Math-Net.Ru

Общероссийский математический портал

И. Д. Шкредов, Некоторые примеры множеств больших тригонометрических сумм, *Матем. сб.*, 2007, том 198, номер 12, 105–140

DOI: <https://doi.org/10.4213/sm3776>

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: 54.224.60.19

26 апреля 2023 г., 05:44:56

УДК 511.218+511.336

И. Д. Шкредов

Некоторые примеры множеств больших тригонометрических сумм

Пусть A – подмножество $\mathbb{Z}/N\mathbb{Z}$, и пусть R – множество больших коэффициентов Фурье множества A . Вопрос о строении R относится к обратным задачам аддитивной теории чисел. Свойства множества R изучались в работах М.-Ч. Чанг, Б. Грина и автора. Настоящая статья посвящена доказательству новых результатов о множествах больших коэффициентов Фурье. Кроме того мы приводим примеры, показывающие неулучшаемость полученных ранее теорем.

Библиография: 27 названий.

§ 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

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

где $e(x) = e^{2\pi i x/N}$.

Пусть δ, α – действительные числа, $0 < \alpha \leq \delta \leq 1$, 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

$$\mathcal{R}_\alpha = \mathcal{R}_\alpha(A) = \{r \in \mathbb{Z}_N : |\widehat{A}(r)| \geq \alpha N\}. \quad (2)$$

Для многих задач комбинаторной теории чисел важно знать структуру множества $\mathcal{R}_\alpha$ (см. [1]). Иными словами, какими нетривиальными свойствами обладает множество $\mathcal{R}_\alpha$? Ясно, что вопрос о строении $\mathcal{R}_\alpha$ относится к обратным задачам аддитивной теории чисел (см. [2]).

Пусть $\log$ означает логарифм по основанию два. В 2002 г. М.-Ч. Чанг получила следующий результат (см. [3]):

ТЕОРЕМА 1.1 (Чанг). 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 (2). Тогда найдется множество $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\} \subseteq \mathbb{Z}_N$,

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант № 06-01-00383), гранта Президента РФ (№ 1726.2006.1) и фонда INTAS (грант № 03-51-5-70).

$|\Lambda| \leq 2(\delta/\alpha)^2 \log(1/\delta)$, такое, что всякий элемент r множества $\mathcal{R}_\alpha$ представляется в виде

$$r = \sum_{i=1}^{|\Lambda|} \varepsilon_i \lambda_i \pmod{N}, \quad (3)$$

где $\varepsilon_i \in \{-1, 0, 1\}$.

Развивая подход из [4] (см. также [5]), Чанг применила свой результат при доказательстве количественного варианта знаменитой теоремы Г. А. Фреймана (см. [6]) о множествах с маленькой суммой. Другие приложения теоремы 1.1 получил Б. Грин в статье [7], а также Т. Чоен в [8]. Вопрос о структуре множества $\mathcal{R}_\alpha$, когда параметр α близок к δ , изучался в работах [9]–[11], см. также обзор [12].

Мы видим, что результаты о строении множества $\mathcal{R}_\alpha$ являются важными для комбинаторной теории чисел.

В [13] 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 $\text{Span}(E)$ множество всех сумм вида $\sum_{i=1}^{|E|} \varepsilon_i e_i$, где $\varepsilon_i \in \{-1, 0, 1\}$.

ТЕОРЕМА 1.2 (Грин). Пусть $\delta \leq 1/8$, $0 < \alpha \leq \delta/32$ – действительные числа. Пусть также

$$\left(\frac{\delta}{\alpha}\right)^2 \log \frac{1}{\delta} \leq \frac{\log N}{\log \log N}. \quad (4)$$

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

В статьях [14], [15] были получены дальнейшие результаты о множествах больших тригонометрических сумм. В частности, там была доказана следующая теорема.

ТЕОРЕМА 1.3. Пусть δ, α – действительные числа, $0 < \alpha \leq \delta$, A – произвольное подмножество $\mathbb{Z}_N$ мощности δN , $k \geq 2$ – натуральное число и множество $\mathcal{R}_\alpha$ определено равенством (2). Пусть также $B \subseteq \mathcal{R}_\alpha \setminus \{0\}$ – произвольное множество. Тогда величина

$$T_k(B) := \left| \{(r_1, \dots, r_k, r'_1, \dots, r'_k) \in B^{2k} : r_1 + \dots + r_k = r'_1 + \dots + r'_k\} \right| \quad (5)$$

не меньше, чем

$$\frac{\delta \alpha^{2k}}{2^{4k} \delta^{2k}} |B|^{2k}. \quad (6)$$

Если не обращать внимания на абсолютные константы, появляющиеся в оценках для мощности диссоциативного множества Λ , то, как было показано в работе [15], из теоремы 1.3 и неравенства В. Рудина (см. [16]) вытекает теорема Чанг. Кроме того в статье [15] было получено усиление теоремы 1.1.

ТЕОРЕМА 1.4. Пусть N – натуральное число, $(N, 2) = 1$, δ, α – действительные числа, $0 < \alpha \leq \delta \leq 1/16$, A – произвольное подмножество $\mathbb{Z}_N$ мощности δN и множество $\mathcal{R}_\alpha$ определено равенством (2). Тогда существует множество $\Lambda^* \subseteq \mathbb{Z}_N$,

$$|\Lambda^*| \leq \max \left\{ 2^{12} \left(\frac{\delta}{\alpha} \right)^2 \log \frac{1}{\delta}, 2^6 \log^2 \frac{1}{\delta} \right\}, \quad (7)$$

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

$$r = \sum_{i=1}^M \varepsilon_i \lambda_i^* \pmod{N}, \quad (8)$$

где $\varepsilon_i \in \{-1, 0, 1\}$.

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

$$|\tilde{\Lambda}| \leq 2^{12} \left(\frac{\delta}{\alpha} \right)^2 \log \frac{1}{\delta} \log \log \frac{1}{\delta}, \quad (9)$$

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

$$r = \sum_{i=1}^M \varepsilon_i \tilde{\lambda}_i \pmod{N}, \quad (10)$$

где $\varepsilon_i \in \{-1, 0, 1\}$.

Скажем несколько слов о содержании настоящей статьи.

В §2 мы покажем, что для достаточно широкой области параметров α, δ и k теорема 1.3 является неулучшаемой. В нашем доказательстве мы строим конкретные множества $A \subseteq \mathbb{Z}_N$, у которых $\mathcal{R}_\alpha(A)$ имеет нужные нам свойства. Кроме того в этом параграфе мы получим результат, в некотором смысле противоположный теореме Чанг (см. теорему 2.8).

Параграф 3 посвящен доказательству усиления теоремы 1.4 (мы рассматриваем ситуацию, когда число N из теоремы 1.4 простое).

ТЕОРЕМА 1.5. Пусть N – простое число, δ, α – действительные числа, $0 < \alpha \leq \delta \leq 2^{-8}$, A – произвольное подмножество $\mathbb{Z}_N$ мощности δN , множество $\mathcal{R}_\alpha$ определено равенством (2) и d – натуральное число. Тогда существует множество $\Lambda^* \subseteq \mathbb{Z}_N$,

$$|\Lambda^*| \leq \max \left\{ 2^{12+4d(\log(1/\delta))^{-1}} \left(\frac{\delta}{\alpha} \right)^2 \log \frac{1}{\delta}, 8 \log^2 \frac{1}{\delta} \right\}, \quad (11)$$

такое, что для любого вычета $r \in \mathcal{R}_\alpha \setminus \{0\}$ существует матрица

$$M = (m_{ij})_{i \in [d], j \in [|\Lambda^*|]}$$

ранга d такая, что для любого $i \in [d]$ выполнено $\sum_{j=1}^{|\Lambda^*|} |m_{ij}| \leq 4 \log(1/\delta)$ и для всех $i \in [d]$ справедливо равенство

$$r = \sum_{j=1}^{|\Lambda^*|} m_{ij} \lambda_j^* \pmod{N}. \quad (12)$$

Кроме того, существует множество $\tilde{\Lambda} \subseteq \mathbb{Z}_N$,

$$|\tilde{\Lambda}| \leq \max \left\{ 2^5 \log \frac{1}{\delta} \log \log \frac{1}{\delta}, \right. \\ \left. 2^{10+2d \log(2 \log \log(1/\delta))(\log(1/\delta))^{-1}} \left(\frac{\delta}{\alpha} \right)^2 \log \frac{1}{\delta} \log \log \frac{1}{\delta} \right\}, \quad (13)$$

такое, что для любого вычета $r \in \mathcal{R}_\alpha \setminus \{0\}$ существует матрица

$$\tilde{M} = (\tilde{m}_{ij})_{i \in [d], j \in [\tilde{\Lambda}]}$$

ранга d такая, что для любого $i \in [d]$ выполнено $\sum_{j=1}^{|\tilde{\Lambda}|} |\tilde{m}_{ij}| \leq 4 \log(1/\delta)$ и для всех $i \in [d]$ справедливо равенство

$$r = \sum_{j=1}^{|\tilde{\Lambda}|} \tilde{m}_{ij} \tilde{\lambda}_j \pmod{N}. \quad (14)$$

Вопрос о строении множеств больших тригонометрических сумм, так же как и любой другой вопрос комбинаторной теории чисел, может быть поставлен для произвольной конечной абелевой группы G , а не только для $\mathbb{Z}_N$. При этом в одних группах G ответить на поставленный вопрос легко, а в других – трудно. Недавно выяснилось (см. [17], [18] и, особенно, замечательный обзор [19]), что чрезвычайно удобно брать в качестве группы G группы $\mathbb{Z}_p^n$, где p – маленькое простое число (например, $p = 2, 3$ или 5). Дело в том, что на таких группах имеется естественная структура векторного пространства и при этом сами группы $\mathbb{Z}_p^n$ не слишком сложно устроены. Более того, общая идеология статьи [19] состоит в следующем: если некоторый результат комбинаторной теории чисел доказан для групп $\mathbb{Z}_p^n$, то, как правило, соответствующий результат может быть доказан и для произвольной конечной абелевой группы, причем без привлечения какой-то принципиально новой идеи.

В § 4 мы получим несколько результатов, аналогичных результатам § 2, для групп $\mathbb{Z}_p^n$. Все технические детали при этом существенно упрощаются, а основные идеи доказательств теорем из § 2 становятся гораздо прозрачнее.

Заметим, наконец, что теоремы 1.1, 1.4 и 1.5 тривиальны в случае, когда параметр δ не стремится к нулю при $N \rightarrow \infty$. В этой ситуации структура множества $\mathcal{R}_\alpha$ может быть произвольной (см. работы [20]–[22]).

Автор выражает глубокую благодарность С. В. Конягину за его идею, позволившую усилить формулировку одного из результатов, а также Н. Г. Мощевитину за постоянное внимание к работе.

§ 2. Примеры множеств больших тригонометрических сумм

Пусть N – натуральное число. Обозначим для удобства через $[N]$ отрезок натурального ряда $[N] = \{1, 2, \dots, N\}$. Пусть также $f: \mathbb{Z}_N \rightarrow \mathbb{C}$ – произвольная функция. Для коэффициентов Фурье функции f справедливо равенство Парсеваля

$$\sum_{r \in \mathbb{Z}_N} |\hat{f}(r)|^2 = N \sum_{n \in \mathbb{Z}_N} |f(n)|^2. \quad (15)$$

Пусть δ, α – действительные числа, $0 < \alpha \leq \delta \leq 1$, и пусть A – некоторое подмножество $\mathbb{Z}_N$ мощности δN . Отметим простейшие свойства множества $\mathcal{R}_\alpha(A)$. Из равенства Парсеваля (15) вытекает верхняя оценка для мощности множества больших тригонометрических сумм $\mathcal{R}_\alpha(A)$, а именно $|\mathcal{R}_\alpha(A)| \leq \delta/\alpha^2$. Кроме того, из определения $\mathcal{R}_\alpha$ следует, 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 $-r \in \mathcal{R}_\alpha$.

В этом параграфе мы приведем несколько примеров множеств больших тригонометрических сумм. Заметим сразу, что произвольное “маленькое” подмножество $\mathbb{Z}_N$ является множеством больших тригонометрических сумм, а точнее справедливо следующее предложение.

ПРЕДЛОЖЕНИЕ 2.1. Пусть $\delta, \alpha \in (0, 1]$ – действительные числа, $\delta \leq 1/2$, $20N^{-1/2} < \alpha \leq \delta/2$, и $S \subseteq \mathbb{Z}_N$ – произвольное множество такое, что $0 \in S$, $S = -S$ и $|S| \leq \delta/(2\alpha)$. Тогда найдется множество $A \subseteq \mathbb{Z}_N$, $|A| = [\delta N]$, такое, что $\mathcal{R}_\alpha(A) = S$.

Всюду ниже мы не будем специально оговаривать, что равенство двух элементов из $\mathbb{Z}_N$ понимается в смысле равенства по модулю N .

Для доказательства предложения 2.1 нам потребуется следующая хорошо известная лемма (см. [13] и [23]).

ЛЕММА 2.2. Пусть $f: \mathbb{Z}_N \rightarrow [0, 1]$ – произвольная функция. Тогда найдется множество $C \subseteq \mathbb{Z}_N$ с $|C| = [\sum_{x \in \mathbb{Z}_N} f(x)]$ такое, что для всех $r \in \mathbb{Z}_N \setminus \{0\}$ выполнено $|\hat{C}(r) - \hat{f}(r)| \leq 20\sqrt{N}$.

ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 2.1. Пусть $S^* = S \setminus \{0\}$. Рассмотрим функцию $f(x) = \delta + 2\alpha \sum_{r \in S^*} e(rx)$. Так как $S = -S$, то $f(x)$ – вещественная функция. По условию $|S| \leq \delta/(2\alpha)$ и $\delta \leq 1/2$. Отсюда для всех $x \in \mathbb{Z}_N$ выполнено $0 \leq f(x) \leq 1$. Кроме того, $\sum_{x \in \mathbb{Z}_N} f(x) = \delta N$ и для всех $r \in \mathbb{Z}_N \setminus \{0\}$ имеем $\hat{f}(r) = 2\alpha S^*(r)N$. Применяя лемму 2.2, находим множество A такое, что $|A| = [\sum_{x \in \mathbb{Z}_N} f(x)] = [\delta N]$ и для любого $r \in \mathbb{Z}_N \setminus \{0\}$ выполнено

$$|\hat{A}(r) - \hat{f}(r)| = |\hat{A}(r) - 2\alpha S^*(r)N| \leq 20\sqrt{N}.$$

Так как $\alpha > 20N^{-1/2}$, то для всех $r \in S^*$ справедливо неравенство

$$|\hat{A}(r)| \geq 2\alpha N - 20\sqrt{N} \geq \alpha N.$$

Таким образом, $S \subseteq \mathcal{R}_\alpha(A)$. Снова применяя неравенство $\alpha > 20N^{-1/2}$, получаем, что для всех $r \notin S^*$, $r \neq 0$, выполнено $|\hat{A}(r)| < \alpha N$. Следовательно, $\mathcal{R}_\alpha(A) = S$. Предложение доказано.

Итак, любое подмножество $\mathbb{Z}_N$ маленькой мощности, симметричное относительно нуля и содержащее нуль, является множеством больших тригонометрических сумм. Что можно сказать о структуре множеств, мощность которых близка к числу δ/α^2 – верхней границе для мощности множества больших тригонометрических сумм, вытекающей из равенства Парсеваля? Эта проблема еще далека от своего разрешения. Ясно, что не всякое множество R , $|R| \leq \delta/\alpha^2$, может быть множеством больших тригонометрических сумм. Например, как показывает теорема 1.3, множества $\mathcal{R}_\alpha$ обладают большой величиной T_k .

Теорема Чанг является другим примером, говорящим о том, что интересующие нас множества имеют весьма специфические свойства. Смысл этой теоремы заключается в следующем: любое множество больших тригонометрических сумм обладает небольшим диссоциативным подмножеством. Множество $\mathcal{D} = \{d_1, \dots, d_{|\mathcal{D}|}\} \subseteq \mathbb{Z}_N$ называется *диссоциативным*, если из равенства

$$\sum_{i=1}^{|\mathcal{D}|} \varepsilon_i d_i = 0 \pmod{N}, \quad (16)$$

где $\varepsilon_i \in \{-1, 0, 1\}$, вытекает, что все ε_i равны нулю. В своей теореме Чанг фактически доказала, что любое диссоциативное подмножество $\mathcal{R}_\alpha(A)$ имеет мощность, не превосходящую $2(\delta/\alpha)^2 \log(1/\delta)$. Если теперь взять в теореме 1.1 в качестве Λ максимальное диссоциативное подмножество $\mathcal{R}_\alpha(A)$, то легко видеть, что для любого элемента $r \in \mathcal{R}_\alpha(A)$ будет справедливо равенство (3) (более подробно см. [3] или [24]).

