О норме Винера подмножеств $\mathbb{Z}_p$ промежуточного размера

С. В. КОНЯГИН
Математический институт им. В. А. Стеклова РАН,
Московский государственный университет
им. М. В. Ломоносова
e-mail: konyagin@mi.ras.ru

И. Д. ШКРЕДОВ
Математический институт им. В. А. Стеклова РАН,
Институт проблем передачи информации РАН
e-mail: ilya.shkredov@gmail.com

УДК 511.321+517.518.4

Ключевые слова: преобразование Фурье, тригонометрический полином, норма Винера.

Аннотация

Доказана нижняя оценка для винеровской нормы характеристической функции подмножества A из $\mathbb{Z}_p$, p — простое число, когда $\exp\bigl((\log p/\log\log p)^{1/3}\bigr) \leqslant |A| \leqslant p/3$.

Abstract

S. V. Konyagin, I. D. Shkredov, On the Wiener norm of subsets of $\mathbb{Z}_p$ of medium size, Fundamentalnaya i prikladnaya matematika, vol. 19 (2014), no. 5, pp. 75—87.

We give a lower bound for the Wiener norm of the characteristic function of a subset A from $\mathbb{Z}_p$, where p is a prime number, in the situation where $\exp\bigl((\log p/\log\log p)^{1/3}\bigr) \leqslant |A| \leqslant p/3$.

1. Введение

Рассмотрим абелеву группу $G = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, где p — простое число. Преобразование Фурье комплексной функции на G — это новая функция, вычисляемая по формуле

$$\hat{f}(\gamma) = \frac{1}{p}\sum_{x\in G} f(x)e_p(x\gamma),$$

в которой $e_p(u) = \exp(2\pi iu/p)$ (заметим, что для $u \in \mathbb{Z}_p$ функция e_p корректно определена). Хорошо известно, что функция f может быть восстановлена по её преобразованию Фурье $\hat{f}$ с помощью формулы

$$f(x) = \sum_{\gamma\in\mathbb{Z}_p} \hat{f}(\gamma)e_p(-x\gamma). \tag{1}$$

Фундаментальная и прикладная математика, 2014, том 19, № 5, с. 75—87.

Определим винеровскую норму функции f как

$$\|f\|_{A(G)} = \|f\|_A = \|\hat{f}\|_1 = \sum_{\gamma\in\mathbb{Z}_p} |\hat{f}(\gamma)|.$$

Через χ_S, $S \subset G$, обозначим характеристическую функцию множества S.

В этой заметке мы обсудим нижние оценки винеровской нормы для функции χ_A, $A \subset \mathbb{Z}_p$, зависящие от p и $|A|$.

Если $x \in A$, то по формуле (1) имеем

$$1 = \left| \sum_{\gamma\in\mathbb{Z}_p} \hat{f}(\gamma) e_p(-x\gamma) \right| \leqslant \sum_{\gamma\in\mathbb{Z}_p} |\hat{f}(\gamma)|.$$

Таким образом, мы получаем тривиальную оценку для нормы Винера произвольного непустого подмножества $A \subset \mathbb{Z}_p$

$$\|\chi_A\|_A \geqslant 1. \tag{2}$$

Далее, поскольку

$$\|\chi_{\mathbb{Z}_p\setminus A}\|_A = \|\chi_A\|_A + \left(1 - \frac{2|A|}{p}\right),$$

достаточно рассмотреть случай $|A| < p/2$. Легко убедиться, что если множество $A \subset \mathbb{Z}_p$ является арифметической прогрессией, такой что

$$2 \leqslant |A| < \frac{p}{2}, \tag{3}$$

то

$$\|\chi_A\|_A \asymp \log|A|.$$

Представляется весьма вероятным, что для любого A, удовлетворяющего (3), справедлива нижняя оценка

$$\|\chi_A\|_A \gg \log|A|. \tag{4}$$

Первая нетривиальная (при некоторых условиях на мощность множества) оценка для $\|\chi_A\|_A$, $|A| < p/2$, была доказана в [6]:

$$\|\chi_A\|_A \gg \frac{|A|}{p}\left(\frac{\log p}{\log\log p}\right)^{1/3}.$$

Это неравенство было затем улучшено Т. Сандерсом [8] для множеств $|A| < p/2$, таких что $|A| \gg p$. Как было показано в [3], из результатов [8] вытекает следующая теорема.

