ДОКЛАДЫ АКАДЕМИИ НАУК, 2006, том 411, № 4, с. 1–5

МАТЕМАТИКА

УДК 511.218+511.336

О МНОЖЕСТВАХ БОЛЬШИХ ТРИГОНОМЕТРИЧЕСКИХ СУММ

© 2006 г. И. Д. Шкредов

Представлено академиком В.В. Козловым 24.04.2006 г.

Поступило 16.05.2006 г.

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

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

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

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

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

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

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

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

Т е о р е м а 1. (Чанг). *Пусть δ, α – действительные числа, $0 < \alpha \le \delta \le 1$, A – произвольное подмножество $\mathbb{Z}_N$ мощности δN и множество $\mathcal{R}_\alpha$ определено равенством* (3).

Тогда найдется множество $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_{|\Lambda|}\} \subseteq \mathbb{Z}_N$, $|\Lambda| \le 2\left(\frac{\delta}{\alpha}\right)^2 \log_2 \frac{1}{\delta}$ такое, что всякий элемент r множества $\mathcal{R}_\alpha$ представляется в виде

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

где $\varepsilon_i \in \{-1, 0, 1\}$.

Развивая подход из [3] (см. также [4]), Чанг приложила свой результат к доказательству знаменитой теоремы Фреймана [5] о множествах с маленькой суммой. Второе приложение теоремы 1 получил Б. Грин в статье [6] (см. также более ранние работы [8, 9]). В другой работе (см. [7]) Грин показал, что в некотором смысле теорема Чанга является точной. Пусть $E = \{e_1, e_2, \ldots, e_{|E|}\} \subseteq \mathbb{Z}_N$ – произвольное множество. Обозначим через Span(E) множество всех сумм вида $\sum_{i=1}^{|E|} \varepsilon_i e_i$, где $\varepsilon_i \in \{-1, 0, 1\}$.

Т е о р е м а 2 (Грин). *Пусть δ, α – действительные числа, $\delta \le \frac{1}{8}$, $0 < \alpha \le \frac{\delta}{32}$. Пусть также $\left(\frac{\delta}{\alpha}\right)^2 \log_2(1/\delta) \le \frac{\log_2 N}{\log_2 \log_2 N}$.*

Тогда найдется множество $A \subset \mathbb{Z}_N$, $|A| = [\delta N]$ такое, что множество $\mathcal{R}_\alpha$, определенное формулой (3), *не содержится в* Span(Λ) *для любого множества Λ мощности $2^{-12}\left(\frac{\delta}{\alpha}\right)^2 \log_2\left(\frac{1}{\delta}\right)$.*

Вопрос о структуре множества $\mathcal{R}_\alpha$, когда параметр α близок к δ, изучался в работах [10–12].

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

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

$$T_k(B) := |\{(r_1, r_2, \ldots, r_k, r'_1, r'_2, \ldots, r'_k) \in B^{2k}\colon r_1 + r_2 + \ldots + r_k = r'_1 + r'_2 + \ldots + r'_k\}| \tag{5}$$

Московский государственный университет
им. М.В. Ломоносова

не меньше чем $\dfrac{\delta\alpha^{2k}|B|^{2k}}{(2^{4k}\delta^{2k})}$.

Доказательству теоремы 3 посвящен следующий раздел. Там мы сначала подробно разбираем случай $k = 2$, а затем приводим схему доказательства теоремы 3 в общей ситуации. Кроме того, мы получим несколько приложений нашего основного результата к задачам комбинаторной теории чисел, докажем результат, усиливающий теорему 1 (см. теорему 4), также будет получено приложение теоремы 3 к уже упомянутой теореме Фреймана.

ДОКАЗАТЕЛЬСТВО ОСНОВНОЙ ТЕОРЕМЫ

Мы начнем этот раздел с объяснения основной идеи доказательства теоремы 3. Пусть N – натуральное число и $\hat{A}(r)$ – коэффициенты Фурье множества A. Как мы уже говорили выше, для коэффициентов Фурье множества A справедливо равенство Парсеваля. Существуют ли еще какие-то нетривиальные соотношения между коэффициентами Фурье $\hat{A}(r)$ кроме равенства (2)? Легко видеть, что ответ на этот вопрос положительный.