В этом параграфе мы получим результат, в некотором смысле противоположный теореме Чанг. Мы покажем, что любое не очень большое диссоциативное подмножество $\mathbb{Z}_N$ является множеством больших тригонометрических сумм. В своем доказательстве мы интенсивно используем подход Грина (см. [13]), связанный с “множествами уровня” И. Ружи (см. [25]).

Нам потребуется одно обобщение понятия диссоциативности. Множество $\mathcal{D} \subseteq \mathbb{Z}_N$ называется *k-диссоциативным*, если из равенства (16), где $|\varepsilon_i| \leq k$, вытекает, что все ε_i равны нулю. Пользуясь этим определением, мы можем переформулировать теорему 1.2.

ТЕОРЕМА 2.3 (Грин). Пусть $\delta \leq 1/8$, $20N^{-1/2} < \alpha \leq \delta/32$ – действительные числа и Λ – произвольное множество, $|\Lambda| \leq 2^{-11}(\delta/\alpha)^2 \log(1/\delta)$, являющееся $6|\Lambda|$ -диссоциативным. Тогда найдется множество $A \subseteq \mathbb{Z}_N$, $|A| = \lfloor \delta N \rfloor$, такое, что $\mathcal{R}_\alpha(A) = \{0\} \sqcup \Lambda \sqcup -\Lambda$.

ЗАМЕЧАНИЕ 2.4. Если множество Λ является $6|\Lambda|$ -диссоциативным, то для мощности Λ справедливо неравенство $|\Lambda| \ll \log N / \log \log N$. Таким образом, теорема 2.3 не работает для множеств, мощность которых по порядку больше, чем $\log N / \log \log N$.

Мы не будем подробно останавливаться на доказательстве теоремы 2.3, а докажем чуть более сильный результат. Чтобы его сформулировать, нам потребуется следующее определение (см. [26] и [14], [15]).

ОПРЕДЕЛЕНИЕ 2.5. 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

$$\sum_{i=1}^{|\Lambda|} \lambda_i s_i = 0 \pmod{N}, \quad \lambda_i \in \Lambda, \quad s_i \in \mathbb{Z}, \quad |s_i| \leq s, \quad \sum_{i=1}^{|\Lambda|} |s_i| \leq k, \quad (17)$$

вытекает, что все s_i равны нулю. Будем обозначать *символом* $\Lambda(k, \infty)$ семейство множеств $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ обладающих тем свойством, что из равенства

$$\sum_{i=1}^{|\Lambda|} \lambda_i s_i = 0 \pmod{N}, \quad \lambda_i \in \Lambda, \quad s_i \in \mathbb{Z}, \quad \sum_{i=1}^{|\Lambda|} |s_i| \leq k, \quad (18)$$

вытекает, что все s_i равны нулю.

Заметим, что для всех $\Lambda \in \Lambda(k, s)$, где s может быть равно и бесконечности, выполнено $0 \notin \Lambda$ и $\Lambda \cap -\Lambda = \emptyset$.

Нам понадобится еще одно более тонкое определение диссоциативности.

ОПРЕДЕЛЕНИЕ 2.6. Пусть k, p – натуральные числа, а s – натуральное число или символ бесконечности. Рассмотрим *семейство множеств* $\Lambda(k, s, p)$ из $\mathbb{Z}_N$, обладающих следующим свойством. Если множество $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ принадлежит семейству $\Lambda(k, s, p)$, то существует разбиение множества Λ на p множеств

$$\Lambda_1 = \{\lambda_1^{(1)}, \dots, \lambda_{|\Lambda_1|}^{(1)}\}, \quad \dots, \quad \Lambda_p = \{\lambda_1^{(p)}, \dots, \lambda_{|\Lambda_p|}^{(p)}\},$$

причем мощности любых двух множеств Λ_i, Λ_j отличаются не более чем в два раза и, кроме того, из равенства

$$\sum_{i=1}^{|\Lambda_1|} \lambda_i^{(1)} s_i^{(1)} + \dots + \sum_{i=1}^{|\Lambda_p|} \lambda_i^{(p)} s_i^{(p)} = 0 \pmod{N}, \quad (19)$$

где

$$\lambda_j^{(i)} \in \Lambda_i, \quad s_j^{(i)} \in \mathbb{Z}, \quad |s_j^{(i)}| \leq s, \quad \sum_{j=1}^{|\Lambda_i|} |s_j^{(i)}| \leq k, \quad i = 1, \dots, p, \quad (20)$$

вытекает, что все $s_j^{(i)}, i = 1, \dots, p, j = 1, \dots, |\Lambda_i|$, равны нулю.

ПРИМЕР 2.7. Пусть k, s, p – натуральные числа. Тогда любое множество $\Lambda \in \Lambda(kp, s)$, мощности не меньшей p , принадлежит семейству $\Lambda(k, s, p)$.

ТЕОРЕМА 2.8. Пусть δ, α – действительные числа, $\delta \leq 1/8, 640N^{-1/2} < \alpha \leq 2^{-27}\delta$ и Λ – произвольное множество, $|\Lambda| \leq 2^{-12}(\delta/\alpha)^2 \log(1/\delta)$, принадлежащее семейству $\Lambda((\delta/\alpha)^2, (\delta/\alpha)^2, [\log(1/\delta)])$. Тогда найдется множество $A \subseteq \mathbb{Z}_N, |A| = [\delta N]$, такое, что $\mathcal{R}_\alpha(A) = \{0\} \sqcup \Lambda \sqcup -\Lambda$.

Прежде чем доказывать теорему 2.8, мы установим один вспомогательный результат.

ПРЕДЛОЖЕНИЕ 2.9. Пусть $\delta, \alpha \in (0, 1]$ – действительные числа такие, что $640N^{-1/2} < \alpha \leq 2^{-10}\delta$, и Λ – произвольное 2-диссоциативное множество, мощность которого не превосходит $(\delta/(3\alpha)) \log(1/\delta)$. Тогда найдется множество $A \subseteq \mathbb{Z}_N$, $|A| = [\delta N]$, такое, что $\mathcal{R}_\alpha(A) = \{0\} \sqcup \Lambda \sqcup -\Lambda$.

Предложение 2.9 говорит о том, что любое 2-диссоциативное множество, мощности чуть большей, чем величина $\delta/(2\alpha)$ (мощность, которая получается в предложении 2.1), является множеством больших тригонометрических сумм.

ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 2.9. Пусть $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ произвольное 2-диссоциативное множество, мощность которого не превосходит величину $(\delta/(3\alpha)) \log(1/\delta)$. Пусть также $m = |\Lambda|$ и $c = (3 \ln 2)/2$. Рассмотрим функцию

$$f(x) = \delta \prod_{j=1}^m \left(1 + \frac{2c\alpha}{\delta} \cos(\lambda_j x)\right) = \delta \prod_{j=1}^m \left(1 + \frac{c\alpha}{\delta} (e(\lambda_j x) + e(-\lambda_j x))\right). \quad (21)$$

Ясно, что $f(x) \geq 0$ и $\sum_{x \in \mathbb{Z}_N} f(x) = \delta N$. По условию $m \leq (\delta/(3\alpha)) \log(1/\delta)$. Отсюда $f(x) \leq \delta(1 + 2c\alpha/\delta)^m \leq 1$. Пусть

$$\nu_d(n) = |\{r_1, \dots, r_d \in \Lambda : n = \pm r_1 \pm \dots \pm r_d\}|, \quad d = 1, \dots, m,$$

– количество представлений вычета n в виде суммы элементов Λ с коэффициентами, равными плюс или минус единица. В частности,

$$\nu_2(n) = |\{r_1, r_2 \in \Lambda : n = \pm r_1 \pm r_2\}|, \quad \nu_1(n) = |\{r_1 \in \Lambda : n = \pm r_1\}|.$$

Раскрывая произведение Рисса (21), находим

$$\begin{aligned} f(x) &= \delta + \delta \frac{c\alpha}{\delta} \sum_n \nu_1(n) e(nx) + \delta \left(\frac{c\alpha}{\delta}\right)^2 \sum_n \nu_2(n) e(nx) \\ &\quad + \dots + \delta \left(\frac{c\alpha}{\delta}\right)^m \sum_n \nu_m(n) e(nx). \end{aligned} \quad (22)$$

Иными словами,

$$f(x) = \delta + c\alpha \widehat{\nu}_1(-x) + \delta \left(\frac{c\alpha}{\delta}\right)^2 \widehat{\nu}_2(-x) + \dots + \delta \left(\frac{c\alpha}{\delta}\right)^m \widehat{\nu}_m(-x). \quad (23)$$

Отсюда

$$\widehat{f}(r) = \begin{cases} \delta N, & r = 0; \\ N \left(c\alpha \nu_1(r) + \delta \left(\frac{c\alpha}{\delta}\right)^2 \nu_2(r) + \dots + \delta \left(\frac{c\alpha}{\delta}\right)^m \nu_m(r) \right), & r \neq 0. \end{cases}$$

Легко видеть, что для всех $i \geq 1$ выполнено $\nu_i(n) \leq 1$. Действительно, из вида произведения Рисса (21) вытекает, что в представлении n любой элемент $\lambda \in \Lambda \sqcup -\Lambda$ не может встречаться более одного раза. Кроме того, в представлении n не могут одновременно встречаться вычеты λ и $-\lambda$, где $\lambda \in \Lambda$. Используя

этот факт и 2-диссоциативность множества Λ , получаем, что для всех n и всех $i \geq 1$ выполнено $\nu_i(n) \leq 1$. Если $r \in \Lambda$ или $r \in -\Lambda$, то

$$|\widehat{f}(r)| \geq c\alpha N - N \left(\delta \left(\frac{c\alpha}{\delta} \right)^2 + \delta \left(\frac{c\alpha}{\delta} \right)^3 + \cdots + \delta \left(\frac{c\alpha}{\delta} \right)^m \right) \geq (1 + 2^{-5})\alpha N. \quad (24)$$

Аналогично, если $r \notin \Lambda \sqcup -\Lambda$, то

$$|\widehat{f}(r)| \leq N \left(\delta \left(\frac{c\alpha}{\delta} \right)^2 + \delta \left(\frac{c\alpha}{\delta} \right)^3 + \cdots + \delta \left(\frac{c\alpha}{\delta} \right)^m \right) \leq \frac{1}{2}\alpha N. \quad (25)$$

Применяя лемму 2.2, находим множество A такое, что

$$|A| = \left[\sum_{x \in \mathbb{Z}_N} f(x) \right] = [\delta N]$$

и для всех $r \in \mathbb{Z}_N \setminus \{0\}$ выполнено $|\widehat{A}(r) - \widehat{f}(r)| \leq 20\sqrt{N}$. Из неравенств (24), (25) и неравенства $\alpha > 640N^{-1/2}$ вытекает, что $\mathcal{R}_\alpha(A) = \{0\} \sqcup \Lambda \sqcup -\Lambda$. Предложение 2.9 доказано.

Вернемся к доказательству теоремы 2.8.

Нам понадобится одна лемма из [13].

ЛЕММА 2.10. Пусть k – натуральное число и

$$p_k(x) = 2 + x \sum_{j=0}^k \frac{(-1)^j x^{2j}}{2^{4j} j!}. \quad (26)$$

Тогда для всех x таких, что $|x| \leq \sqrt{k}$, выполнено $0 \leq p_k(x) \leq 4$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2.8. Пусть $k = s = (\delta/\alpha)^2$, $p = [\log(1/\delta)]$. Пусть также $k_i = |\Lambda_i|$ и $\Lambda_i = \{\lambda_1^{(i)}, \dots, \lambda_{k_i}^{(i)}\}$, $i = 1, 2, \dots, p$. Из определения семейства $\Lambda(k, k, p)$ вытекает неравенство

$$\frac{|\Lambda|}{2p} \leq k_i \leq \frac{2|\Lambda|}{p}. \quad (27)$$

Заметим, что можно предполагать справедливость неравенства

$$|\Lambda| > \frac{\delta}{3\alpha} \log \frac{1}{\delta} > 2 \log \frac{1}{\delta}. \quad (28)$$

Действительно, если $|\Lambda| \leq (\delta/(3\alpha)) \log(1/\delta)$, то для всех $i \in [p]$ выполнено $2k_i + 1 \leq 8\delta/\alpha \leq k$. Кроме того $s \geq 2$. Следовательно, в этом случае множество Λ является 2-диссоциативным и существование множества A с требуемыми свойствами легко вытекает из предложения 2.9.

Пусть

$$g(x) = 4^{-p} \prod_{i=1}^p p_{k_i} \left(\frac{\cos(2\pi \lambda_1^{(i)} x/N) + \cdots + \cos(2\pi \lambda_{k_i}^{(i)} x/N)}{\sqrt{k_i}} \right). \quad (29)$$

Из леммы 2.10 вытекает, что для любого x из $\mathbb{Z}_N$ выполнено $0 \leq g(x) \leq 1$. Рассмотрим i -й член произведения (29). Пользуясь формулой $\cos(2\pi x/N) = (e(x) + e(-x))/2$, получаем

$$\begin{aligned} p_{k_i} & \left(\frac{\cos(2\pi\lambda_1^{(i)} x/N) + \dots + \cos(2\pi\lambda_{k_i}^{(i)} x/N)}{\sqrt{k_i}} \right) \\ & = 2 + \frac{1}{2\sqrt{k_i}} \sum_{j=0}^{k_i} \frac{(-1)^j}{(64k_i)^j j!} (e(\lambda_1^{(i)} x) + e(-\lambda_1^{(i)} x) + \dots + e(\lambda_{k_i}^{(i)} x) + e(-\lambda_{k_i}^{(i)} x))^{2j+1}. \end{aligned} \quad (30)$$

Перемножая все члены (30), находим

$$\begin{aligned} g(x) & = \sum_{\sum_{l=1}^{k_1} |s_l^{(1)}| \leq 2k_1+1} \dots \sum_{\sum_{l=1}^{k_p} |s_l^{(p)}| \leq 2k_p+1} Q(s_1^{(1)}, \dots, s_{k_1}^{(1)}, \dots, s_1^{(p)}, \dots, s_{k_p}^{(p)}) \\ & \quad \times e((s_1^{(1)}\lambda_1^{(1)} + \dots + s_{k_1}^{(1)}\lambda_{k_1}^{(1)} + \dots + s_1^{(p)}\lambda_1^{(p)} + \dots + s_{k_p}^{(p)}\lambda_{k_p}^{(p)})x), \end{aligned} \quad (31)$$

где $Q(s_1^{(1)}, \dots, s_{k_1}^{(1)}, \dots, s_1^{(p)}, \dots, s_{k_p}^{(p)})$ – некоторые действительные числа, стоящие перед $e((s_1^{(1)}\lambda_1^{(1)} + \dots + s_{k_1}^{(1)}\lambda_{k_1}^{(1)} + \dots + s_1^{(p)}\lambda_1^{(p)} + \dots + s_{k_p}^{(p)}\lambda_{k_p}^{(p)})x)$. Записывая i -й член произведения (29) в виде, аналогичном (31), получаем

$$\begin{aligned} p_{k_i} & \left(\frac{\cos(2\pi\lambda_1^{(i)} x/N) + \dots + \cos(2\pi\lambda_{k_i}^{(i)} x/N)}{\sqrt{k_i}} \right) \\ & = \sum_{\sum_{l=1}^{k_i} |s_l^{(i)}| \leq 2k_i+1} Q(s_1^{(i)}, \dots, s_{k_i}^{(i)}) e((s_1^{(i)}\lambda_1^{(i)} + \dots + s_{k_i}^{(i)}\lambda_{k_i}^{(i)})x). \end{aligned} \quad (32)$$

Ясно, что

$$Q(s_1^{(1)}, \dots, s_{k_1}^{(1)}, \dots, s_1^{(p)}, \dots, s_{k_p}^{(p)}) = 4^{-p} \prod_{i=1}^p Q(s_1^{(i)}, \dots, s_{k_i}^{(i)}).$$