Теорема 1. *Пусть p — простое число, $A \subset \mathbb{Z}_p$, $0 < \eta = |A|/p < 1/2$. Если $\eta \geqslant (\log p)^{-1/4}(\log\log p)^{1/2}$, то*

$$\|\chi_A\|_A \gg (\log p)^{1/2}(\log\log p)^{-1}\eta^{3/2}\big(1 + \log(\eta^2(\log p)^{1/2}(\log\log p)^{-1})\big)^{-1/2},$$

а если $\eta < (\log p)^{-1/4}(\log\log p)^{1/2}$, то

$$\|\chi_A\|_A \gg \eta^{1/2}(\log p)^{1/4}(\log\log p)^{-1/2}.$$

Наш интерес в изучении норм Винера больших подмножеств $\mathbb{Z}_p$ был инициирован работой В. В. Лебедева [4], посвящённой количественным вариантам теоремы Берлинга—Хелсона.

Теорема 1 нетривиальна, только если наше множество A является большим, а именно

$$|A|p^{-1}(\log p)^{1/2}(\log\log p)^{-1} \to \infty$$

(конечно же, при условии $|A| < p/2$). Для маленьких A в [3] была доказана точная оценка.

Теорема 2. *Пусть p — простое число, $A \subset \mathbb{Z}_p$ и*

$$2 \leqslant |A| \leqslant \exp\left(\left(\frac{\log p}{\log\log p}\right)^{1/3}\right).$$

Тогда

$$\|\chi_A\|_A \gg \log|A|.$$

В этой заметке мы изучаем подмножества $A \subset \mathbb{Z}_p$ «промежуточного» размера. Сформулируем наш основной результат.

Теорема 3. *Пусть p — простое число, $A \subset \mathbb{Z}_p$,*

$$\exp\left(\left(\frac{\log p}{\log\log p}\right)^{1/3}\right) \leqslant |A| \leqslant \frac{p}{3}.$$

Тогда при $p/|A| \to \infty$ выполнено

$$\|\chi_A\|_A \gg \left(\log\frac{p}{|A|}\right)^{1/3}\left(\log\log\frac{p}{|A|}\right)^{-1+o(1)}.$$

Отметим, что, используя рассуждения из доказательства теоремы 2, можно получить аналогичные неравенства при чуть более слабых ограничениях на мощность A. Тем не менее данное улучшение является незначительным. Более того, по-видимому, указанный подход не даёт нетривиальных оценок для достаточно больших множеств, а именно таких, что $\log|A| \gg \log p$.

2. Сравнение с непрерывным случаем

Обозначим $e(u) = \exp(2\pi i u)$. Для множеств $B \subset \mathbb{Z}$ непрерывный аналог оценки (4) хорошо известен. А именно, в [2, 7] было доказано, что если $B \subset \mathbb{Z}$, $2 \leqslant |B| < \infty$, то

$$\int\limits_0^1 \left|\sum_{b\in B} e(bu)\right| du \gg \log|B|.$$

Более того, в [7] содержится более сильный результат: если $b_1 < \ldots < b_l$ — вещественные числа и c_j — произвольные комплексные числа, то

$$\int\limits_0^1 \Big| \sum_{j=1}^{l} c_j e(b_j u) \Big| \, du \gg \sum_{j=1}^{l} \frac{|c_j|}{j}. \qquad (5)$$

Из этого неравенства вытекает следующая лемма.