Пусть $f, g: \mathbb{Z}_N \to \mathbb{C}$ – произвольные комплексные функции. Пользуясь формулой обращения

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

легко получить тождество

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

Если теперь f – характеристическая функция некоторого множества $A \subset \mathbb{Z}_N$, то формулу (7) можно переписать в виде

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

Ясно, что (8) содержит все соотношения между коэффициентами Фурье множества A. Например, равенство Парсеваля (2) получается, если в формуле (8) положить $u = 0$.

Перейдем теперь к доказательству теоремы 3. Чтобы лучше показать главную идею доказательства нашего основного результата, докажем теорему 3 отдельно для случая $k = 2$. Итак, пусть $k = 2$ и B – произвольное подмножество $\mathcal{R}_\alpha \setminus\{0\}$. Нам понадобится следующая

Л е м м а 1. *Пусть* δ, α' – *действительные числа,* $0 < \alpha' \le \delta$ *и* A – *произвольное подмножество* $\mathbb{Z}_N$ *мощности* δN. *Пусть также*

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

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

Д о к а з а т е л ь с т в о. Пусть $f_{B'}(x) = \frac{1}{N}\sum_{r \in B'} \hat{A}(r)e(rx)$. Легко видеть, что $\hat{f}_{B'}(r) = \hat{A}(r)B'(r)$. Рассмотрим сумму $\sigma = \sum_s \left|\sum_r \hat{f}_{B'}(r)\overline{\hat{A}(r-s)}\right|^2$. Применяя формулу (7) и равенство Парсеваля, находим

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

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

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

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

Кроме того,

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

Применяя неравенства (12) и (13), находим $\sigma^2 \ge \dfrac{\alpha'^8}{\delta^2}|B'|^4N^8$. Оценим величину σ^2 сверху. Имеем

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

Отсюда

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

Применяя формулу (8) и равенство Парсеваля, получаем

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

Поскольку $\hat{f}_{B'}(r) = \hat{A}(r)B'(r)$ и $B' \subseteq \mathcal{R}'_{\alpha'}\backslash\{0\}$, то $|\hat{f}_{B'}(r)| \le 2\alpha' B'(r)N$. Отсюда $\sigma_1 \le 16(\alpha')^4T_2(B')N^4$. Применяя оценки для σ_1, σ_2 и нижнюю оценку для σ^2, находим $T_2(B') \ge \frac{(\alpha')^4|B'|^4}{16\delta^3}$. Лемма 1 доказана.

Пусть

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

Ясно, что $B = \bigsqcup_{i\ge1} B_i$. Применяя лемму 1 к каждому B_i, получаем $T_2(B_i) \ge \frac{(\alpha\cdot 2^{i-1})^4|B_i|^4}{16\delta^3}$, $i \ge 1$. Отсюда

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

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

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

Подставляя оценку (18) в (17), получаем неравенство $T_2(B) \ge \frac{\alpha^4}{\delta^3 2^8}|B|^4$. Таким образом, в случае $k = 2$ теорема 3 доказана. В общей ситуации, когда $k \ge 2$ четное, мы доказываем следующий аналог леммы 1.

Л е м м а 2. *Пусть* δ, α' – *действительные числа*, $0 < \alpha' \le \delta$, A – *произвольное подмножество* $\mathbb{Z}_N$ *мощности* δN *и* $k \ge 2$ *четное. Пусть множество* $\mathcal{R}'_{\alpha'}$ *определено равенством* (9) *и* B' – *произвольное подмножество* $\mathcal{R}'_{\alpha'}\backslash\{0\}$.

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

Затем, применяя лемму 2 и проводя рассуждения, аналогичные тем, которые были применены в (16)–(18), получаем требуемую оценку. Теорема 3 доказана.

ПРИЛОЖЕНИЯ К ЗАДАЧАМ КОМБИНАТОРНОЙ ТЕОРИИ ЧИСЕЛ

В этом разделе мы докажем результат, усиливающий теорему Чанг. Наш метод доказательства и работы [13, 14] имеют много общих моментов.

Т е о р е м а 4. *Пусть* N – *натуральное число*, $(N, 6) = 1$, δ, α – *действительные числа*, $0 < \alpha \le \delta \le \frac{1}{16}$, A – *произвольное подмножество* $\mathbb{Z}_N$ *мощности* δN *и множество* $\mathcal{R}_\alpha$ *определено равенством* (3).