Заметим, что из определения семейства $\Lambda(k, k, p)$ вытекает, что все числа $s_1^{(1)}\lambda_1^{(1)} + \dots + s_{k_1}^{(1)}\lambda_{k_1}^{(1)} + \dots + s_1^{(p)}\lambda_1^{(p)} + \dots + s_{k_p}^{(p)}\lambda_{k_p}^{(p)}$ различные. Отсюда, в частности, следует, что

$$\sum_{x \in \mathbb{Z}_N} g(x) = 2^{-p} N. \quad (33)$$

Из формулы (31) вытекает, что r -й коэффициент Фурье функции $g(x)$, не имеющий вида $s_1^{(1)}\lambda_1^{(1)} + \dots + s_{k_1}^{(1)}\lambda_{k_1}^{(1)} + \dots + s_1^{(p)}\lambda_1^{(p)} + \dots + s_{k_p}^{(p)}\lambda_{k_p}^{(p)}$, где

$$\sum_{l=1}^{k_i} |s_l^{(i)}| \leq 2k_i + 1, \quad i \in [p],$$

равен нулю. Напротив, r -й коэффициент Фурье $g(x)$ вида $s_1^{(1)}\lambda_1^{(1)} + \dots + s_{k_1}^{(1)}\lambda_{k_1}^{(1)} + \dots + s_1^{(p)}\lambda_1^{(p)} + \dots + s_{k_p}^{(p)}\lambda_{k_p}^{(p)}$ равен $NQ(s_1^{(1)}, \dots, s_{k_1}^{(1)}, \dots, s_1^{(p)}, \dots, s_{k_p}^{(p)})$. Докажем, что для всех $i \in [p]$, $j \in [k_i]$ выполнено

$$|\widehat{g}(\lambda_j^{(i)})| = |\widehat{g}(-\lambda_j^{(i)})| \geq 2^{-p} \frac{N}{8\sqrt{k_i}}. \quad (34)$$

Ясно, что достаточно доказать формулу (34) для $i = j = 1$. Другими словами, нам необходимо найти коэффициент $Q(1, 0, \dots, 0)$. Пользуясь определением семейства $\Lambda(k, k, p)$, легко видеть, что для вычисления $Q(1, 0, \dots, 0)$ необходимо взять двойки из разложения (30) многочленов $p_{k_i}(x)$, $i \geq 2$. Имеем

$$\begin{aligned} & p_{k_1} \left(\frac{\cos(2\pi\lambda_1^{(1)}x/N) + \dots + \cos(2\pi\lambda_{k_1}^{(1)}x/N)}{\sqrt{k_1}} \right) \\ &= 2 + \frac{1}{2\sqrt{k_1}} \sum_{j=0}^{k_1} \frac{(-1)^j}{(64k_1)^j j!} (e(\lambda_1^{(1)}x) + e(-\lambda_1^{(1)}x) + \dots \\ & \quad + e(\lambda_{k_1}^{(1)}x) + e(-\lambda_{k_1}^{(1)}x))^{2j+1} \\ &= \sum_{\sum_{i=1}^{k_1} |s_i^{(1)}| \leq 2k_1+1} Q(s_1^{(1)}, \dots, s_{k_1}^{(1)}) e((s_1^{(1)}\lambda_1^{(1)} + \dots + s_{k_1}^{(1)}\lambda_{k_1}^{(1)})x). \end{aligned} \quad (35)$$

Коэффициент перед $e(\lambda_1^{(1)}x)$ в формуле (35) при $j = 0$ равен $1/(2\sqrt{k_1})$. Докажем, что сумма коэффициентов перед $e(\lambda_1^{(1)}x)$ при $j \geq 1$ меньше, чем $1/(4\sqrt{k_1})$.

Пусть $l = 1, 2, \dots, k_1$ и рассмотрим произведение $(2l + 1)$ скобки

$$(e(\lambda_1^{(1)}x) + e(-\lambda_1^{(1)}x) + \dots + e(\lambda_{k_1}^{(1)}x) + e(-\lambda_{k_1}^{(1)}x))^{2l+1}$$

в формуле (35). Слагаемое $e(\lambda_1^{(1)}x)$ при раскрытии скобок в этом произведении получается следующим способом. Во-первых, мы выбираем член $e(\lambda_1^{(1)}x)$ в одной из скобок. Это можно сделать $(2l + 1)$ способом. Во-вторых, мы выбираем член $e(\lambda_u^{(1)}x)$ с некоторым u из первой среди еще не выбранных скобок. Это можно сделать $2k_1$ способами. Ясно, что необходимо компенсировать член $e(\lambda_u^{(1)}x)$ членом $e(-\lambda_u^{(1)}x)$, выбрав последний из какой-то другой скобки. А это можно сделать $(2l - 1)$ способом. И так далее. Таким образом, коэффициент перед $e(\lambda_1^{(1)}x)$ при $j = l$ не превосходит

$$\frac{1}{2\sqrt{k_1}} \cdot \frac{1}{(64k_1)^l l!} \cdot (2l + 1) \cdot 2k_1 \cdot (2l - 1) \cdot 2k_1 \cdot (2l - 3) \cdot 2k_1 \cdot 1 \leq \frac{1}{2\sqrt{k_1}} \cdot \frac{2l + 1}{2^{4l}}.$$

Следовательно,

$$\begin{aligned} \frac{1}{4\sqrt{k_1}} &\leq \frac{1}{2\sqrt{k_1}} \left(1 - \sum_{j=1}^{\infty} \frac{2j+1}{2^{4j}} \right) \leq Q(1, 0, \dots, 0) \\ &\leq \frac{1}{2\sqrt{k_1}} \left(1 + \sum_{j=1}^{\infty} \frac{2j+1}{2^{4j}} \right) \leq \frac{1}{\sqrt{k_1}} \end{aligned} \quad (36)$$

и неравенство (34) доказано. Чуть более тонкий расчет показывает, что

$$Q(1, 0, \dots, 0) \leq \frac{1}{2\sqrt{k_1}}. \quad (37)$$

Действительно, член при $j = 1$ в формуле (35) берется со знаком минус и его абсолютная величина равна

$$\frac{1}{2\sqrt{k_1}} \cdot \frac{1}{64k_1} (3(2k_1 - 2) + 3) \geq \frac{1}{2\sqrt{k_1}} \cdot \frac{1}{16}.$$

Следовательно,

$$Q(1, 0, \dots, 0) \leq \frac{1}{2\sqrt{k_1}} \left(1 - \frac{1}{16} + \sum_{j=2}^{\infty} \frac{2j+1}{2^{4j}} \right) \leq \frac{1}{2\sqrt{k_1}}$$

и неравенство (37) доказано.

Легко видеть, что существует $\gamma \in [1/2, 1]$ такое, что функция $f(x) = \gamma g(x)$ обладает свойством $\sum_x f(x) = \delta N$. Имеем $|\Lambda| \leq 2^{-12}(\delta/\alpha)^2 \log(1/\delta)$. Так как $f = \gamma g$, то для любого $i \in [p]$ и любого $j \in [k_i]$ выполнено

$$|\widehat{f}(\lambda_j^{(i)})| = |\widehat{f}(-\lambda_j^{(i)})| \geq 2\alpha N \quad (38)$$

(при выводе последнего неравенства мы воспользовались (27) и (34)). Применяя лемму 2.2, находим множество A такое, что $|A| = [\sum_{x \in \mathbb{Z}_N} f(x)] = [\delta N]$ и для всех $r \in \mathbb{Z}_N \setminus \{0\}$ выполнено

$$|\widehat{A}(r) - \widehat{f}(r)| \leq 20\sqrt{N}. \quad (39)$$

Из неравенства (38) и неравенства $\alpha > 40N^{-1/2}$ вытекает, что

$$\{0\} \sqcup \Lambda \sqcup -\Lambda \subseteq \mathcal{R}_\alpha(A).$$

Докажем обратное включение. Пусть $r \notin \{0\} \sqcup \Lambda \sqcup -\Lambda$. Покажем, что тогда $r \notin \mathcal{R}_\alpha(A)$. Как мы уже отмечали ранее, достаточно рассматривать только те вычеты r , которые можно представить в виде $r = s_1^{(1)}\lambda_1^{(1)} + \dots + s_{k_1}^{(1)}\lambda_{k_1}^{(1)} + \dots + s_1^{(p)}\lambda_1^{(p)} + \dots + s_{k_p}^{(p)}\lambda_{k_p}^{(p)}$, где для любого $i \in [p]$ выполнено $\sum_{l=1}^{k_i} |s_l^{(i)}| \leq 2k_i + 1$. Так как $r \notin \{0\} \sqcup \Lambda \sqcup -\Lambda$, то $\sum_{i=1}^p \sum_{l=1}^{k_i} |s_l^{(i)}| \geq 2$. Пусть $\sigma_i = \sum_{l=1}^{k_i} |s_l^{(i)}|$. Тогда $\sum_{i=1}^p \sigma_i \geq 2$ и либо существует $i \in [p]$ такое, что $\sigma_i \geq 2$, либо найдутся $i, j \in [p]$, $i \neq j$, для которых справедливо $\sigma_i, \sigma_j \geq 1$.

Докажем, что для любого $i \in [p]$ выполнено

$$|Q_i(s_1^{(i)}, \dots, s_{k_i}^{(i)})| \leq \begin{cases} 2, & \sigma_i = 0; \\ \frac{1}{2\sqrt{k_i}}, & \sigma_i = 1; \\ \frac{2}{k_i\sqrt{k_i}}, & \sigma_i \neq 0, 1. \end{cases}$$

Ясно, что достаточно рассмотреть случай $i = 1$. Пусть $\sigma = \sigma_1$. Если $\sigma = 0$, то оценка на Q_1 выполняется. Если $\sigma = 1$, то из неравенства (37) вытекает, что верхняя оценка на Q_1 снова справедлива. Пусть $\sigma \geq 2$, и пусть j_0 – минимальное натуральное число из набора $1, 2, \dots, k_1$ такое, что $2j_0 + 1 \geq \sigma$ (если такого j_0 не существует, то $Q_1 = 0$ и все доказано). Ясно, что все члены в формуле (35) с $j < j_0$ не дают вклад в $Q_1(s_1^{(1)}, \dots, s_{k_1}^{(1)})$. Предположим, что число σ нечетное. Тогда $\sigma = 2r + 1$, $r \geq 1$. Коэффициент при $j = l \geq j_0$ в формуле (35) по модулю не превосходит

$$\begin{aligned} & \frac{1}{2\sqrt{k_1}} \cdot \frac{1}{(64k_1)^l l!} \cdot \frac{(2l+1)!}{|s_1^{(1)}|! \cdots |s_{k_1}^{(1)}|! \cdot (2l+1-\sigma)!} \\ & \times 2k_1 \cdot (2l+1-\sigma-1) \cdot 2k_1 \cdot (2l+1-\sigma-3) \cdots 2k_1 \cdot 1 := \rho. \end{aligned} \quad (40)$$

Действительно, из произведения $(2l + 1)$ скобки в формуле (35) мы должны выбрать член $e(\lambda_1^{(1)}x)$, если $s_1^{(1)} \geq 0$, или член $e(-\lambda_1^{(1)}x)$, если $s_1^{(1)} < 0$, в количестве $|s_1^{(1)}|$ штук. Кроме того, мы должны выбрать $e(\lambda_2^{(1)}x)$, если $s_2^{(1)} \geq 0$, или $e(-\lambda_2^{(1)}x)$, если $s_2^{(1)} < 0$, в количестве $|s_2^{(1)}|$ штук и т.д. Такой выбор можно сделать

$$\frac{(2l + 1)!}{|s_1^{(1)}|! \cdots |s_{k_1}^{(1)}|! \cdot (2l + 1 - \sigma)!}$$

способами. Затем мы выбираем член $e(\lambda_u^{(1)}x)$ с некоторым u из первой среди еще не выбранных скобок. Это можно сделать $2k_1$ способами. Ясно, что необходимо компенсировать член $e(\lambda_u^{(1)}x)$ членом $e(-\lambda_u^{(1)}x)$, выбрав последний из какой-то другой скобки. Это можно сделать $(2l + 1 - \sigma - 1)$ способом. И так далее. В конце концов мы получим оценку (40). Из изложенных выше рассуждений видно, что если σ четное, $\sigma \geq 2$, то число $Q_1(s_1^{(1)}, \dots, s_{k_1}^{(1)})$ равно нулю. Применяя неравенство $\sigma \leq 2l + 1$, находим

$$\begin{aligned} \rho &\leq \frac{1}{2\sqrt{k_1}} \cdot \frac{k_1^{l-r}}{k_1^l 2^{5l}} \\ &\quad \times \frac{(2l+1)(2l)(2l-1) \cdots (2l+1-\sigma+1)(2l+1-\sigma-1)(2l+1-\sigma-3) \cdots 1}{l!} \\ &\leq \frac{1}{2\sqrt{k_1}} k_1^{-r} (2l)^r \frac{2l+1}{2^{4l}} \leq \frac{1}{2k_1\sqrt{k_1}} \frac{(2l+1)2l}{2^{4l}}. \end{aligned}$$

Следовательно,

$$|Q_1(s_1^{(1)}, \dots, s_{k_1}^{(1)})| \leq \frac{1}{k_1\sqrt{k_1}} \sum_{l=1}^{\infty} \frac{(2l+1)2l}{2^{4l}} \leq \frac{2}{k_1\sqrt{k_1}}$$

и верхняя оценка на Q_1 доказана.

Если найдется $i \in [p]$ такое, что $\sigma_i \geq 2$, то из только что доказанной оценки вытекает неравенство $|\widehat{g}(r)| \leq 2^{-p}N/(k')^{3/2}$, где $k' = \min\{k_i : i \in [p]\}$. Пользуясь (27), (28) и (36), получаем, что $|\widehat{g}(r)| \leq \alpha N/4$. Если существует более двух σ_i , равных единице, то опять из (27), (28) и (36) вытекает, что $|\widehat{g}(r)| \leq \alpha N/4$. Пусть, наконец, найдется ровно две σ_i , равных единице. Применяя неравенства (27), (28) и (37), находим

$$|\widehat{g}(r)| \leq \frac{2^{-p}N}{16k'} \leq \frac{\delta p N}{4|\Lambda|} < \frac{3\alpha N}{4}.$$

В любом случае для всех $r \notin \{0\} \sqcup \Lambda \sqcup -\Lambda$ выполнено $|\widehat{f}(r)| \leq |\widehat{g}(r)| < 3\alpha N/4$. Используя неравенство (39), находим $|\widehat{A}(r)| < \alpha N$ для всех $r \notin \{0\} \sqcup \Lambda \sqcup -\Lambda$. Следовательно, $\mathcal{R}_\alpha(A) = \{0\} \sqcup \Lambda \sqcup -\Lambda$. Теорема доказана.

Приведем теперь пример множества больших тригонометрических сумм, для которых теорема 1.3 является точной. В отличие от теоремы 2.8 наше новое множество $\mathcal{R}_\alpha$ не является диссоциативным, а, напротив, обладает сильными аддитивными свойствами.

ТЕОРЕМА 2.11. Пусть $\delta, \alpha \in (0, 1]$ – вещественные числа, N – простое число, k – натуральное число, $2 \leq k \leq 2^{-1} \log(1/\delta)$, $32\delta^2 \leq \alpha \leq \delta/4$, и

$$2k \max \left\{ \log \left(\frac{2^6 \delta k}{\alpha^2} \right), \log \left(\frac{2^6 \delta^2}{\alpha^3} \right) \right\} \leq \log N. \quad (41)$$

Тогда найдется множество $A \subseteq \mathbb{Z}_N$ такое, что $\delta N \leq |A| \leq 3\delta N$, $|\mathcal{R}_\alpha(A)| \geq \delta/(64\alpha^2)$ и для всех k , удовлетворяющих неравенству (41), выполнено

$$T_k(\mathcal{R}_\alpha(A)) \leq \frac{2^{14k} \delta}{\alpha^{2k}}.$$

ЗАМЕЧАНИЕ 2.12. В теореме 2.11 доказывается $|\mathcal{R}_\alpha(A)| \geq \delta/(64\alpha^2)$. Это неравенство совпадает по порядку с верхней оценкой для мощности множества $\mathcal{R}_\alpha(A)$, вытекающей из равенства Парсеваля: $|\mathcal{R}_\alpha(A)| \leq 3\delta/\alpha^2$. Какая-то нижняя оценка для $|\mathcal{R}_\alpha(A)|$ в теореме 2.11 необходима, поскольку иначе эта теорема становится тривиальной. Действительно, если $|\mathcal{R}_\alpha(A)|$ мало, то, очевидно, и величина $T_k(\mathcal{R}_\alpha(A))$ мала.

Для доказательства теоремы 2.11 нам понадобятся определение и лемма.

ОПРЕДЕЛЕНИЕ 2.13. Пусть k, s – натуральные числа. Рассмотрим семейство множеств $\tilde{\Lambda}(k, s)$ из $\mathbb{Z}_N$, обладающих следующим свойством. Если множество $\tilde{\Lambda} = \{\tilde{\lambda}_1, \dots, \tilde{\lambda}_{|\tilde{\Lambda}|}\}$ принадлежит семейству $\tilde{\Lambda}(k, s)$, то из равенства

$$\sum_{i=1}^{|\tilde{\Lambda}|} \tilde{\lambda}_i s_i = 0 \pmod{N}, \quad (42)$$

$$\tilde{\lambda}_i \in \Lambda, \quad s_i \in \mathbb{Z}, \quad |s_i| \leq s, \quad \text{число } s_i \neq 0 \text{ не превосходит } k,$$

вытекает, что все s_i равны нулю.