Лемма 4. *Пусть* $n \in \mathbb{N}$, $B \subset [-2n, 2n] \subset \mathbb{Z}$, $|B| \geqslant 2$, $0 < \eta < 1/2$, $|B \cap [-n, n]| \geqslant (1-\eta)|B|$, $c(b)$ $(b \in B)$ *— такие комплексные числа, что* $c(b) = 1$ *для* $b \in B \cap [-n, n]$. *Тогда*

$$\int\limits_0^1 \Big| \sum_{b \in B} c(b) e(bu) \Big| \, du \gg \min \left(\log \frac{1}{\eta}, \log |B| \right).$$

Доказательство. Пусть $B = \{b_1 < \ldots < b_l\}$, где $l = |B|$, и пусть также $B \cap [-n, n] = \{b_{l_1} < \ldots < b_{l_2}\}$. Перепишем тригонометрический полином $\sum\limits_{b \in B} c(b) e(bu)$ в виде $\sum\limits_{j=1}^{l} c_j e(b_j u)$, где $c_j = 1$ для $l_1 \leqslant j \leqslant l_2$. Обозначим через S интеграл

$$S = \int\limits_0^1 \Big| \sum_{b \in B} c(b) e(bu) \Big| \, du.$$

По неравенству (5) имеем

$$S \gg \sum_{j=l_1}^{l_2} \frac{1}{j} \gg \log \left(\frac{l_2 + 1}{l_1} \right).$$

Далее, $l_2 - l_1 + 1 \geqslant (1-\eta) l$. Если $\eta < 1/l$, то $l_1 = 1$, $l_2 = l$ и $S \gg \log\big((l_2+1)/l_1\big) = \log(l+1)$, как и требовалось. Если же $\eta \geqslant 1/l$, то

$$l_1 \leqslant \eta l + 1 \leqslant 2\eta l.$$

Значит,

$$\log \frac{l_2 + 1}{l_1} \geqslant \log \frac{l_1 + (1-\eta) l}{l_1} \geqslant \log \frac{1+\eta}{2\eta} \gg \log \frac{1}{\eta},$$

и мы снова получаем утверждение леммы. □

Дискретная и непрерывная L^1-нормы тригонометрических многочленов связаны друг с другом следующей леммой.

Лемма 5 [1, гл. 10, теорема 7.28]. *Справедливо неравенство*

$$\frac{1}{p} \sum_{\gamma \in \mathbb{Z}_p} \Big| \sum_{|x| \leqslant p/3} c_x e_p(x\gamma) \Big| \gg \int\limits_0^1 \Big| \sum_{|x| \leqslant p/3} c_x e(xu) \Big| \, du.$$

Неравенство (4) сразу следует из леммы 5, если $A \subset [-p/3, p/3]$ (это включение означает, что каждый вычет $a \in A$ представляется некоторым целым из $[-p/3, p/3]$) или же если некоторый невырожденный аффинный образ A из $\mathbb{Z}_p$ содержится в интервале $[-p/3, p/3]$. Подобные рассуждения были использованы в доказательстве теоремы 2.

Теперь мы определим полиномы Валле Пуссена, а также средние Валле Пуссена. Свёртка двух функций

$$F(\gamma) = \sum_{x \in \mathbb{Z}_p} c_x e_p(x\gamma), \quad G(\gamma) = \sum_{x \in \mathbb{Z}_p} d_x e_p(x\gamma)$$

задаётся формулой

$$F * G(\gamma) = \sum_{x \in \mathbb{Z}_p} c_x d_x e_p(x\gamma).$$

Легко убедиться, что

$$F * G(\gamma) = \frac{1}{p} \sum_{\xi_1 + \xi_2 = \gamma} F(\xi_1) G(\xi_2).$$

Следовательно,

$$\sum_{\gamma \in \mathbb{Z}_p} |F * G(\gamma)| \leqslant \frac{1}{p} \sum_{\gamma \in \mathbb{Z}_p} |F(\gamma)| \sum_{\gamma \in \mathbb{Z}_p} |G(\gamma)|. \tag{6}$$

Средние Валле Пуссена в $\mathbb{Z}_p$ позволяют сводить изучение произвольных тригонометрических полиномов в $\mathbb{Z}_p$ к изучению обыкновенных тригонометрических полиномов малой степени. А именно, определим полином степени $n \leqslant p/4$ по формуле

$$V_n(\gamma) = \sum_{|x| \leqslant n} e_p(x\gamma) + \sum_{n < |x| \leqslant 2n} \frac{2n - |x| + 1}{n+1} e_p(x\gamma),$$

а среднее полинома F степени $n \leqslant p/4$ — как свёртку $F * V_n$.

Нам понадобится следующая лемма.