Тогда существует множество $\Lambda^* \subseteq \mathbb{Z}_N$, $|\Lambda|^* \le \max\left(2^{30}\left(\frac{\delta}{\alpha}\right)^2\log_2(1/\delta), 4\exp\left(4\left(\log_2\log_2\left(\frac{1}{\delta}\right)\right)^2\right)\right)$, *такое, что для любого вычета* $r \in \mathcal{R}_\alpha$ *существует набор* $\lambda_1^*, \lambda_2^*, \ldots, \lambda_M^*$ *из не более чем* $8\log_2\left(\frac{1}{\delta}\right)$ *элементов* Λ^*, *такой, что*

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

где $\varepsilon_i \in \{-1, 0, 1\}$.

Для доказательства теоремы 4 нам понадобятся несколько вспомогательных утверждений и определений.

О п р е д е л е н и е 1. Пусть k, s – натуральные числа. Рассмотрим семейство множеств $\Lambda(k, s)$ из $\mathbb{Z}_N$, обладающих следующим свойством. Если множество $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_{|\Lambda|}\}$ принадлежит семейству $\Lambda(k, s)$, из равенства

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

вытекает, что все s_i равны нулю.

Определение класса $\Lambda(k, 1)$ можно найти в статье [15]. Для множеств семейства $\Lambda(k, 3)$ справедлива следующая верхняя оценка на величину T_k.

Утверждение 1. *Пусть k – натуральное число, Λ – произвольное множество из семейства $\Lambda(k, 3)$ и справедливо неравенство $\log_2|\Lambda| \ge \log_2^2 k$.*

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

Доказательство теоремы 4. Пусть $k = 2\lceil \log_2(1/\delta) \rceil$. Пусть $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_{|\Lambda|}\}$ – максимальное подмножество $\mathcal{R}_\alpha \setminus \{0\}$, принадлежащее семейству $\Lambda(k, 3)$. Если $\mathcal{R}_\alpha = \{0\}$, то доказывать нечего. Если $\mathcal{R}_\alpha \setminus \{0\}$ непусто, то тогда и Λ непусто. Пусть $\Lambda^* = \left(\bigcup_{j=1}^{s} j^{-1}\Lambda\right) \cup \{0\}$. Тогда $|\Lambda^*| \le 4|\Lambda|$ и $0 \in \Lambda^*$. Докажем, что для любого $x \in \mathcal{R}_\alpha \setminus \{0\}$ найдется $j \in \{1, 2, \ldots, s\}$ такое, что

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

Поскольку для любых $i \in \{1, 2, \ldots, |\Lambda|\}$, $j \in \{1, 2, \ldots, s\}$ выполнено $j^{-1}\lambda_i \in \Lambda^*$, то из равенства (21) будет вытекать нужное нам утверждение. Итак, пусть x – произвольный элемент из $\mathcal{R}_\alpha \setminus \Lambda$, $x \ne 0$. Рассмотрим все соотношения вида $\sum_{i=1}^{|\Lambda|+1} \tilde{\lambda}_i s_i = 0$, где $\tilde{\lambda}_i \in \Lambda \bigsqcup \{x\}$ и $s_i \in \mathbb{Z}$, $|s_i| \le s$, $\sum_{i=1}^{|\Lambda|+1} |s_i| \le 2k$. Если все такие соотношения тривиальны, т.е. если для любого такого соотношения выполнено $s_i = 0$, $i \in \{1, 2, \ldots, |\Lambda| + 1\}$, то мы получаем противоречие с максимальностью Λ. Значит, существует нетривиальное соотношение вида (21) такое, что не все числа $s_1, s_2, \ldots, s_{|\Lambda|}, j$ равны нулю. При этом $j \in \{-s, s + 1, \ldots, s\}$. Если $j = 0$, то получаем противоречие с тем, что Λ принадлежит классу $\Lambda(k, 3)$. Следовательно, можно считать, что $j \in \{1, 2, \ldots, s\}$. Так как $2k \le 8\log_2\left(\frac{1}{\delta}\right)$, то мы получаем, что для любого элемента $x \in \mathcal{R}_\alpha$ существуют набор $\lambda_1^*, \lambda_1^*, \ldots, \lambda_M^*$ из не более чем $8\log_2\left(\frac{1}{\delta}\right)$ элементов Λ^*, такой, что выполнено равенство (19).