Ясно, что $\Lambda(k, s) \subseteq \tilde{\Lambda}(k, s) \subseteq \Lambda(k, s)$.

ЛЕММА 2.14. Пусть N, t, k, s – натуральные числа, $k \leq t$ и $N > \binom{t}{k}(2s+1)^k$. Тогда семейство $\tilde{\Lambda}(k, s)$ содержит некоторое множество из t элементов.

ДОКАЗАТЕЛЬСТВО. Рассмотрим все наборы $(a_1, \dots, a_t)$ длины t , где $a_i \in \mathbb{Z}_N$. Ясно, что существует ровно N^t таких наборов. Далее, существует не более чем $\binom{t}{k}(2s+1)^k$ уравнений (42) с коэффициентами $s_1, \dots, s_t$. Любому уравнению (42), не все коэффициенты которого нулевые, удовлетворяет не более чем $N^{k-1}N^{t-k} = N^{t-1}$ решений $(a_1, \dots, a_t)$. Кроме того,

$$N^{t-1} \binom{t}{k} (2s+1)^k < N^t.$$

Значит, найдется набор $(a_1, \dots, a_t)$, удовлетворяющий только одному уравнению (42), а именно уравнению с нулевыми коэффициентами. Легко видеть, что все вычеты в наборе $(a_1, \dots, a_t)$ различные. Следовательно, множество $\tilde{\Lambda} = \{a_1, \dots, a_t\}$, состоящее из t элементов, принадлежит семейству $\tilde{\Lambda}(k, s)$. Лемма доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2.11. Пусть

$$k_1 = 2k, \quad t = \left\lceil \frac{\delta}{\alpha} \right\rceil, \quad \varepsilon = \frac{\delta}{t}, \quad m = \max\{t, k_1\}, \quad s = \left\lceil \frac{8m}{\varepsilon} \right\rceil.$$

По условию

$$2k \log \frac{2^6 \delta^2}{\alpha^3} \leq \log N, \quad 2k \log \frac{2^6 \delta k}{\alpha^2} \leq \log N.$$

Отсюда $N > \binom{t}{k_1} (2s+1)^{k_1}$ и все условия леммы 2.14 выполнены. Применяя эту лемму, находим множество $\Lambda = \{\lambda_1, \dots, \lambda_t\}$, принадлежащее семейству $\tilde{\Lambda}(k_1, s)$.

Для любого $\lambda \in \mathbb{Z}_N$ рассмотрим одномерное множество Бора

$$B_\lambda = B_\lambda(\varepsilon) = \left\{ x \in \mathbb{Z}_N : \left\| \frac{x\lambda}{N} \right\| \leq \varepsilon \right\}, \quad (43)$$

где $\|\cdot\|$ означает целую часть действительного числа (более подробная информация о множествах Бора может быть найдена в [18]). Ясно, что

$$B_\lambda(\varepsilon) = \{0, \pm\lambda^{-1}, \dots, \pm[\varepsilon N]\lambda^{-1}\}.$$

Отсюда $|B_\lambda(\varepsilon)| = 2[\varepsilon N] + 1$. Обозначим через $B_\lambda^{s'} = B_\lambda^{s'}(\varepsilon)$ множество, получающееся сдвигом множества Бора: $B_\lambda^{s'} = B_\lambda + s'$. Пользуясь индукцией, построим семейство множеств $B_{\lambda_1}^{s_1}, \dots, B_{\lambda_t}^{s_t}$, где $\lambda_i \in \Lambda$, $s_i \in \mathbb{Z}_N$. Пусть $s_1 = 0$ и множество $B_{\lambda_1}^{s_1}$ построено. Предположим, что у нас есть множества $B_{\lambda_1}^{s_1}, \dots, B_{\lambda_d}^{s_d}$. Найдем вычет s_{d+1} и множество $B_{\lambda_{d+1}}^{s_{d+1}}$. Пусть $C_d = \bigcup_{i=1}^d B_{\lambda_i}^{s_i}$. Ясно, что $|C_d| \leq d(2[\varepsilon N] + 1) \leq t(2[\varepsilon N] + 1) \leq 3\delta N$. Возьмем в качестве s_{d+1} такой вычет, что

$$|B_{\lambda_{d+1}}^{s_{d+1}} \cap C_d| \leq (2\varepsilon N + 1)^2 t \leq 8\varepsilon \delta N. \quad (44)$$

Так как

$$\sum_{s' \in \mathbb{Z}_N} |C_d \cap B_{\lambda_{d+1}}^{s'}| = |C_d| |B_{\lambda_{d+1}}|,$$

то легко видеть, что вычет s_{d+1} с требуемыми свойствами существует. Таким образом, мы построили множества $B_{\lambda_1}^{s_1}, \dots, B_{\lambda_t}^{s_t}$. Пусть $A = C_t = \bigcup_{i=1}^t B_{\lambda_i}^{s_i}$. Ясно, что $|A| \leq 3\delta N$. Докажем, что $|A| \geq \delta N$. Из условий (41) и неравенства $32\delta^2 \leq \alpha \leq \delta/4$ вытекает, что $N \geq 2^6 \delta^2 / (\alpha^3) \geq 4\delta / (\alpha^2)$. Отсюда $t \leq \varepsilon N / 4$ и $8t\varepsilon \delta N \leq \varepsilon N / 4$. Применяя формулу (44) и два последних неравенства, находим

$$|A| = |C_t| = |C_{t-1}| + |B_{\lambda_t}^{s_t}| - |C_{t-1} \cap B_{\lambda_t}^{s_t}| \geq |C_{t-1}| + (2[\varepsilon N] + 1) - 8\varepsilon \delta N. \quad (45)$$

Продолжим выкладки

$$\begin{aligned} |C_{t-1}| + (2[\varepsilon N] + 1) - 8\varepsilon \delta N &\geq |C_{t-2}| + 2(2[\varepsilon N] + 1) - 2 \cdot 8\varepsilon \delta N \\ &\geq \dots \geq t(2[\varepsilon N] + 1) - t8\varepsilon \delta N \end{aligned} \quad (46)$$

и, наконец,

$$t(2[\varepsilon N] + 1) - t8\varepsilon \delta N \geq 2\varepsilon tN - t - \frac{\varepsilon N}{4} \geq \varepsilon tN = \delta N. \quad (47)$$

Докажем теперь, что $|\mathcal{R}_\alpha(A)| \geq \delta/(64\alpha^2)$. Пусть $a \in \mathbb{Z}_N$. Считая, что a принадлежит приведенной системе вычетов, обозначим через $|a|$ абсолютную величину a . Имеем $|a| \leq N/2$ для всех a из $\mathbb{Z}_N$. Пусть $r \in \mathbb{Z}_N$, $r \neq 0$. Применяя неравенство $|1 - e^{i\theta}| \geq 2|\theta|/\pi$, $\theta \in [-\pi, \pi]$, находим

$$\begin{aligned} |\widehat{B}_\lambda(r)| &= \left| \sum_{l=-[\varepsilon N]}^{[\varepsilon N]} e(\lambda^{-1}lr) \right| = \left| \frac{e((2[\varepsilon N] + 1)\lambda^{-1}r) - 1}{e(\lambda^{-1}r) - 1} \right| \\ &\leq \frac{4}{|e(\lambda^{-1}r) - 1|} \leq \frac{N}{|\lambda^{-1}r|}. \end{aligned} \quad (48)$$

Получим теперь нижнюю оценку для величины $\widehat{B}_\lambda(r)$. Пусть λ принадлежит множеству Λ , и пусть

$$M_\lambda = \left\{ x \in \mathbb{Z}_N : x = \lambda p, |p| \leq \frac{1}{16\varepsilon} \right\}. \quad (49)$$

Имеем $|M_\lambda| = 2[1/(16\varepsilon)] + 1$. Для всех $r \in M_\lambda$ справедлива формула

$$\widehat{B}_\lambda(r) = 2 \sum_{l=0}^{[\varepsilon N]} \cos\left(\frac{2\pi\lambda^{-1}rl}{N}\right) - 1 \geq 2([\varepsilon N] + 1) - 1 - \frac{[\varepsilon N] + 1}{4} \geq \frac{3}{2}\varepsilon N. \quad (50)$$

Формулы (48) и (50) позволяют оценивать коэффициенты Фурье множеств $B_\lambda = B_\lambda(\varepsilon)$. Заметим, что для всех s' и r из $\mathbb{Z}_N$ выполнено $|\widehat{B}_\lambda^{s'}(r)| = |\widehat{B}_\lambda(r)|$. Таким образом, формулы (48), (50) можно использовать и для нахождения модулей коэффициентов Фурье множеств $B_\lambda^{s'}$.

Легко видеть, что для всех $i, j \in [t]$, $i \neq j$, выполнено $M_{\lambda_i} \cap M_{\lambda_j} = \{0\}$. Действительно, по построению множество Λ принадлежит семейству $\widetilde{\Lambda}(k_1, s)$ и $s \geq 1/(16\varepsilon)$. Отсюда уравнение $\lambda_i p_i = \lambda_j p_j$, $i \neq j$, $|p_i|, |p_j| \leq 1/(16\varepsilon)$, имеет единственное решение $p_i = p_j = 0$. Докажем, что $\bigcup_{i=1}^t M_{\lambda_i} \subseteq \mathcal{R}_\alpha(A)$. Очевидно, что $0 \in \mathcal{R}_\alpha(A)$. Пусть число $i \in [t]$ произвольное и r — любой ненулевой вычет, принадлежащий некоторому M_{λ_i} . Имеем

$$\widehat{A}(r) = \widehat{B}_{\lambda_i}^{s_i}(r) + \widehat{C}_{t-1}(r) + 8\theta\varepsilon\delta N,$$

где $|\theta| \leq 1$. Действуя аналогично (45)–(47), получаем

$$\widehat{A}(r) = \sum_{l=1}^t \widehat{B}_{\lambda_l}^{s_l}(r) + 8\widetilde{\theta}\varepsilon\delta tN, \quad (51)$$

где $|\widetilde{\theta}| \leq 1$. Так как $r \in M_{\lambda_i}$, то по формуле (50) имеем $|\widehat{B}_{\lambda_i}^{s_i}(r)| \geq 3\varepsilon N/2$. Пусть $r = \lambda_i p_i$, $|p_i| \leq 1/(16\varepsilon)$ и $j \in [t]$ — любое число, не равное i . Пусть $p := \lambda_j^{-1}r = \lambda_j^{-1}\lambda_i p_i$. Тогда $\lambda_j p = \lambda_i p_i$. Так как множество Λ принадлежит семейству $\widetilde{\Lambda}(k_1, s)$, то $|p| > s$. Применяя это неравенство и формулу (48), получаем

$$|\widehat{B}_{\lambda_j}^{s_j}(r)| \leq \frac{N}{s}, \quad r \in M_{\lambda_i}, \quad i \neq j, \quad r \neq 0. \quad (52)$$

Отсюда и из (51) находим

$$|\widehat{A}(r)| \geq \frac{3}{2} \varepsilon N - \sum_{j \neq i} |\widehat{B}_{\lambda_j}^{s_j}(r)| - 8\varepsilon \delta t N \geq \frac{3}{2} \varepsilon N - \frac{tN}{s} - 8\varepsilon \delta t N \geq \alpha N.$$

Следовательно, $\bigcup_{i=1}^t M_{\lambda_i} \subseteq \mathcal{R}_\alpha(A)$ и

$$|\mathcal{R}_\alpha(A)| \geq \sum_{i=1}^t |M_{\lambda_i}| - t = 2t \left[\frac{1}{16\varepsilon} \right] \geq \frac{\delta}{64\alpha^2}.$$

Наконец докажем, что для всех натуральных k , $2 \leq k \leq 2^{-1} \log(1/\delta)$, выполнено $T_k(\mathcal{R}_\alpha(A)) \leq 2^{14k} \delta / (\alpha^{2k})$. Пусть g – действительное число, λ принадлежит множеству Λ , и пусть

$$L_\lambda(g) = \{x \in \mathbb{Z}_N : x = \lambda p, |p| \leq g\}. \quad (53)$$

Пусть также $M'_\lambda = L_\lambda(8/\varepsilon)$. Тогда $|M'_\lambda| \leq 32/\varepsilon$. Докажем, что $\mathcal{R}_\alpha(A) \subseteq \bigcup_{\lambda \in \Lambda} M'_\lambda$. Предположим противное. Пусть $r \in \mathcal{R}_\alpha(A) \setminus \{0\}$ и $r \notin \bigcup_{\lambda \in \Lambda} M'_\lambda$. Если $r \notin \bigcup_{\lambda \in \Lambda} L_\lambda(s)$, то, применяя формулу (51), находим

$$|\widehat{A}(r)| \leq \frac{tN}{s} + 8\varepsilon \delta t N \leq \frac{\varepsilon}{2} N < \alpha N$$

и $r \notin \mathcal{R}_\alpha(A)$. Пусть теперь $r \in \bigcup_{\lambda \in \Lambda} L_\lambda(s)$. Пользуясь тем фактом, что $\Lambda \in \widetilde{\Lambda}(k_1, s)$, получаем, что для всех $\lambda_1, \lambda_2 \in \Lambda$, $\lambda_1 \neq \lambda_2$, выполнено $L_{\lambda_1}(s) \cap L_{\lambda_2}(s) = \{0\}$. Пусть $r \neq 0$. Тогда вычет r принадлежит некоторому множеству $L_{\lambda_i}(s)$, где $i \in [t]$ и число i определяется по r однозначно. Применяя формулу (51), находим

$$|\widehat{A}(r)| \leq |\widehat{B}_{\lambda_i}^{s_i}(r)| + \frac{tN}{s} + 8\varepsilon \delta t N. \quad (54)$$

Так как $r \notin \bigcup_{\lambda \in \Lambda} M'_\lambda$, то из формулы (48) вытекает, что $|\widehat{B}_{\lambda_i}^{s_i}(r)| \leq N/g \leq \varepsilon N/8$. Подставляя последнее неравенство в (54), получаем $|\widehat{A}(r)| \leq \varepsilon N/2 < \alpha N$ и $r \notin \mathcal{R}_\alpha(A)$. Следовательно, $\mathcal{R}_\alpha(A) \subseteq \bigcup_{\lambda \in \Lambda} M'_\lambda$.

Рассмотрим уравнение

$$r_1 + \dots + r_k = r'_1 + \dots + r'_k, \quad (55)$$

где все r_j, r'_j принадлежат $\mathcal{R}_\alpha(A)$. Так как $\mathcal{R}_\alpha(A) \subseteq \bigcup_{i=1}^t M'_{\lambda_i}$, то каждый вычет из (55) принадлежит некоторому множеству M'_{λ_i} .