Лемма 6. *Для любого $n \leqslant p/4$ справедливо неравенство*

$$\sum_{\gamma \in \mathbb{Z}_p} |V_n(\gamma)| \leqslant 3p.$$

Доказательство леммы содержится в доказательстве теоремы 7.28 в главе 10 книги [1].

Применяя лемму 6 и оценку (6), получаем следующий результат.

Лемма 7. *Для любого $n \leqslant p/4$ справедливо неравенство*

$$\sum_{\gamma \in \mathbb{Z}_p} \left| \sum_{|x| \leqslant n} c_x e_p(x\gamma) + \sum_{n < |x| \leqslant 2n} \frac{2n - |x| + 1}{n+1} c_x e_p(x\gamma) \right| \leqslant 3 \sum_{\gamma \in \mathbb{Z}_p} \left| \sum_{|x| \leqslant p/2} c_x e_p(x\gamma) \right|.$$

Объединение лемм 7, 5 и 4 даёт следующий результат.

Лемма 8. *Пусть* $B \subset \mathbb{Z}_p$, $n \leqslant p/6$, $0 < \eta < 1/2$. *Предположим, что* $|B \cap [-2n, 2n]| \geqslant 2$ *и*

$$|B \cap [-n, n]| \geqslant (1-\eta)|B \cap [-2n, 2n]|.$$

Тогда

$$\|\hat{\chi}_B\|_1 \gg \min\left(\log\frac{1}{\eta}, \log|B \cap [-2n, 2n]|\right).$$

3. Теорема Балога—Семереди—Гауэрса, теорема Фреймана и структура множеств с малой винеровской нормой

Для произвольного множества $Q \subset \mathbb{Z}_p$ и натурального числа k обозначим через $\mathbf{T}_k(Q)$ число решений уравнения

$$x_1 + \ldots + x_k = x'_1 + \ldots + x'_k,$$

где $x_1, \ldots, x_k, x'_1, \ldots, x'_k \in Q$. Величина $\mathbf{T}_2(Q)$ обычно называется аддитивной энергией Q (см., например, [11]). Имеем

$$\mathbf{T}_k(Q) = p^{2k-1}\sum_{\gamma}|\hat{\chi}_Q(\gamma)|^{2k}.$$

Следующая лемма является частным случаем леммы 4 из [3].

Лемма 9. *Пусть* $Q \subset A \subset \mathbb{Z}_p$, $\|\chi_A\|_A \leqslant K$, $k \in \mathbb{N}$. *Тогда*

$$\mathbf{T}_k(Q) \geqslant \frac{|Q|^{2k}}{|A|K^{2k-2}}.$$

В частности,

$$\mathbf{T}_2(A) \geqslant \frac{|A|^3}{\|\chi_A\|_A^2}. \tag{7}$$

Для подмножеств A, B некоторой абелевой группы определим их сумму и разность естественным образом:

$$A \pm B = \{a \pm b\colon a \in A,\ b \in B\}.$$

Результат ниже представляет собой текущую версию теоремы Балога—Семереди—Гауэрса [10] (см. также [5]).

Лемма 10. *Если* $G = (G, +)$ *— произвольная абелева группа,* A *— некоторое непустое подмножество* G, $\mathbf{T}_2(A) \geqslant |A|^3/L$, *то найдётся множество* $A' \subset A$, *такое что* $|A'| \gg |A|/L$ *и при этом*

$$|A' - A'| \ll L^4|A'|. \tag{8}$$

Хорошо известно, что

$$|A'|\,|A'+A'| \leqslant |A'-A'|^2$$

(см. [11, следствие 6.29]). Значит, из формулы (8) вытекает неравенство

$$|A'+A'| \ll L^8|A'|. \tag{9}$$

Другой необходимый нам важный ингредиент из аддитивной комбинаторики — это теорема Фреймана. Определим обобщённую арифметическую прогрессию как подмножество $\mathbb{Z}_p$ вида

$$P = P(x_0;\mathbf{x};\mathbf{w}) = \Big\{x_0 + \sum_{i=1}^{d} v_i x_i \colon 0 \leqslant v_i < w_i \ (i=1,\dots,d)\Big\},$$

где $\mathbf{x} = (x_1,\dots,x_d) \in \mathbb{Z}_p^d$, $\mathbf{w} = (w_1,\dots,w_d) \in \mathbb{N}^d$. Будем считать, что все x_i отличны от нуля. Число d называется размерностью P, а величина $\prod\limits_{i=1}^{d} w_i$ — объёмом P. Следующий результат представляет собой современную версию теоремы Фреймана [8].

