 (1977), 1001–1003.
16. Ф. Л. Назаров, “Ударное решение задачи о коэффициентах”, *Алгебра и анализ*, **9**:2 (1997), 272–287; англ. пер.: F. L. Nazarov, “The Bang solution of the coefficient problem”, *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, 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, 83–96.
22. И. М. Виноградов, *Метод тригонометрических сумм в теории чисел*, Наука, М., 1971.
23. Yu. V. Linnik, “On Weyl’s sums”, *Матем. сб.*, **12(54)**:1 (1943), 28–39 (English).
24. Ю. В. Нестеренко, “К теореме о среднем И. М. Виноградова”, *Тр. ММО*, **48** (1985), 97–105; англ. пер.: Yu. V. Nesterenko, “On I. M. Vinogradov’s mean value theorem”, *Trans. Moscow Math. Soc.*, 1986, 105–113.
25. B. Bajnok, I. Ruzsa, “The independence number of a subset of an Abelian group”, *Integers*, **3** (2003), A02.
26. J. Bourgain, “On triples in arithmetic progression”, *Geom. Funct. Anal.*, **9**:5 (1999), 968–984.

И. Д. ШКРЕДОВ (I. D. SHKREDOV)
Московский государственный университет
им. М. В. Ломоносова,
механико-математический факультет
E-mail: ishkredov@rambler.ru

Поступило в редакцию
12.07.2006