Пусть z – целое неотрицательное число и $s_1, \dots, s_l$ – натуральные числа такие, что $s_1 + \dots + s_l + z = 2k$. Можно считать, для определенности, набор $s_1, \dots, s_l$ упорядоченным по убыванию $s_1 \geq s_2 \geq \dots \geq s_l \geq 1$. Выше отмечалось, что для всех $\lambda_1, \lambda_2 \in \Lambda$, $\lambda_1 \neq \lambda_2$, выполнено $L_{\lambda_1}(s) \cap L_{\lambda_2}(s) = \{0\}$. Следовательно, для всех $i, j \in [t]$, $i \neq j$, имеем $M'_{\lambda_i} \cap M'_{\lambda_j} = \{0\}$. Пусть $M'_i = M'_{\lambda_i}$, $i \in [t]$, и $w = 2^5/\varepsilon$. Тогда для всех $i \in [t]$ выполнено $|M'_i| \leq w$. Пусть $E(s_1, \dots, s_l, z)$ – множество таких решений $r_1, \dots, r_k, r'_1, \dots, r'_k$ уравнения (55),

что среди r_j, r'_j существует ровно z нулей, существует ровно s_1 ненулевых вычетов, принадлежащих некоторому множеству M'_{j_1} , существует ровно s_2 ненулевых вычетов, принадлежащих некоторому множеству M'_{j_2} , ..., существует ровно s_l ненулевых вычетов, принадлежащих некоторому множеству M'_{j_l} , и при этом все множества $M'_{j_1}, M'_{j_2}, \dots, M'_{j_l}$ различные. Пользуясь тем, что $\Lambda \in \tilde{\Lambda}(k_1, s)$, получаем

$$\begin{aligned} T_k(\mathcal{R}_\alpha(A)) &= \sum_{l=0}^{2k} \sum_{z=0}^{2k} \sum_{\substack{s_1, \dots, s_l \\ s_1 + \dots + s_l + z = 2k}} |E(s_1, \dots, s_l, z)| \\ &\leq 1 + tw^{2k-1} + \sum_{l=2}^{2k} \sum_{z=0}^{2k} \sum_{\substack{s_1, \dots, s_l \\ s_1 + \dots + s_l + z = 2k}} |E(s_1, \dots, s_l, z)|. \end{aligned} \quad (56)$$

Зафиксируем $s_1, \dots, s_l, z$ и рассмотрим решения уравнения (55), принадлежащие фиксированным подмножествам $M'_{j_1}, M'_{j_2}, \dots, M'_{j_l}$. Обозначим множество этих решений через

$$E(s_1, \dots, s_l, z)(M'_{j_1}, M'_{j_2}, \dots, M'_{j_l}).$$

Перепишем уравнение (55) в виде

$$u_1 + \dots + u_l = 0, \quad (57)$$

где $u_i \in M'_{j_i}$, $i \in [l]$. Так как множество Λ принадлежит семейству $\tilde{\Lambda}(k_1, s)$, то все вычеты u_i равны нулю. Следовательно, для мощности множества решений $E(s_1, \dots, s_l, z)(M'_{j_1}, M'_{j_2}, \dots, M'_{j_l})$ справедлива оценка

$$\begin{aligned} &|E(s_1, \dots, s_l, z)(M'_{j_1}, M'_{j_2}, \dots, M'_{j_l})| \\ &\leq \frac{(2k)!}{s_1! \dots s_l! z!} w^{s_1-1} \dots w^{s_l-1} \leq \frac{(2k)!}{s_1! \dots s_l! z!} w^{2k-l}. \end{aligned}$$

Отсюда

$$|E(s_1, \dots, s_l, z)| \leq \binom{t}{l} \frac{(2k)!}{s_1! \dots s_l! z!} w^{2k-l} \leq \frac{t^l}{l!} \cdot \frac{(2k)!}{s_1! \dots s_l! z!} w^{2k-l}. \quad (58)$$

Подставляя оценку (58) в формулу (56), находим

$$\begin{aligned} T_k(\mathcal{R}_\alpha(A)) &\leq 2tw^{2k-1} + \sum_{l=2}^{2k} \frac{t^l}{l!} w^{2k-l} \sum_{\substack{s_1, \dots, s_l \\ s_1 + \dots + s_l + z = 2k}} \frac{(2k)!}{s_1! \dots s_l! z!} \\ &\leq 2tw^{2k-1} + \sum_{l=2}^{2k} \frac{t^l}{l!} w^{2k-l} (l+1)^{2k} \\ &= 2tw^{2k-1} + w^{2k} \sum_{l=2}^{2k} \left(\frac{t}{w}\right)^l (l+1)^{2k} \frac{1}{l!}. \end{aligned} \quad (59)$$

Рассмотрим функцию $f(l) = (t/w)^l(l+1)^{2k}$. Взяв производную, получаем, что максимальное значение этой функции достигается при $l_0 = 2k/\ln(w/t) - 1$, а для всех $l \geq l_0$ функция $f(l)$ монотонно убывает. По условию $k \leq 2^{-1} \log(1/\delta)$. Отсюда $l_0 \leq 1$. Следовательно,

$$T_k(\mathcal{R}_\alpha(A)) \leq 2tw^{2k-1} + 2^{2k}tw^{2k-1} \leq 2^{2k+1}tw^{2k-1} \leq \frac{2^{14k}\delta}{\alpha^{2k}}.$$

Теорема доказана.

§ 3. Доказательство теоремы 1.5

Мы будем предполагать на протяжении всего этого параграфа, что число N простое.

ОПРЕДЕЛЕНИЕ 3.1. Пусть k, s, d – натуральные числа. Пусть также $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\} \subseteq \mathbb{Z}_N$ – некоторое множество такое, что $\Lambda \cap -\Lambda = \emptyset$. Пусть $\vec{v}_1 = (v_1^{(1)}, \dots, v_1^{(d)}), \dots, \vec{v}_{|\Lambda|} = (v_{|\Lambda|}^{(1)}, \dots, v_{|\Lambda|}^{(d)})$ – произвольные векторы из $\mathbb{Z}^d$, все координаты которых не превосходят по модулю числа s . Рассмотрим уравнение

$$\lambda_1 \vec{v}_1 + \dots + \lambda_{|\Lambda|} \vec{v}_{|\Lambda|} = 0 \pmod{N}, \quad (60)$$

где $\lambda_i \in \Lambda$ и для каждого $i \in [d]$ выполнено $\sum_{j=1}^{|\Lambda|} |v_j^{(i)}| \leq k$. В уравнении (60) неизвестными являются $v_j^{(i)}$, $i \in [d]$, $j \in [|\Lambda|]$. Множество Λ принадлежит семейству $\Lambda_d(k, s)$, если для любого решения уравнения (60) матрица

$$\begin{pmatrix} v_1^{(1)} & \dots & v_{|\Lambda|}^{(1)} \\ \dots & \dots & \dots \\ v_1^{(d)} & \dots & v_{|\Lambda|}^{(d)} \end{pmatrix}$$

имеет ранг строго меньше d .

Как уже было сказано ранее, определение семейства $\Lambda_1(k, 1)$ можно найти в статье [26], а семейства $\Lambda_1(k, s)$ – в [15].

Заметим, что условие $\Lambda \cap -\Lambda = \emptyset$ для множеств семейств $\Lambda_1(k, s)$ выполнено автоматически.

Для множеств семейства $\Lambda_d(k, s)$ справедлива следующая верхняя оценка на величину T_k .

ПРЕДЛОЖЕНИЕ 3.2. Пусть N, k, s, d – натуральные числа, $N \geq s + 1$ простое и $\Lambda \subseteq \mathbb{Z}_N$ – произвольное множество из семейства $\Lambda_d(2k, s)$. Тогда

$$T_k(\Lambda) \leq (s+1)^{d5k} k^k |\Lambda|^k \max \left\{ 1, \left(\frac{k}{|\Lambda|} \right)^k |\Lambda|^{k/s} \right\}. \quad (61)$$

ПРИМЕР 3.3. Пусть $k \geq 2$, $|\Lambda| \geq k^2$ и Λ – произвольное множество из класса $\Lambda_d(k, 2)$. Применяя неравенство (61), получаем $T_k(\Lambda) \leq 2^{5k+2d} k^k |\Lambda|^k$. Легко видеть, что если $d = O(k)$, то эта оценка является неулучшаемой по порядку.

ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 3.2. 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

$$\lambda_1 + \dots + \lambda_k = x. \quad (62)$$

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 $s_1 \geq s_2 \geq \dots \geq s_l \geq 1$. Пусть $E(s_1, \dots, s_l)(x)$ – множество таких решений $(\lambda_1, \dots, \lambda_k)$ уравнения (62), что среди $\lambda_1, \dots, \lambda_k$ существует ровно s_1 одинаковых $\tilde{\lambda}_1$, существует ровно s_2 одинаковых $\tilde{\lambda}_2, \dots$, существует ровно s_l одинаковых $\tilde{\lambda}_l$ таких, что $s_1 \tilde{\lambda}_1 + \dots + s_l \tilde{\lambda}_l = x$ и при этом все $\tilde{\lambda}_i$ 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, для которых $\sum_{i=1}^l s_i = k$. Отсюда

$$\sigma = T_k(\Lambda) = \sum_{x \in \mathbb{Z}_N} \left(\sum_{\vec{s}} |E(\vec{s})(x)| \right)^2. \quad (63)$$

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

$$l \leq k - s|B|. \quad (64)$$

Действительно,

$$k = \sum_{i \in G} s_i + \sum_{i \in B} s_i \geq |G| + (s+1)|B| = l + s|B|. \quad (65)$$

Из неравенства (65) вытекает неравенство (64). Пусть также

$$l_j = l_j(\vec{s}) = |\{i : s_i = j, i \in [l]\}|, \quad j = 1, 2, \dots, r = r(\vec{s}), \quad r \neq 0.$$

Нам понадобятся две леммы.

ЛЕММА 3.4. Пусть n, t, s – натуральные числа, $t \leq n$, $\vec{u}_1, \dots, \vec{u}_t \in \mathbb{Z}_N^n$ – линейно независимая над $\mathbb{Z}_N$ система векторов и $N \geq s+1$. Пусть также

$$Q(s) := \{\vec{x} = (x_1, \dots, x_n) \in \mathbb{Z}_N^n : x_i \in \{0, 1, \dots, s\}, i = 1, \dots, n\}$$

– n -мерный куб и

$$L = \{\vec{x} \in \mathbb{Z}_N^n : \vec{x} = \sum_{i=1}^t m_i \vec{u}_i, m_i \in \mathbb{Z}_N\}.$$

Тогда $|L \cap Q(s)| \leq (s+1)^t$.

ДОКАЗАТЕЛЬСТВО. Пусть $\vec{u}_1 = (u_1^{(1)}, \dots, u_1^{(n)})$, $\dots$, $\vec{u}_t = (u_t^{(1)}, \dots, u_t^{(n)})$. Заметим, что куб $Q(s)$ инвариантен относительно перестановок координат. Переходя, если это необходимо, к другой линейно независимой системе векторов $\vec{w}_1, \dots, \vec{w}_t$ такой, что линейная оболочка векторов $\vec{w}_1, \dots, \vec{w}_t$ совпадает с L , можно, не ограничивая общности, считать, что векторы $\vec{u}_1, \dots, \vec{u}_t$ имеют вид

$$\begin{aligned}\vec{u}_1 &= (1, \dots, 0, 0, u_t^{(t+1)}, \dots, u_1^{(n)}), \\ \vec{u}_2 &= (0, 1, \dots, 0, u_t^{(t+1)}, \dots, u_2^{(n)}), \\ &\vdots \\ \vec{u}_t &= (0, \dots, 0, 1, u_t^{(t+1)}, \dots, u_t^{(n)}).\end{aligned}$$

Пусть $\vec{x}$ – произвольный вектор из $L \cap Q(s)$. Тогда найдутся вычеты $m_1, \dots, m_t$ такие, что $\vec{x} = \sum_{i=1}^t m_i \vec{u}_i$. Ясно, что $m_1 = x_1, \dots, m_t = x_t$. Так как $\vec{x} \in Q(s)$, то $m_i \in \{0, 1, \dots, s\}$, $i = 1, \dots, t$. Отсюда $|L \cap Q(s)| \leq (s+1)^t$. Лемма 3.4 доказана.

ЛЕММА 3.5. Для любого $\vec{s}$, $\sum_{i=1}^l s_i = k$, и любого $x \in \mathbb{Z}_N$ выполнено

$$|E(\vec{s})(x)| \leq \frac{k!}{s_1! \cdots s_l!} (s+1)^d |\Lambda|^{|\mathcal{B}(\vec{s})|}. \quad (66)$$

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. Мы видим, что набору $(\lambda^{(1)}, \dots, \lambda^{(k)}) \in E(\vec{s})(x)$ однозначно соответствует набор $(\tilde{\lambda}^{(1)}, \dots, \tilde{\lambda}^{(l)})$, все элементы которого – различные числа. Зафиксируем вычеты $\tilde{\lambda}^{(i)}$ с $i \in B(\vec{s})$ и рассмотрим множество $K = K(B(\vec{s}))$ всех наборов из $E(\vec{s})(x)$ с этими фиксированными $\tilde{\lambda}^{(i)}, i \in B(\vec{s})$. Докажем, что мощность K не превосходит $(s+1)^d k! / (s_1! \cdots s_l!)$.

Пусть $(\lambda^{(1)}, \dots, \lambda^{(k)})$ – произвольный набор из K . Имеем

$$\sum_{i \in G(\vec{s})} s_i \tilde{\lambda}^{(i)} = x - \sum_{i \in B(\vec{s})} s_i \tilde{\lambda}^{(i)} = x'. \quad (67)$$

Так как элементы $\tilde{\lambda}^{(i)}, i \in B(\vec{s})$, фиксированы, то вычет x' не зависит от набора $(\lambda^{(1)}, \dots, \lambda^{(k)}) \in K$.

Упорядочим множество $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ произвольным способом. Сопоставим каждому набору $(\lambda^{(1)}, \dots, \lambda^{(k)})$ из K вектор $\vec{u} = (u_1, \dots, u_{|\Lambda|})$, где

$$u_j = \begin{cases} s_i, & \text{если для некоторого } i \in G(\vec{s}) \text{ выполнено } \lambda_j = \tilde{\lambda}^{(i)}; \\ 0 & \text{в противном случае.} \end{cases}$$

Пусть $\vec{w} = (w_1, \dots, w_m)$, $\vec{w}' = (w'_1, \dots, w'_m)$ – два вектора из $\mathbb{Z}^m$. Обозначим через $(\vec{w}, \vec{w}')$ скалярное произведение этих векторов: $(\vec{w}, \vec{w}') = \sum_{j=1}^m w_j w'_j$. Тогда равенство (67) может быть переписано в виде

$$(\vec{u}, \vec{\lambda}) = x', \quad (68)$$

где $\vec{\lambda} = (\lambda_1, \dots, \lambda_{|\Lambda|})$. Пусть $\vec{u}_1, \dots, \vec{u}_t$ – максимальная линейно независимая над $\mathbb{Z}_N$ система векторов, каждый из которых удовлетворяет уравнению (68).

Зафиксируем b и оценим сумму σ_b . Имеем

$$\sigma_b \leq \left(\sum_{x \in \mathbb{Z}_N} \sum_{\vec{s}: |B(\vec{s})|=b} |E(\vec{s})(x)| \right) \left(\max_{x \in \mathbb{Z}_N} \sum_{\vec{s}: |B(\vec{s})|=b} |E(\vec{s})(x)| \right). \quad (70)$$

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

$$\sum_{\vec{s}} P_k(\vec{s}) \leq \sum_{l=1}^k \sum_{\substack{s_1, \dots, s_l=0 \\ s_1 + \dots + s_l = k}}^k \frac{k!}{s_1! \cdots s_l!} = \sum_{l=1}^k l^k \leq 2k^k. \quad (71)$$

Применяя лемму 3.5, находим $|E(\vec{s})(x)| \leq (s+1)^d P_k(\vec{s}) |\Lambda|^{|B(\vec{s})|}$. Отсюда и из неравенства (71) получаем

$$\max_{x \in \mathbb{Z}_N} \sum_{\vec{s}: |B(\vec{s})|=b} |E(\vec{s})(x)| \leq 2(s+1)^d k^k |\Lambda|^b. \quad (72)$$

Рассмотрим сумму

$$\sum_{x \in \mathbb{Z}_N} \sum_{\vec{s}: |B(\vec{s})|=b} |E(\vec{s})(x)|. \quad (73)$$

Из неравенства (64) 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 чем $k - sb$ различных. Следовательно,

$$\begin{aligned} \sum_{x \in \mathbb{Z}_N} \sum_{\vec{s}: |B(\vec{s})|=b} |E(\vec{s})(x)| &\leq \binom{|\Lambda|}{k-sb} (k-sb)^k \leq \frac{|\Lambda|^{k-sb}}{(k-sb)!} (k-sb)^k \\ &\leq e^k k^{sb} |\Lambda|^{k-sb}. \end{aligned} \quad (74)$$

Отсюда и из (72) находим

$$\sigma_b \leq 2(s+1)^d e^k k^k |\Lambda|^b \left(\frac{k}{|\Lambda|} \right)^{sb} |\Lambda|^k. \quad (75)$$

Значит,

$$\sigma \leq 2(k+1)^2 (s+1)^d e^k k^k |\Lambda|^k \sum_{b=0}^{\lfloor k/s \rfloor} \left(\frac{k^s}{|\Lambda|^{s-1}} \right)^b = 2(k+1)^2 (s+1)^d e^k k^k |\Lambda|^k \sigma^*. \quad (76)$$

Оценим сумму σ^* . Если $k^s \leq |\Lambda|^{s-1}$, то легко видеть, что $\sigma^* \leq k$. Если же $k^s > |\Lambda|^{s-1}$, то $\sigma^* \leq k(k/|\Lambda|)^k |\Lambda|^{k/s}$. В любом случае

$$\sigma^* \leq k \max \left\{ 1, \left(\frac{k}{|\Lambda|} \right)^k |\Lambda|^{k/s} \right\}.$$

Следовательно,

$$\sigma = T_k(\Lambda) \leq (s+1)^d 2^{5k} k^k |\Lambda|^k \max \left\{ 1, \left(\frac{k}{|\Lambda|} \right)^k |\Lambda|^{k/s} \right\}. \quad (77)$$

Предложение 3.2 доказано.