Лемма 11. *Если B — произвольное непустое подмножество $\mathbb{Z}_p$, $|B+B| \leqslant M|B|$, $M \geqslant 2$, то найдётся обобщённая арифметическая прогрессия P размерности не больше $\log^{3+o(1)} M$ и объёма не больше $|B|$, такая что*

$$|B \cap P| \geqslant |B| \exp\bigl(-\log^{3+o(1)} M\bigr).$$

Применяя последовательно формулу (7), лемму 10 с (9) и затем лемму 11, получаем следующий результат.

Лемма 12. *Пусть $\varepsilon > 0$, $K \geqslant K(\varepsilon)$ и $A \subseteq \mathbb{Z}_p$ — произвольное непустое множество, такое что $\|\chi_A\|_A \leqslant K$. Положим*

$$d_\varepsilon = d_\varepsilon(K) = \log^{3+\varepsilon} K. \tag{10}$$

Тогда найдётся обобщённая арифметическая прогрессия P размерности, не превосходящей d_ε, и объёма не больше $|A|$, такая что

$$|A \cap P| \geqslant |A| e^{-d_\varepsilon}.$$

Нашей текущей целью является вложение подходящего аффинного образа множества с малой винеровской нормой в малый интервал из $\mathbb{Z}_p$. Для этого напомним лемму Блихфельдта [11, лемма 3.27].

Лемма 13. *Пусть $\Gamma \subset \mathbb{R}^d$ — некоторая решётка полного ранга, и пусть V — открытое множество из $\mathbb{R}^d$, такое что $\operatorname{mes}(V) > \operatorname{mes}(\mathbb{R}^d/\Gamma)$. Тогда найдутся различные $x, y \in V$, для которых $x - y \in \Gamma$.*

Пусть $P = P(x_0;\mathbf{x};\mathbf{w})$ — обобщённая арифметическая прогрессия из леммы 12, пусть также

$$\alpha_i = \frac{(|A|/p)^{1/d}}{w_i}, \quad i = 1,\dots,d,$$

$\delta > 0$ — маленькое число и, наконец,

$$V_\delta = \prod_{i=1}^{d} (-\delta, \alpha_i + \delta) \subset \mathbb{R}^d.$$

Заметим, что

$$\mathrm{mes}(V_\delta) > \prod_{i=1}^{d} \alpha_i = \frac{|A|}{p} \prod_{i=1}^{d} w_i^{-1} \geqslant \frac{1}{p}.$$

Пусть Γ — решётка

$$\Gamma = \mathbb{Z}^d + \frac{\mathbf{x}}{p}\mathbb{Z}.$$

Тогда Γ является объединением p трансляций решётки $\mathbb{Z}^d$. Следовательно, $\mathrm{mes}(\mathbb{R}^d/\Gamma) = 1/p$. Применяя теперь лемму 13, находим различные $x, y \in V_\delta$, такие что $x - y \in \Gamma$. Устремляя δ к 0, мы видим, что существуют различные точки

$$x, y \in V_0 = \prod_{i=1}^{d} [0, \alpha_i]$$

с условием $x - y \in \Gamma$. Другими словами, полагая

$$\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$$

и обозначая через $|z|$, $z \in \mathbb{Z}_p$, минимальное по модулю значение соответствующего целого числа, мы находим вычет $q \in \mathbb{Z}_p^*$, $q < p$, такой что для $i = 1, \dots, d$ выполнено $|qx_i| \leqslant p\alpha_i$.

Для всякого $x \in P$ имеем

$$|q(x - x_0)| = \left| q \sum_{i=1}^{d} v_i x_i \right| < \sum_{i=1}^{d} w_i |qx_i| \leqslant p \sum_{i=1}^{d} w_i \alpha_i = dp \left(\frac{|A|}{p} \right)^{1/d}.$$

Таким образом, мы получаем следующее структурное свойство множеств с малой винеровской нормой.