Нам осталось доказать оценку мощности Λ^*. Если $\log_2|\Lambda| \le (\log_2 k)^2$, то $|\Lambda| \le \exp\left(4\left(\log_2\log_2\left(\frac{1}{\delta}\right)\right)^2\right)$ и, следовательно, $|\Lambda^*| \le 4\exp\left(4\left(\log_2\log_2\left(\frac{1}{\delta}\right)\right)^2\right)$.

Если же $\log_2|\Lambda| \ge (\log_2 k)^2$, то по утверждению 1 имеем $T_k(\Lambda) \le 2^{20k}k^k|\Lambda|^k$. Кроме того, применяя теорему 3, получаем $T_k \ge \frac{\delta\alpha^{2k}|\Lambda|^{2k}}{(2^{4k}\delta^{2k})}$. Отсюда $|\Lambda| \le 2^{27}\left(\frac{\delta}{\alpha}\right)^2\log_2\left(\frac{1}{\delta}\right)$ и, следовательно, $|\Lambda^*| \le 2^{30}\left(\frac{\delta}{\alpha}\right)^2\log_2\left(\frac{1}{\delta}\right)$.

В любом случае $|\Lambda^*| \le \max(2^{30}(\delta/\alpha)^2\log_2(1/\delta)$, $4\exp\left(4\left(\log_2\log_2\left(\frac{1}{\delta}\right)\right)^2\right))$. Теорема доказана.

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

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

При доказательстве теореме Фреймана в работе [2] Чанг использовала следующее.

Предложение 1. *Пусть N – натуральное число, $\delta \in (0, 1)$ – действительное число и A – произвольное подмножество $\mathbb{Z}_N$, $|A| = \delta N$.*

Тогда $2A - 2A$ содержит множество Бора $B(K, \varepsilon)$, где $|K| \le 8\delta^{-1}\log_2(1/\delta)$ и $\varepsilon = \frac{\delta}{(2^8\log_2(1/\delta))}$.

Применяя теорему 4 и используя подход из [2], мы доказываем небольшое усиление предложения 1.

Предложение 2. *Пусть N – натуральное число, $(N, 6) = 1$, $0 < \delta \le 2^{-128}$ – действительное число и A – произвольное подмножество $\mathbb{Z}_N$, $|A| = \delta N$.*

Тогда $2A - 2A$ содержит множество Бора $B(K, \varepsilon)$, где $|K| \le 2^{33}\frac{1}{\delta}\log_2(1/\delta)$ и $\varepsilon = \frac{1}{(2^8\log_2(1/\delta))}$.

Автор выражает глубокую благодарность С.В. Конягину за его идею, позволившую усилить формулировку основного результата, а также

проф. Н.Г. Мощевитину за постоянное внимание к работе.

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

СПИСОК ЛИТЕРАТУРЫ

1. *Gowers W.T.* // Geom. Funct. Anal. 1999. Spec. V. Pt. 1. P. 79–117.
2. *Chang M.-C.* // Duke Math. J. 2002. V. 113. № 3. P. 399–419.
3. *Ruzsa I.* // Acta math. hung. 1994. V. 65. P. 379–388.
4. *Bilu Y.* // Asterisque. 1999. V. 258. P. 77–108.
5. *Фрейман Г.А.* Основания структурной теории сложения множеств. Казань: Казан. гос. пед. ин-т, 1966. 139 с.
6. *Green B.* // Combin. Probab. Comp. 2003. V. 12. № 2. P. 127–138.
8. *Bourgain J.* A Tribute of Paul Erdös. Cambridge: Cambridge Univ. Press. 1990. P. 105–109.
9. *Freiman G.A., Halberstam H., Ruzsa I.* // J. London Math. Soc. 1992. V. 46. № 2. P. 193–201.
10. *Юдин А.А.* Теория чисел М.: 1973.Калинин. гос. ун-т. С. 163–174.
11. *Besser A.* // Asterisque. 1999. V. 258. P. 35–76.
12. *Lev V.F.* // Duke Math. J. 2001. V. 107. P. 239–263.
13. *Линник Ю.В.* // Мат. сб. 1943. Т. 12. В. 1. С. 28–39.
14. *Нестеренко Ю.В.* // Тр. ММО. 1985. Т. 48. С. 97–105.
15. *Bajnok B., Ruzsa I.* // Integers: Electr. J. Comb. Number Theory. 2003. V. 3. № A02.