Приступим непосредственно к доказательству теоремы 1.5.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1.5. Пусть $k = \lceil \log(1/\delta) \rceil$. Так как $0 \in \mathcal{R}_\alpha$ и $\mathcal{R}_\alpha = -\mathcal{R}_\alpha$, то существует множество $\mathcal{R}_\alpha^{(1)}$ такое, что $\mathcal{R}_\alpha = \mathcal{R}_\alpha^{(1)} \sqcup -\mathcal{R}_\alpha^{(1)} \sqcup \{0\}$ и $\mathcal{R}_\alpha^{(1)} \cap -\mathcal{R}_\alpha^{(1)} = \emptyset$. Пусть $s = 2$ и $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ – максимальное подмножество $\mathcal{R}_\alpha^{(1)}$, принадлежащее семейству $\Lambda_d(2k, s)$. Пусть

$$\Lambda^* = \left(\bigcup_{j=1}^s j^{-1}\Lambda \right) \cup \left(-\bigcup_{j=1}^s j^{-1}\Lambda \right).$$

Тогда $|\Lambda^*| \leq 8|\Lambda|$.

Докажем, что для любого $r \in \mathcal{R}_\alpha^{(1)}$ найдутся вектор $\vec{u} = (u_1, \dots, u_d)$ и векторы $\vec{v}_1 = (v_1^{(1)}, \dots, v_1^{(d)})$, $\dots$, $\vec{v}_{|\Lambda|} = (v_{|\Lambda|}^{(1)}, \dots, v_{|\Lambda|}^{(d)})$ такие, что $|u_l| \leq s$, $l = 1, \dots, d$, $|v_j^{(i)}| \leq s$, $i = 1, \dots, d$, $j = 1, \dots, |\Lambda|$, и

$$r\vec{u} = \sum_{i=1}^{|\Lambda|} \lambda_i \vec{v}_i, \quad (78)$$

где для всех $i \in [d]$ выполнено $\sum_{j=1}^{|\Lambda|} |v_j^{(i)}| \leq k$ и ранг матрицы

$$M = \begin{pmatrix} v_1^{(1)} & \dots & v_{|\Lambda|}^{(1)} \\ \dots & \dots & \dots \\ v_1^{(d)} & \dots & v_{|\Lambda|}^{(d)} \end{pmatrix}$$

равен d .

Легко видеть, что из существования векторов $\vec{u}, \vec{v}_1, \dots, \vec{v}_{|\Lambda|}$ вытекает справедливость равенства (12). Действительно, так как множество Λ принадлежит семейству $\Lambda_d(2k, s)$, то вектор $\vec{u}$ ненулевой и, следовательно, у $\vec{u}$ есть ненулевая компонента. Без ограничения общности можно считать, что первая компонента вектора $\vec{u}$ является ненулевой. Сложим первое уравнение системы (78) со всеми уравнениями (78), где вектор $\vec{u}$ имеет нулевую компоненту. Получим новую систему

$$r\vec{u}' = \sum_{i=1}^{|\Lambda|} \lambda_i \vec{v}'_i, \quad (79)$$

где все компоненты вектора $\vec{u}'$ не равны нулю, для любого $i \in [d]$ выполнено $\sum_{j=1}^{|\Lambda|} |(v'_j)^{(i)}| \leq 2k \leq 4\log(1/\delta)$ и матрица M' , составленная из векторов $\vec{v}'_1, \dots, \vec{v}'_{|\Lambda|}$, имеет ранг, равный d . Домножая, если это необходимо, уравнения системы (79) на -1 , можно добиться того, чтобы все компоненты вектора $\vec{u}'$ принадлежали отрезку $[s]$. Так как для любого $i \in [|\Lambda|]$ и любого $j \in [s]$ выполнено $j^{-1}\lambda_i \in \Lambda^*$, то из системы (79) вытекает равенство (12) для всех $r \in \mathcal{R}_\alpha^{(1)}$. Ясно, что тогда равенство (12) справедливо и для всех $r \in -\mathcal{R}_\alpha^{(1)}$.

Итак, пусть r – произвольный элемент из $\mathcal{R}_\alpha^{(1)} \setminus \Lambda$. Рассмотрим все соотношения вида

$$\sum_{i=1}^{|\Lambda|} \tilde{\lambda}_i \vec{v}_i + r\vec{u} = \vec{0}, \quad (80)$$

где коэффициенты векторов $\vec{v}_i, \vec{u} \in \mathbb{Z}^d$ не превосходят по модулю числа s и строки матрицы

$$M_1 = \begin{pmatrix} v_1^{(1)} & \dots & v_{|\Lambda|}^{(1)} & u^{(1)} \\ \dots & \dots & \dots & \dots \\ v_1^{(d)} & \dots & v_{|\Lambda|}^{(d)} & u^{(d)} \end{pmatrix}$$

обладают тем свойством, что для любого $i \in [d]$ выполнено $\sum_{j=1}^{|\Lambda|} |v_j^{(i)}| + |u^{(i)}| \leq k$. Если ранг любой такой матрицы M_1 строго меньше d , то мы получаем противоречие с максимальностью множества Λ . Значит, существует соотношение вида (80) такое, что ранг матрицы M_1 равен d . Принимая во внимание уравнение (80), легко видеть, что ранг соответствующей матрицы M , составленной из первых $|\Lambda|$ столбцов матрицы M_1 , тоже равен d . Как было показано выше, отсюда вытекает справедливость равенства (12).

Получим оценку

$$|\Lambda^*| \leq \max \left\{ 2^{12+4d(\log(1/\delta))^{-1}} \left(\frac{\delta}{\alpha} \right)^2 \log \left(\frac{1}{\delta} \right), 8 \log^2 \left(\frac{1}{\delta} \right) \right\}.$$

Если $|\Lambda| \leq k^2$, то $|\Lambda| \leq \log^2(1/\delta)$ и, следовательно, $|\Lambda^*| \leq 8 \log^2(1/\delta)$. Если же $|\Lambda| > k^2$, то по предложению 3.2 имеем $T_k(\Lambda) \leq 2^{5k+2d} k^k |\Lambda|^k$. С другой стороны, применяя теорему 1.3, получаем $T_k(\Lambda) \geq \delta \alpha^{2k} |\Lambda|^{2k} / (2^{4k} \delta^{2k})$. Отсюда

$$|\Lambda| \leq 2^{9+4d(\log(1/\delta))^{-1}} \left(\frac{\delta}{\alpha} \right)^2 \log \left(\frac{1}{\delta} \right)$$

и, следовательно,

$$|\Lambda^*| \leq 2^{12+4d(\log(1/\delta))^{-1}} \left(\frac{\delta}{\alpha} \right)^2 \log \left(\frac{1}{\delta} \right).$$

В любом случае

$$|\Lambda^*| \leq \max \left\{ 2^{12+4d(\log(1/\delta))^{-1}} \left(\frac{\delta}{\alpha} \right)^2 \log \left(\frac{1}{\delta} \right), 8 \log^2 \left(\frac{1}{\delta} \right) \right\}.$$

Теперь докажем существование множества $\tilde{\Lambda}$. Пусть $s = \lceil \log \log(1/\delta) \rceil$ и Λ_1 – максимальное подмножество $\mathcal{R}_\alpha^{(1)}$, принадлежащее семейству $\Lambda_d(2k, s)$. Пусть

$$\tilde{\Lambda} = \left(\bigcup_{j=1}^s j^{-1} \Lambda_1 \right) \sqcup \left(- \bigcup_{j=1}^s j^{-1} \Lambda_1 \right).$$

Тогда $|\tilde{\Lambda}| \leq 2s|\Lambda_1|$. Применяя рассуждения, аналогичные приведенным выше, легко показать, что для любого вычета $r \in \mathcal{R}_\alpha$ существует матрица

$$\tilde{M} = (\tilde{m}_{ij})_{i \in [d], j \in [\tilde{\Lambda}]}$$

ранга d такая, что для любого $i \in [d]$ выполнено $\sum_{j=1}^{|\tilde{\Lambda}|} |\tilde{m}_{ij}| \leq 4 \log(1/\delta)$ и для всех $i \in [d]$ справедливо равенство (14).

Докажем неравенство (13). Если $|\Lambda_1| \leq k^{s/(s-1)}$, то $|\Lambda_1| \leq 2^4 \log(1/\delta)$ и $|\tilde{\Lambda}| \leq 2s|\Lambda_1| \leq 2^5 \log(1/\delta) \log \log(1/\delta)$. Мы видим, что в этом случае неравенство (13) доказано. Пусть теперь $|\Lambda_1| > k^{s/(s-1)}$. Применяя утверждение 3.2, находим $T_k(\Lambda_1) \leq 2^{5k} (2 \log \log(1/\delta))^d k^k |\Lambda_1|^k$. С другой стороны, из теоремы 1.3 вытекает, что $T_k(\Lambda_1) \geq \delta \alpha^{2k} |\Lambda_1|^{2k} / (2^{4k} \delta^{2k})$. Отсюда

$$|\Lambda_1| \leq 2^{9+2d \log(2 \log \log(1/\delta))(\log(1/\delta))^{-1}} \left(\frac{\delta}{\alpha}\right)^2 \log\left(\frac{1}{\delta}\right)$$

и, следовательно,

$$|\tilde{\Lambda}| \leq 2^{10+2d \log(2 \log \log(1/\delta))(\log(1/\delta))^{-1}} \left(\frac{\delta}{\alpha}\right)^2 \log\left(\frac{1}{\delta}\right) \log \log\left(\frac{1}{\delta}\right).$$

Теорема доказана.

§ 4. Примеры множеств больших тригонометрических сумм в линейных пространствах над полем простой характеристики

Пусть p – простое число, n и N – натуральные числа, $N = p^n$. Рассмотрим конечную абелеву группу $\mathbb{Z}_p^n = (\mathbb{Z}/p\mathbb{Z})^n$, $|\mathbb{Z}_p^n| = N$. Группа $\mathbb{Z}_p^n$ является векторным пространством со скалярным произведением

$$\vec{x} \cdot \vec{y} = \langle \vec{x}, \vec{y} \rangle = x_1 y_1 + \dots + x_n y_n \pmod{p}.$$

Преобразование Фурье функции f , $f: \mathbb{Z}_p^n \rightarrow \mathbb{C}$, задается формулой

$$\hat{f}(\vec{r}) = \sum_{\vec{x} \in \mathbb{Z}_p^n} f(\vec{x}) e(-(\vec{r} \cdot \vec{x})),$$

где $e(x) = e^{2\pi i x/p}$, $x \in \mathbb{Z}_p$.

Понятия множества Бора и многомерной арифметической прогрессии в группах $\mathbb{Z}_p^n$ совпадают между собой. Всем этим объектам соответствует аффинное подпространство. Пусть $\vec{v}_1, \dots, \vec{v}_k$ – некоторые линейно независимые векторы, и пусть $\varepsilon_1, \dots, \varepsilon_k$ – произвольные элементы $\mathbb{Z}_p$. Аффинным подпространством *к-размерности* k называется множество

$$P = P_{\varepsilon_1, \dots, \varepsilon_k} = \{ \vec{x} \in \mathbb{Z}_p^n : \langle \vec{x}, \vec{v}_1 \rangle = \varepsilon_1, \dots, \langle \vec{x}, \vec{v}_k \rangle = \varepsilon_k \}.$$

Коэффициенты Фурье множества P вычисляются чрезвычайно просто. Пусть L – линейное пространство размерности k , натянутое на векторы $\vec{v}_1, \dots, \vec{v}_k$, и $\vec{r} \in \mathbb{Z}_p^n$ – произвольный вектор. Пусть также $L^\perp$ – подпространство $\mathbb{Z}_p^n$, ортогональное пространству L . Имеем $\vec{r} = \sum_{i=1}^k r_i \vec{v}_i + \vec{v}$, где $\vec{v} \in L^\perp$. Тогда

$$\hat{P}(\vec{r}) = L(\vec{r})|P|e\left(-\sum_{i,j=1}^k \varepsilon_i r_j \langle \vec{v}_i, \vec{v}_j \rangle\right). \quad (81)$$

Таким образом, $|\hat{P}(\vec{r})|$ либо нуль, либо равен $|P|$.

В этом параграфе мы ограничимся случаем $p = 2$, т.е. рассмотрим группу $\mathbb{Z}_2^n$. Если $p = 2$, то преобразование Фурье функции f , $f: \mathbb{Z}_2^n \rightarrow \mathbb{C}$, вычисляется по формуле

$$\widehat{f}(\vec{r}) = \sum_{\vec{x} \in \mathbb{Z}_p^n} (-1)^{\langle \vec{r}, \vec{x} \rangle} f(\vec{x}).$$

Прежде всего докажем аналог теоремы 2.11. Очень удобно разбить наши результаты на две теоремы 4.1 и 4.3. Теорема 4.1 более простая и в ее доказательстве более четко прослеживается основная идея, хотя ограничение (82) на параметры δ и α достаточно обременительно.

ТЕОРЕМА 4.1. Пусть $\delta, \alpha \in (0, 1]$ – вещественные числа, $\alpha \leq \delta/2$, $\delta \leq 2^{-5}$ и

$$\frac{2\delta}{\alpha} \log \frac{1}{2\alpha} \leq \log N. \quad (82)$$

Тогда найдется множество $A \subseteq \mathbb{Z}_2^n$ такое, что $\delta N \leq |A| \leq 8\delta N$, $|\mathcal{R}_\alpha(A)| \geq \delta/(8\alpha^2)$ и для всех k , $2 \leq k \leq 2^{-1} \log(1/(8\delta))$, выполнено $T_k(\mathcal{R}_\alpha(A)) \leq 8\delta/(\alpha^{2k})$.

ДОКАЗАТЕЛЬСТВО. Пусть

$$\begin{aligned} \vec{e}_1 &= (1, 0, \dots, 0), \\ \vec{e}_2 &= (0, 1, \dots, 0), \\ &\dots\dots\dots \\ \vec{e}_n &= (0, \dots, 0, 1) \end{aligned}$$

– базис $\mathbb{Z}_2^n$. Пусть также $k' = \lceil \log(1/(2\alpha)) \rceil$, $t = \lceil \delta/\alpha \rceil$, $n = \log N$. Пусть аффинное подпространство P_i , $i \in [t]$, имеет следующий вид:

$$P_i = \{ \vec{x} \in \mathbb{Z}_2^n : \langle \vec{x}, \vec{e}_j \rangle = 0, j = (i-1)k' + 1, \dots, ik' \}.$$

Так как $tk' \leq (2\delta/\alpha) \log(1/(2\alpha)) \leq \log N = n$, то подпространства P_i корректно определены. Пусть $A = \bigcup_{i=1}^t P_i$. Ясно, что $|A| \leq t2^{-k'}N \leq 8\delta N$. Докажем, что $|A| \geq \delta N$. Имеем $|P_i| = N2^{-k'}$, $i \in [t]$. Кроме того, для любого $l \in [t]$ и любых различных подпространств $P_{i_1}, \dots, P_{i_l}$ выполнено

$$|P_{i_1} \cap \dots \cap P_{i_l}| = N2^{-k'l}. \quad (83)$$

Применяя формулу включения–исключения и оценку $\delta \leq 2^{-5}$, находим

$$|A| \geq \sum_{i=1}^t |P_i| - \sum_{i,j=1, i \neq j}^t |P_i \cap P_j| \geq t2^{-k'}N - t^2(2^{-k'})^2N = t2^{-k'}N \left(1 - \frac{t}{2^{k'}}\right) \geq \delta N.$$

Докажем теперь, что $|\mathcal{R}_\alpha(A)| \geq \delta/(8\alpha^2)$. Пусть L_i – подпространство $\mathbb{Z}_2^n$ размерности k' , натянутое на векторы $\{\vec{e}_j\}_{j=(i-1)k'+1, \dots, ik'}$. Пусть $\vec{s} \in \mathbb{Z}_2^n$ – произвольный вектор. Применяя формулу (81), получаем

$$\widehat{P}_i(\vec{s}) = |P_i|L_i(\vec{s}). \quad (84)$$

Отсюда $\mathcal{R}_\alpha(A) \subseteq \bigcup_{i=1}^t L_i$. Докажем, что $\bigcup_{i=1}^t L_i \subseteq \mathcal{R}_\alpha(A)$. Очевидно, что $\vec{0} \in \mathcal{R}_\alpha(A)$. Пусть $\vec{s}$ – произвольный ненулевой вектор, принадлежащий некоторому L_i . Ясно, что для любых $i, j \in [t]$, $i \neq j$, выполнено $L_i \cap L_j = \{\vec{0}\}$. Используя это соображение, формулу включения-исключения и (84), находим

$$\widehat{A}(\vec{s}) = \widehat{P}_i(\vec{s}) - \sum_{j=1}^t (P_i \cap P_j)^\wedge(\vec{s}) + \sum_{j,l=1, j \neq l, j, l \neq i}^t (P_i \cap P_j \cap \widehat{P}_l)(\vec{s}) + \dots \quad (85)$$

Применяя формулы (83) и (85), получаем

$$|\widehat{A}(\vec{s})| \geq 2^{-k'} N - 2^{-k'} N \left(\frac{t}{2^{k'}} + \frac{t^2}{(2^{k'})^2} + \dots \right) \geq 2^{-k'-1} N \geq \alpha N. \quad (86)$$

Следовательно, $\bigcup_{i=1}^t L_i \subseteq \mathcal{R}_\alpha(A)$ и $|\mathcal{R}_\alpha(A)| \geq \sum_{i=1}^t |L_i| - t \geq t2^{k'} - t \geq \delta/(8\alpha^2)$.