Лемма 14. *Пусть $\varepsilon > 0$, $K \geqslant K(\varepsilon)$ и A — произвольное непустое подмножество $\mathbb{Z}_p$ с $\|\chi_A\|_A \leqslant K$. Пусть число d_ε определено формулой* (10) *и*

$$m = \left[d_\varepsilon p \left(\frac{|A|}{p} \right)^{1/d_\varepsilon} \right].$$

Тогда найдутся $x_0 \in \mathbb{Z}_p$ и $q \in \mathbb{Z}_p^*$, такие что для множества

$$B = q(A - x_0) = \{q(x - x_0) \colon x \in A\}$$

выполнено

$$|B \cap [-m, m]| \geqslant |A| e^{-d_\varepsilon}.$$

4. Верхние оценки величины $T_k(Q)$ для разреженного Q

Сформулируем основной результат этого раздела.

Лемма 15. *Пусть I, k, m, M — натуральные числа. Пусть $Q = \bigsqcup\limits_{i=1}^{I} Q_i \subseteq \mathbb{Z}$ — множество, такое что*

$$Q_i \subseteq \left[-4^i m, -\frac{4^i}{2}m\right) \cup \left(\frac{4^i}{2}m, 4^i m\right],$$

$|Q_i| = M$, где i пробегает множество индексов из $\mathbb{N}$, имеющее мощность I. Тогда

$$\mathbf{T}_k(Q) \leqslant 2^{8k} k^k I^k M^{2k-1}. \tag{11}$$

Доказательство. Прежде всего положим $Q^+ = Q \cap \{x\colon x \geqslant 0\}$ и $Q^- = Q \setminus Q^+$. Применяя неравенство Гёльдера, легко получаем, что

$$\mathbf{T}_k(Q) \leqslant 4^k \max\{\mathbf{T}_k(Q^+), \mathbf{T}_k(Q^-)\}.$$

Таким образом, достаточно найти подходящую верхнюю оценку для величин $\mathbf{T}_k(Q^+)$, $\mathbf{T}_k(Q^-)$. Не ограничивая общности, мы оценим лишь $\mathbf{T}_k(Q^+)$. Более того, ниже мы пишем Q вместо Q^+.

Положим

$$N_k(x) = |\{q_1 + \ldots + q_k = x\colon q_j \in Q\}|.$$

Очевидно, что $\sum\limits_x N_k^2(x) = \mathbf{T}_k(Q)$ и

$$\sum_x N_k(x) = |Q|^k = I^k M^k.$$

В свете последней формулы достаточно доказать следующую равномерную оценку для величины $N_k(x)$.

Лемма 16. *Для произвольного x выполнено*

$$N_k(x) \leqslant 2^{6k} k^k M^{k-1}.$$

Доказательство. Рассмотрим вектор $\vec{s} = (s_1, \ldots, s_b)$, $s_1 + \ldots + s_b = k$, и положим $N_k^{\vec{s}}(x)$ равным числу решений уравнения $q_1 + \ldots + q_k = x$, таких что

$$\text{имеется } s_1 \text{ элементов из } Q_{i_1}, \ldots, \text{имеется } s_b \text{ элементов из } Q_{i_b},$$

где $i_1 < i_2 < \ldots < i_b$ и $q_1, \ldots, q_{s_1} \in Q_{i_1}$, $q_{s_1+1}, \ldots, q_{s_1+s_2} \in Q_{i_2}, \ldots$. Тогда

$$N_k(x) = \sum_{\vec{s}} N_k^{\vec{s}}(x) \cdot \frac{k!}{s_1! \ldots s_b!}. \tag{12}$$

Таким образом, нам требуется оценить величину $N_k^{\vec{s}}(x)$ для любого вектора $\vec{s}$. Поскольку

$$N_k^{\vec{s}}(x) \leqslant \sum_{q_1 \in Q_{i_1}} \ldots \sum_{q_b \in Q_{i_{b-1}}} \delta_0(q_1 + \ldots + q_b - x) \leqslant \Delta_1(\vec{s}) \ldots \Delta_{b-1}(\vec{s}) M^{k-1}, \tag{13}$$