Наконец докажем, что для всех $2 \leq k \leq 2^{-1} \log(1/(8\delta))$ выполнено неравенство $T_k(\mathcal{R}_\alpha(A)) \leq 8\delta/(\alpha^{2k})$. Рассмотрим уравнение

$$r_1 + \dots + r_k = r'_1 + \dots + r'_k, \quad (87)$$

где все векторы r_j, r'_j принадлежат $\mathcal{R}_\alpha(A)$. Выше было отмечено, что $\mathcal{R}_\alpha(A) \subseteq \bigcup_{i=1}^t L_i$. Следовательно, каждый вектор из (87) принадлежит некоторому подпространству L_{j_i} . Пусть z – целое неотрицательное число и $s_1, \dots, s_l$ – натуральные числа такие, что $s_1 + \dots + s_l + z = 2k$. Можно считать для определенности набор $s_1, \dots, s_l$ упорядоченным по убыванию $s_1 \geq s_2 \geq \dots \geq s_l \geq 1$. Пусть $E(s_1, \dots, s_l, z)$ – множество таких решений $r_1, \dots, r_k, r'_1, \dots, r'_k$ уравнения (87), что среди r_j, r'_j существует ровно z нулей, существует ровно s_1 ненулевых векторов, принадлежащих некоторому подпространству L_{j_1} , существует ровно s_2 ненулевых векторов, принадлежащих некоторому подпространству L_{j_2} , ..., существует ровно s_l ненулевых векторов, принадлежащих некоторому подпространству L_{j_l} , и при этом все подпространства $L_{j_1}, L_{j_2}, \dots, L_{j_l}$ различные. Имеем

$$\begin{aligned} T_k(\mathcal{R}_\alpha(A)) &= \sum_{l=0}^{2k} \sum_{z=0}^{2k} \sum_{\substack{s_1, \dots, s_l \\ s_1 + \dots + s_l + z = 2k}} |E(s_1, \dots, s_l, z)| \\ &= 1 + t(2^{k'})^{2k-1} + \sum_{l=2}^{2k} \sum_{z=0}^{2k} \sum_{\substack{s_1, \dots, s_l \\ s_1 + \dots + s_l + z = 2k}} |E(s_1, \dots, s_l, z)|. \end{aligned} \quad (88)$$

Зафиксируем $s_1, \dots, s_l, z$ и рассмотрим решения уравнения (87), принадлежащие фиксированным подмножествам $L_{j_1}, \dots, L_{j_l}$. Обозначим множество этих решений через $E(s_1, \dots, s_l, z)(L_{j_1}, \dots, L_{j_l})$. Перепишем уравнение (87) в виде

$$\vec{u}_1 + \dots + \vec{u}_l = \vec{0}, \quad (89)$$

где $\vec{u}_i \in L_{j_i}$, $i \in [l]$. Так как для всех $i, h \in [t]$, $i \neq h$, выполнено

$$\{\vec{e}_\beta\}_{\beta=(j_i-1)k'+1, \dots, j_i k'} \cap \{\vec{e}_\gamma\}_{\gamma=(j_h-1)k'+1, \dots, j_h k'} = \emptyset,$$

то все $\vec{u}_i$ равны $\vec{0}$. Следовательно, для мощности $E(s_1, \dots, s_l, z)(L_{j_1}, \dots, L_{j_l})$ справедлива оценка

$$\begin{aligned} |E(s_1, \dots, s_l, z)(L_{j_1}, \dots, L_{j_l})| &\leq \frac{(2k)!}{s_1! \dots s_l! z!} (2^{k'})^{s_1-1} \dots (2^{k'})^{s_l-1} \\ &\leq \frac{(2k)!}{s_1! \dots s_l! z!} (2^{k'})^{2k-l}. \end{aligned}$$

Отсюда

$$|E(s_1, \dots, s_l, z)| \leq \binom{t}{l} \frac{(2k)!}{s_1! \dots s_l! z!} (2^{k'})^{2k-l} \leq \frac{t^l}{l!} \cdot \frac{(2k)!}{s_1! \dots s_l! z!} (2^{k'})^{2k-l}. \quad (90)$$

Подставляя оценку (90) в формулу (88), находим

$$\begin{aligned} T_k(\mathcal{R}_\alpha(A)) &\leq 2t(2^{k'})^{2k-1} + \sum_{l=2}^{2k} \frac{t^l}{l!} (2^{k'})^{2k-l} \sum_{z=0}^{2k} \sum_{\substack{s_1, \dots, s_l \\ s_1 + \dots + s_l + z = 2k}} \frac{(2k)!}{s_1! \dots s_l! z!} \\ &\leq 2t(2^{k'})^{2k-1} + \sum_{l=2}^{2k} \frac{t^l}{l!} (2^{k'})^{2k-l} (l+1)^{2k} \\ &= 2t(2^{k'})^{2k-1} + (2^{k'})^{2k} \sum_{l=2}^{2k} \left(\frac{t}{2^{k'}} \right)^l (l+1)^{2k} \frac{1}{l!}. \end{aligned} \quad (91)$$

Рассмотрим функцию $f(l) = (t/(2^{k'}))^l (l+1)^{2k}$. Взяв производную, получаем, что максимальное значение этой функции достигается при $l_0 = 2k/\ln(2^{k'}/t) - 1$, а для всех $l \geq l_0$ функция $f(l)$ монотонно убывает. По условию для k верно $k \leq 2^{-1} \log(1/(8\delta))$. Отсюда $l_0 \leq 1$. Следовательно,

$$\begin{aligned} T_k(\mathcal{R}_\alpha(A)) &\leq 2t(2^{k'})^{2k-1} + 2^{2k} t (2^{k'})^{2k-1} \leq 2^{2k+1} t (2^{k'})^{2k-1} \\ &\leq 2^{2k+1} \frac{2\delta}{\alpha} \left(\frac{1}{2\alpha} \right)^{2k-1} = \frac{8\delta}{\alpha^{2k}}. \end{aligned}$$

Теорема доказана.

ЗАМЕЧАНИЕ 4.2. Ограничение на число k вида $k \ll \log(1/\delta)$ в теореме 4.1 возникло из-за того, что область значений параметров δ и α в этой теореме достаточно широка. Если параметры δ и α выбраны специальным образом, то можно добиться того, чтобы никаких ограничений на k не было. Действительно, пусть $\alpha \approx \delta$, и пусть A – подпространство $\mathbb{Z}_2^n$ коразмерности k' , $k' \approx \log(1/\delta)$. Тогда множество $\mathcal{R}_\alpha(A)$ является подпространством размерности k' и имеет мощность $\approx 1/\delta$. Легко видеть, что для всех $k \geq 2$ выполнено $T_k(\mathcal{R}_\alpha(A)) = (2^{k'})^{2k-1} \approx (1/\delta)^{2k-1}$, что совпадает с оценкой (6).

Для простоты изложения в нашей следующей теореме 4.3 мы разберем лишь случай, когда $k = 2$, т.е. докажем неухудшаемость нижней оценки величины $T_2(\mathcal{R}_\alpha(A))$, полученной в теореме 1.3.

ТЕОРЕМА 4.3. Пусть $\delta, \alpha \in (0, 1]$ – вещественные числа, $32\delta^2 \leq \alpha \leq \delta/2$, $\alpha \geq N^{-2^{-300}}$, $\alpha \leq 2^{-100}$ и $(\delta/\alpha) \log(1/(2\alpha)) \geq 400 \log N \log(8 \log N)$. Тогда найдется множество $A \subseteq \mathbb{Z}_2^n$ такое, что $\delta N \leq |A| \leq 8\delta N$, $|\mathcal{R}_\alpha(A)| \geq \delta/(8\alpha^2)$ и $T_2(\mathcal{R}_\alpha(A)) \leq 16\delta/(\alpha^4)$.

Для доказательства нам понадобится широко известное неравенство Бернштейна (см. [27]) об оценках вероятностей больших отклонений суммы независимых случайных величин. Нужный нам вариант этого неравенства может быть найден в [7].

ТЕОРЕМА 4.4. Пусть $X_1, \dots, X_n$ – последовательность независимых случайных величин, каждая из которых имеет нулевое математическое ожидание $\mathbb{E}X_j = 0$ и конечный второй момент $\mathbb{E}|X_j|^2 = \sigma_j^2$. Пусть $\sigma^2 = \sigma_1^2 + \dots + \sigma_n^2$ и для всех $j \in [n]$ выполнено $|X_j| \leq 1$. Пусть, наконец, t – вещественное число такое, что $\sigma^2 \geq 6nt$. Тогда

$$\mathbb{P}\left(\left|\frac{X_1 + \dots + X_n}{n}\right| \geq t\right) \leq 4e^{-n^2 t^2 / (8\sigma^2)}.$$

С помощью теоремы 4.4 мы докажем комбинаторную лемму.

ЛЕММА 4.5. Пусть n, k, r, t – натуральные числа, $4 \leq r \leq k/2$, $2k \leq n$, удовлетворяющие неравенствам

$$kt > 288n \ln(8n), \quad t^2 \frac{2^k \binom{n-k}{k-\lceil k/r \rceil}}{\binom{n}{k}} \leq \frac{1}{2}. \quad (92)$$

Тогда найдутся множества $A_1, \dots, A_t$ из отрезка $[n]$, каждое из которых имеет мощность k , такие, что

- i) для всех $i, j \in [t]$, $i \neq j$, выполнено $|A_i \cap A_j| < k/r$;
- ii) для любого $i \in [t]$ существует не более чем $2tk^2/n$ множеств A_j , пересекающих A_i .

ДОКАЗАТЕЛЬСТВО. Пусть Ω – семейство всех подмножеств отрезка $[n]$, имеющих мощность k , $|\Omega| = \binom{n}{k} = M$. Выберем множества $A_1, \dots, A_t$ случайным образом: равномерно и независимо. Иными словами, возьмем точку из вероятностного пространства $(\Omega^t, \mathcal{B}, \mathbb{P})$, где $\mathcal{B}$ – все подмножества Ω^t и $\mathbb{P}$ – соответствующая вероятностная мера на Ω^t .

Пусть U_{ij} , $i, j \in [t]$, $i \neq j$, – событие, состоящее в том, что $|A_i \cap A_j| \geq k/r$, и пусть

$$U = \bigcup_{i, j \in [t], i \neq j} U_{ij}.$$

Легко видеть, что найдется ровно

$$\sigma := \sum_{l=\lceil k/r \rceil}^k \binom{k}{l} \binom{n-k}{k-l}$$

множеств из Ω , которые пересекают фиксированное множество A_i по не менее чем k/r точкам. Следовательно, вероятность события U_{ij} равна σ/M . Отсюда $P(U) \leq t^2 \sigma/M$.

Пусть x – произвольный элемент $[n]$ и $\xi_j^x(\omega)$, $\omega \in \Omega^t$, $j \in [t]$, – случайная величина, равная 1, если j -я компонента ω содержит x , и равная нулю в противном случае. Ясно, что величина $\xi^x(\omega) = \sum_{j=1}^t \xi_j^x(\omega)$ есть в точности число множеств A_j , содержащих x . Математическое ожидание величины ξ_j^x для всех x и j равно $E\xi_j^x = k/n$, а дисперсия – $D\xi_j^x = k/n - (k/n)^2$. Более того, случайная величина ξ^x имеет биномиальное распределение с параметрами k/n и n . Пусть V_x , $x \in [n]$, – событие, состоящее в том, что элемент x содержится в более чем $7tk/(6n)$ множествах A_j , и пусть также $V = \bigcup_{x \in [n]} V_x$. Применяя теорему 4.4, находим

$$P(V_x) \leq P\left(\omega : \left| \xi^x(\omega) - \frac{tk}{n} \right| > \frac{tk}{6n}\right) \leq 4e^{-kt/(288n)}.$$

Отсюда

$$P(V) \leq \sum_{x \in [n]} P(V_x) \leq 4ne^{-kt/(288n)}. \quad (93)$$

По условию $kt > 288n \ln(8n)$. Значит, $4ne^{-kt/(288n)} < 1/2$. Кроме того, $\sigma \leq 2^k \binom{n-k}{k-\lceil k/r \rceil}$. Снова используя условие (92) леммы и неравенство (93), находим

$$\begin{aligned} P(U \cup V) &\leq P(U) + P(V) \leq t^2 \frac{\sigma}{M} + 4ne^{-kt/(288n)} \leq t^2 \frac{2^k \binom{n-k}{k-\lceil k/r \rceil}}{\binom{n}{k}} + 4ne^{-kt/(288n)} \\ &< \frac{1}{2} + \frac{1}{2} = 1. \end{aligned}$$

Следовательно, существует набор множеств $A_1, \dots, A_t \subseteq [n]$, каждое множество мощности k , для которого выполняется свойство i) леммы и такой, что любой элемент $x \in [n]$ принадлежит не более чем $7tk/(6n) \leq 2tk/n$ множествам. Из последнего условия вытекает, что для всех $i \in [t]$ существует не более чем $2tk^2/n$ множеств A_j , пересекающих множество A_i . Действительно, в противном случае найдется элемент $a \in A_i$, принадлежащий более чем $2tk/n$ множествам A_j . Лемма доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 4.3. Пусть

$$\begin{aligned} \vec{e}_1 &= (1, 0, \dots, 0), \\ \vec{e}_2 &= (0, 1, \dots, 0), \\ &\dots\dots\dots \\ \vec{e}_n &= (0, \dots, 0, 1) \end{aligned}$$

– базис $\mathbb{Z}_2^n$. Пусть также $r = 32$, $k = \lceil \log(1/(2\alpha)) \rceil$, $t = \lceil \delta/\alpha \rceil$, $n = \log N$. По условию

$$\frac{\delta}{\alpha} \log\left(\frac{1}{2\alpha}\right) \geq 400 \log N \log(8 \log N).$$

Отсюда $kt > 288n \ln(8n)$. Кроме того, $\alpha \geq N^{-2^{-300}}$. Следовательно,

$$t^2 \frac{2^k \binom{n-k}{k - \lceil k/32 \rceil}}{\binom{n}{k}} \leq t^2 2^k \frac{k^{k/32+1}}{(n-k)^{k/32}} \leq kt^2 2^k \left(\frac{2k}{n} \right)^{k/32} \leq \frac{1}{2}$$

и все условия леммы 4.5 выполнены. Применяя эту лемму, находим семейство множеств $A_1, \dots, A_t$, удовлетворяющих условиям i) и ii).