где $\Delta_l(\vec{s})$ — число всевозможных индексов у множества Q_{i_l}, а $\delta_0(z)$ — функция, такая что $\delta_0(z) = 1$ тогда и только тогда, когда $z = 0$. Требуется оценить величины $\Delta_l(\vec{s})$. Предположим, что множества $Q_{i_1}, \dots, Q_{i_{l-1}}$ зафиксированы. Найдём тогда верхнюю границу на число множеств Q_{i_l}. Пусть z — наименьшее целое, такое что

$$\sum_{j=1}^{l-1} s_j 4^j \leqslant s_l \frac{4^{l+z}}{2}. \tag{14}$$

Тогда число множеств Q_{i_l} ограничено величиной $z+1$. В самом деле, без ограничения общности можно считать, что $i_j = j$, $j \in \{1, \dots, l-1\}$, и $i_l = l + z'$, $z' > z$. Тогда множество Q_{i_l} определяется однозначно, ибо в противном случае мы имеем решение уравнения

$$\mu_1 + \ldots + \mu_{l-1} + \mu_l = x = \mu'_1 + \ldots + \mu'_{l-1} + \mu'_l, \tag{15}$$

где $\mu_j, \mu'_j \in s_j Q_{i_j}$, $j \in \{1, \dots, l-1\}$, и аналогично $\mu_l \in s_l Q_{l+z'}$, $\mu'_l \in s_l Q_{i_l}$, $i_l < l + z'$. Если равенство (15) имеет место, то

$$s_l \frac{4^{l+z}}{2} \leqslant s_l \frac{4^{l+z'}}{2} < \mu'_l - \mu_l \leqslant \mu_1 + \ldots + \mu_{l-1} \leqslant \sum_{j=1}^{l-1} s_j 4^j,$$

что противоречит выбору числа z. Отсюда следует, что

$$\Delta_l(\vec{s}) \leqslant \log\Big(2\sum_{j=1}^{l-1} s_j 4^{j-l}\Big) + 1 \leqslant \log\Big(2 \max_{1 \leqslant j \leqslant l-1} \{s_j 2^{j-l}\}\Big) + 1.$$

Пусть $m_1 < m_2 < \ldots < m_t$ — локальные максимумы последовательности $\max\limits_{1 \leqslant j \leqslant l-1} \{s_j 2^{j-l}\}$, $l \in \{1, \dots, b-1\}$. Пусть d_j — число появлений максимума m_j в этой последовательности. Тогда $\sum\limits_{j=1}^{t} d_j = k$. Далее по определению последовательности $\max\limits_{1 \leqslant j \leqslant l-1} \{s_j 2^{j-l}\}$, $l \in \{1, \dots, b-1\}$, легко убедиться, что $d_j \leqslant \log 2s_j$, $j \in \{1, \dots, t\}$. Возвращаясь к (12) и учитывая (13), получаем

$$N_k(x) \leqslant M^{k-1} \sum_{\vec{s}} \frac{k!}{s_1! \dots s_b!} \cdot (\log 2s_{m_1} + 1)^{d_1} \dots (\log 2s_{m_t} + 1)^{d_t} \leqslant$$

$$\leqslant M^{k-1} e^k k! \sum_{s_{m_1}, \dots, s_{m_t}} \prod_{j=1}^{t} \frac{(\log 2s_{m_j} + 1)^{\log 2s_{m_j}}}{s_{m_j}!} \leqslant$$

$$\leqslant M^{k-1} e^{2k} k! \Big(\sum_{s} \frac{(\log 2s + 1)^{\log 2s}}{s^s} \Big)^t \leqslant 2^{6k} k^k M^{k-1},$$

как и требовалось. Таким образом, мы доказали нашу лемму, а следовательно, и лемму 15. □

Замечание 17. Если в оценке (11) разрешить появление множителей вида $(\log k)^k$, то требуемый результат вытекает немедленно. В самом деле, разобьём

наше множество Q на множества $B_1, \dots, B_r$, $r \sim \log k$, так, чтобы каждое B_j содержало лишь те Q_l, для которых $l \equiv j \pmod r$. Таким образом, мы теряем в точности множитель $(\log k)^k$, но при этом каждое множество Q_{i_l} в произвольном B_j определено однозначно. Далее, $\Delta_j(\vec{s}) = 1$ (см. формулы (13), (14)), и следовательно, $\mathbf{T}_k(B_j) \leqslant C^k k^k M^{k-1} |B_j|^k$, где $C > 0$ — некоторая абсолютная константа.