По индукции построим семейство аффинных подпространств $P_1, \dots, P_t$. Подпространства P_i имеют следующий вид:

$$P_i = P_i^{\vec{\varepsilon}} = \{ \vec{x} \in \mathbb{Z}_2^n : \langle \vec{x}, \vec{e}_j \rangle = \varepsilon_i^{(j)}, j \in A_i \},$$

где $\vec{\varepsilon}_i = (\varepsilon_i^{(j)})$ – некоторый вектор из $\mathbb{Z}_2^k$. Таким образом, чтобы построить подпространства P_i , нам необходимо выбрать векторы $\vec{\varepsilon}_1, \dots, \vec{\varepsilon}_t$. Пусть $\vec{\varepsilon}_1 = \vec{0}$ и подпространство P_1 построено. Предположим, что у нас уже есть подпространства $P_1, \dots, P_d$. Построим вектор $\vec{\varepsilon}_{d+1}$ и подпространство P_{d+1} . Пусть $C_d = \bigcup_{i=1}^d P_i$. Ясно, что $|C_d| \leq dN2^{-k} \leq tN2^{-k} \leq 8\delta N$. Пусть вектор $\vec{\varepsilon}_{d+1}$ такой, что

$$|P_{d+1}^{\vec{\varepsilon}} \cap C_d| \leq 8\delta 2^{-k} N. \quad (94)$$

Так как

$$\sum_{\vec{\varepsilon} = (\varepsilon_i^{(j)}), j \in A_r} |C_d \cap P_{d+1}^{\vec{\varepsilon}}| = |C_d|,$$

то легко видеть, что вектор $\vec{\varepsilon}_{d+1}$ существует. Таким образом, мы построили аффинные подпространства $P_1, \dots, P_t$. Пусть $A = C_t = \bigcup_{i=1}^t P_i$. Ясно, что $|A| \leq 8\delta N$. Докажем, что $|A| \geq \delta N$. Имеем $|P_i| = N2^{-k}$, $i \in [t]$. Применяя формулу (94), находим

$$|A| = |C_t| = |C_{t-1}| + |P_t| - |C_{t-1} \cap P_t| \geq |C_{t-1}| + N2^{-k} - \frac{8\delta N}{2^k}. \quad (95)$$

Продолжим выкладку

$$\begin{aligned} |C_{t-1}| + N2^{-k} - \frac{8\delta N}{2^k} &\geq |C_{t-2}| + 2N2^{-k} - 2\frac{8\delta N}{2^k} \geq \dots \geq tN2^{-k} - t\frac{8\delta N}{2^k} \\ &= tN2^{-k}(1 - 8\delta) \geq \delta N. \end{aligned} \quad (96)$$

Докажем теперь, что $|\mathcal{R}_\alpha(A)| \geq \delta/(8\alpha^2)$. Пусть L_i – подпространство $\mathbb{Z}_2^n$ размерности k , натянутое на векторы $\{\vec{e}_j\}_{j \in A_i}$, и пусть

$$M_i = \left\{ \vec{x} \in L_i : \text{число единиц в } \vec{x} \text{ не меньше чем } \frac{k}{8} \right\}.$$

Ясно, что для всех $i \in [t]$ справедливо неравенство $|M_i| \geq 2^{k-1}$. Так как для любых $i, j \in [t]$, $i \neq j$, выполнено $|A_i \cap A_j| < k/r < k/8$, то для всех $i, j \in [t]$, $i \neq j$, имеем $M_i \cap L_j = \emptyset$. В частности, для всех $i, j \in [t]$, $i \neq j$, выполнено

$M_i \cap M_j = \emptyset$. Пусть $\vec{s} \in \mathbb{Z}_2^n$ – произвольный вектор. Применяя формулу (81), получаем

$$\widehat{P}_i(\vec{s}) = e\left(-\sum_{j \in A_i} \varepsilon_i^{(j)} s_j\right) |P_i| L_i(r). \quad (97)$$

Отсюда $\mathcal{R}_\alpha(A) \subseteq \bigcup_{i=1}^t L_i$. Докажем, что $\bigsqcup_{i=1}^t M_i \subseteq \mathcal{R}_\alpha(A)$. Пусть число $i \in [t]$ произвольное и $\vec{s} \in M_i$ – некоторый вектор. Имеем

$$\widehat{A}(\vec{s}) = \widehat{P}_t(\vec{s}) + \widehat{C}_{t-1}(\vec{s}) + \theta \frac{8\delta N}{2^k},$$

где $|\theta| \leq 1$. Действуя аналогично (95), (96), получаем

$$\widehat{A}(\vec{s}) = \sum_{l=1}^t \widehat{P}_l(\vec{s}) + \widetilde{\theta} t \frac{8\delta N}{2^k}, \quad (98)$$

где $|\widetilde{\theta}| \leq 1$. Так как для всех $i, j \in [t]$, $i \neq j$, выполнено $M_i \cap L_j = \emptyset$, то

$$\left| \sum_{l=1}^t \widehat{P}_l(\vec{s}) \right| = |\widehat{P}_i(\vec{s})| = N 2^{-k}. \quad (99)$$

Применяя формулы (98), (99) и неравенство $\alpha \geq 32\delta^2$, находим

$$|\widehat{A}(\vec{s})| \geq N 2^{-k} - t \frac{8\delta N}{2^k} = \frac{N}{2^k} (1 - 8\delta t) \geq \alpha N.$$

Следовательно, $\bigsqcup_{i=1}^t M_i \subseteq \mathcal{R}_\alpha(A)$ и $|\mathcal{R}_\alpha(A)| \geq t 2^{k-1} \geq \delta / (8\alpha^2)$.

Наконец докажем, что $T_2(\mathcal{R}_\alpha(A)) \leq 16\delta / (\alpha^4)$. Рассмотрим уравнение

$$\vec{r}_1 + \vec{r}_2 = \vec{r}_3 + \vec{r}_4, \quad (100)$$

где все $\vec{r}_l$, $l = 1, 2, 3, 4$, принадлежат $\mathcal{R}_\alpha(A)$. Выше было отмечено, что $\mathcal{R}_\alpha(A) \subseteq \bigcup_{i=1}^t L_i$. Следовательно, каждый вектор $\vec{r}_l$ принадлежит некоторому подпространству L_{i_l} . Пусть $M = \bigsqcup_{i=1}^t M_i$ и $Q = (\bigcup_{i=1}^t L_i) \setminus M$. Для любого $i \in [t]$ справедливо неравенство

$$|L_i \setminus M_i| = \sum_{l=0}^{[k/8]} \binom{k}{l} \leq \frac{k}{8} \binom{k}{[k/8]} + 1. \quad (101)$$

Отсюда

$$|Q| \leq \sum_{i=1}^t |L_i \setminus M_i| \leq \frac{kt}{8} \binom{k}{[k/8]} + t \leq \frac{kt}{4} \binom{k}{[k/8]}. \quad (102)$$

По условию $\alpha \geq 32\delta^2$. Следовательно,

$$t^2 \leq \frac{4\delta^2}{\alpha^2} \leq 8 \cdot 2^k. \quad (103)$$

Так как $\alpha \leq 2^{-100}$, то $k \geq \log(1/(2\alpha)) - 1 \geq 50$. Применяя эту оценку, формулу Стирлинга и неравенства (102), (103), находим

$$T_2(Q) \leq |Q|^3 \leq \frac{k^3 t^3}{4^3} \left(\frac{k}{[k/8]} \right)^3 \leq \frac{k^3 t^3}{4^3} \left(\frac{8^2}{\sqrt{14\pi k}} \cdot \frac{8^k}{7^{7k/8}} \right)^3 \leq \frac{t}{8} (2^k)^3. \quad (104)$$

При выводе последнего неравенства мы пользовались оценкой

$$\left(\frac{k}{14\pi} \right)^{3/2} 8^6 \leq \left(\frac{7^{21/8}}{128} \right)^k,$$

верной для всех $k \geq 50$. Из неравенства (104) вытекает формула

$$\begin{aligned} T_2(\mathcal{R}_\alpha(A)) &\leq T_2(M \sqcup Q) = \frac{1}{N} \sum_{\vec{r} \in \mathbb{Z}_2^n} |\widehat{M}(r) + \widehat{Q}(r)|^4 \\ &\leq \frac{8}{N} \sum_{\vec{r} \in \mathbb{Z}_2^n} |\widehat{M}(r)|^4 + \frac{8}{N} \sum_{\vec{r} \in \mathbb{Z}_2^n} |\widehat{Q}(r)|^4 \\ &\leq 8T_2(M) + 8T_2(Q) \leq 8T_2(M) + t(2^k)^3. \end{aligned} \quad (105)$$

Таким образом, чтобы оценить величину $T_2(\mathcal{R}_\alpha(A))$ сверху, нам необходимо получить оценку для $T_2(M)$.

Итак, пусть векторы $\vec{r}_l$ принадлежат некоторым M_{i_l} . Так как для всех $i, j \in [t]$, $i \neq j$, выполнено $|A_i \cap A_j| < k/r$ и $3k/r = 3k/32 < k/8$, то легко видеть, что среди множеств M_{i_l} , $l = 1, 2, 3, 4$, нет множества, не совпадающего ни с одним из трех оставшихся. Таким образом, возможны лишь четыре ситуации:

- 1) $i_1 = i_2 = i_3 = i_4$;
- 2) $i_1 = i_3$, $i_2 = i_4$ и $i_1 \neq i_2$;
- 3) $i_1 = i_4$, $i_2 = i_3$ и $i_1 \neq i_2$;
- 4) $i_1 = i_2$, $i_3 = i_4$ и $i_1 \neq i_3$.

В первом случае число решений уравнения (100) не превосходит $t(2^k)^3$. Рассмотрим вторую возможность (случаи 3) и 4) разбираются аналогично). Зафиксируем i_1 и i_2 , $i_1 \neq i_2$. Пусть $\vec{u} = \vec{r}_1 - \vec{r}_3 = \vec{r}_4 - \vec{r}_2$. Ясно, что $\vec{u} \in L_{i_1} \cap L_{i_2}$. Если $A_{i_1} \cap A_{i_2} = \emptyset$, то $\vec{u} = \vec{0}$ и $\vec{r}_1 = \vec{r}_3$, $\vec{r}_2 = \vec{r}_4$. Следовательно, в случае, когда $A_{i_1} \cap A_{i_2} = \emptyset$, уравнение (100) имеет не более чем $(2^k)^2$ решений. Пусть теперь $A_{i_1} \cap A_{i_2} \neq \emptyset$. Так как $|A_{i_1} \cap A_{i_2}| < k/r$, то число решений уравнения (100) не превосходит $(2^k)^2 2^{k/r}$. Отсюда число решений (100) в ситуации 2) не больше чем

$$\sum_{i_1=1}^t \sum_{\substack{i_2=1, i_2 \neq i_1 \\ A_{i_1} \cap A_{i_2} = \emptyset}}^t (2^k)^2 + \sum_{i_1=1}^t \sum_{\substack{i_2=1, i_2 \neq i_1 \\ A_{i_1} \cap A_{i_2} \neq \emptyset}}^t (2^k)^2 2^{k/r} := \sigma_1.$$

По свойству ii) семейства множеств $A_1, \dots, A_t$ число значений $i_2 \neq i_1$ таких, что $A_{i_1} \cap A_{i_2} \neq \emptyset$, не превосходит $2tk^2/n$. Отсюда

$$\sigma_1 \leq t^2 (2^k)^2 + t \frac{2tk^2}{n} (2^k)^2 2^{k/32}.$$

Применяя последнее неравенство и оценку $\alpha \geq 32\delta^2$, находим

$$\sigma_1 \leq t(2^k)^3 + t(2^k)^3 = 2t(2^k)^3.$$

Следовательно, общее число решений уравнения (100) не превосходит

$$\begin{aligned} T_2(\mathcal{R}_\alpha(A)) &\leq 8(t(2^k)^3 + 2t(2^k)^3 + 2t(2^k)^3 + 2t(2^k)^3) + t(2^k)^3 = 57t(2^k)^3 \\ &\leq 57 \frac{2\delta}{\alpha} \cdot \frac{1}{(2\alpha)^3} \leq \frac{16\delta}{\alpha^4}. \end{aligned}$$

Теорема доказана.

Итак, как показывают теоремы 4.1, 4.3, оценка теоремы 1.3 является неулучшаемой. Легко видеть, что число элементов λ_i^* в представлении (8) теоремы 1.4 также не может быть уменьшено. Действительно, пусть $\alpha \approx \delta$, и пусть A – подмножество $\mathbb{Z}_2^n$, для которого $|\mathcal{R}_\alpha(A)| \approx \delta/\alpha^2 \approx 1/\delta$. Такие множества A существуют, например можно взять в качестве A любое подпространство $\mathbb{Z}_2^n$ мощности δN . Тогда по теореме Чанг найдется множество Λ^* , $|\Lambda^*| \ll \log(1/\delta)$, такое, что для любого элемента $\vec{r} \in \mathcal{R}_\alpha(A)$ справедливо представление (8). Так как $|\mathcal{R}_\alpha(A)| \approx 1/\delta$, то легко видеть, что существует вектор $\vec{r} \in \mathcal{R}_\alpha(A)$, для представления в виде (8) которого необходимо $k \gg \log(1/\delta)$ векторов. Действительно, так как линейных комбинаций, натянутых на произвольные k векторов из Λ^* , не более чем $2^k \binom{|\Lambda^*|}{k}$, то должно выполняться неравенство $2^k \binom{|\Lambda^*|}{k} \gg 1/\delta$, из которого и вытекает оценка $k \gg \log(1/\delta)$.

Список литературы

- [1] W. T. Gowers, “Rough structure and classification”, *GAFA*, Special Volume – GAFA2000 “Visions in Mathematics” (Tel Aviv, 1999), Part I, 79–117.
- [2] M. B. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets*, Grad. Texts in Math., Springer-Verlag, New York, 1996.
- [3] M.-C. Chang, “A polynomial bound in Freiman’s theorem”, *Duke Math. J.*, **113**:3 (2002), 399–419.
- [4] I. Z. Ruzsa, “Generalized arithmetical progressions and sumsets”, *Acta Math. Hungar.*, **65**:4 (1994), 379–388.
- [5] Yu. Bilu, “Structure of sets with small sumset”, *Structure theory of set addition*, Astérisque, **258**, Soc. Math. France, Paris, 1999, 77–108.
- [6] Г. А. Фрейман, *Начала структурной теории сложения множеств*, Казан. гос. пед. ин-т, Казань, 1966; англ. пер.: G. A. Freiman, *Foundations of a structural theory of set addition*, Transl. Math. Monogr., **37**, Providence, RI, Amer. Math. Soc., 1973.
- [7] B. Green, “Arithmetic progressions in sumsets”, *Geom. Funct. Anal.*, **12**:3 (2002), 584–597.
- [8] T. Schoen, “Linear equations in $\mathbb{Z}_p$ ”, *Bull. London Math. Soc.*, **37**:4 (2005), 495–501.
- [9] А. А. Юдин, “Теория чисел”, *Теоретико-числовые исследования по спектру Маркова и структурной теории сложения множеств*, ред. Г. А. Фрейман, А. М. Рубинов, Е. В. Новоселов, Изд-во КГУ, М., 1973, 163–174.
- [10] A. Besser, “Sets of integers with large trigonometric sums”, *Structure theory of set addition*, Astérisque, **258**, Soc. Math. France, Paris, 1999, 35–76.

- [11] V. F. Lev, “Linear equations over $\mathbb{F}_p$ and moments of exponential sums”, *Duke Math. J.*, **107**:2 (2001), 239–263.
- [12] S. V. Konyagin, V. F. Lev, “On the distribution of exponential sums”, *Integers*, **0**:A1 (2000), electronic only.
- [13] B. Green, “Some constructions in the inverse spectral theory of cyclic groups”, *Combin. Probab. Comput.*, **12**:2 (2003), 127–138.
- [14] И. Д. Шкредов, “О множествах больших тригонометрических сумм”, *Докл. РАН*, **411**:4 (2006), 455–459; англ. пер.: I. D. Shkredov, “On sets of large exponential sums”, *Russian Acad. Sci. Dokl. Math.*, **74**:3 (2006), 860–864.
- [15] И. Д. Шкредов, “О множествах больших тригонометрических сумм”, *Изв. РАН. Сер. матем.* (в печати).
- [16] W. Rudin, *Fourier analysis on groups*, Wiley Classics Lib., Wiley, New York, 1990.
- [17] B. Green, “A Szemerédi-type regularity lemma in Abelian groups, with applications”, *Geom. Funct. Anal.*, **15**:2 (2005), 340–376.
- [18] J. Bourgain, “On triples in arithmetic progression”, *Geom. Funct. Anal.*, **9**:5 (1999), 968–984.
- [19] B. Green, “Finite field models in additive combinatorics”, *Surveys in combinatorics 2005*, Papers from the 20th British combinatorial conference (Durham, UK, 2005), London Math. Soc. Lecture Note Ser., **327**, Cambridge Univ. Press, Cambridge, 2005, 1–27.
- [20] K. de Leeuw, Y. Katznelson, J.-P. Kahane, “Sur les coefficients de Fourier des fonctions continues”, *C. R. Acad. Sci. Paris Sér. A-B*, **285**:16 (1977), 1001–1003.
- [21] 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.
- [22] K. Ball, “Convex geometry and functional analysis”, *Handbook of the geometry of Banach spaces. Vol. I*, Elsevier, North-Holland, Amsterdam, 2001, 161–194.
- [23] J. Spencer, “Six standard deviations suffice”, *Trans. Amer. Math. Soc.*, **289**:2 (1985), 679–706.
- [24] B. Green, “Structure theory of set addition”, *ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis* (Edinburgh, 2002), 2002.
- [25] I. Z. Ruzsa, “Arithmetic progressions in sumsets”, *Acta Arith.*, **60**:2 (1991–1992), 191–202.
- [26] B. Bajnok, I. Ruzsa, “The independence number of a subset of an Abelian group”, *Integers*, **3**:A2 (2003), electronic only.
- [27] S. Bernstein, “Sur une modification de l’inégalité de Tchebichef”, *Annal. Sci. Inst. Sav. Ukr. Sect. Math. I*, 1924, 38–49.

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

Поступила в редакцию
 11.10.2006 и 22.07.2007