5. Доказательство теоремы 3

Зафиксируем произвольное $\varepsilon > 0$ и предположим, что

$$\|\chi_A\|_A \leqslant K, \quad K_\varepsilon \leqslant K \leqslant \left(\log \frac{p}{|A|}\right)^{1/3} \left(\log\log \frac{p}{|A|}\right)^{-1-\varepsilon}. \tag{16}$$

Наша цель — доказать, что неравенство (16) не может быть выполнено, если отношение $p/|A|$ превосходит некоторую величину, зависящую от ε. Так как $\varepsilon > 0$ произвольное, отсюда будет вытекать теорема 3.

Применение леммы 14 даёт нам величины x_0, q, m и B. Так как

$$\hat{\chi}_B(\gamma) = e_p(-qx_0\gamma)\hat{\chi}_A(q\gamma),$$

то $\|\chi_B\|_A = \|\chi_A\|_A$. Значит,

$$\|\chi_B\|_A \leqslant K. \tag{17}$$

Пусть l_0 — такое максимальное натуральное число l, что $2^l m < p/3$,

$$D_l = \{b \in B \colon |b| \leqslant 2^l m\}, \quad 0 \leqslant l \leqslant l_0,$$

$\eta = \exp(-CK)$, где C — большая константа, и

$$M = [\eta |A| e^{-d_\varepsilon}].$$

Если для некоторого $l \geqslant 1$ выполнено $|D_l \setminus D_{l-1}| < M$, то применение леммы 8 (параметр n равен $n = 2^{l-1}m$) с учётом неравенства $|D_l| \geqslant |D_0|$ и нижней оценки для $|D_0|$ из леммы 14 даёт нам

$$\|\hat{\chi}_B\|_1 \gg \min\left(\log \frac{1}{\eta}, \log |D_0|\right).$$

Поскольку

$$\log |D_0| \geqslant \log |A| - d_\varepsilon \gg \left(\frac{\log p}{\log\log p}\right)^{1/3} > K(\log\log p)^{2/3} > \log \frac{1}{\eta},$$

то

$$\|\hat{\chi}_B\|_1 \gg \log \frac{1}{\eta},$$

и мы получаем противоречие с (17), если константа C достаточно большая.

Таким образом, нам осталось рассмотреть случай, когда $|D_l \setminus D_{l-1}| \geqslant M$ для всех $l = 1, \dots, l_0$. Для каждого l, такого что $l \equiv 0 \pmod 2$, возьмём множество $S_l \subset D_l \setminus D_{l-1}$ мощности $|S_l| = M$. Положим

$$Q = \bigsqcup_l S_l.$$

Применим лемму 15 с параметром $k = [K]$, где Q_i — это множества S_l в другой нумерации ($I = [l_0/2]$). Теперь сравним верхнюю оценку (11) для величины $\mathbf{T}_k(Q)$ с соответствующей нижней оценкой из леммы 9. При этом $|Q| = IM$. После простых вычислений получаем

$$\frac{|Q|}{|A|} I^{k-1} \leqslant K^{3k-2} 2^{8k},$$

откуда следует (поскольку $|Q|/|A| \geqslant M/|A| \gg \eta e^{-d_\varepsilon}$ и $\eta = \exp(-CK)$), что

$$I \ll K^3. \tag{18}$$

Имеем

$$I \geqslant \frac{l_0}{2} - 1 \gg \log \frac{p}{m} \geqslant d_\varepsilon^{-1} \log \frac{p}{|A|} - \log d_\varepsilon.$$

Вспоминая формулы (16) и (10), мы видим, что

$$I \gg d_\varepsilon^{-1} \log \frac{p}{|A|} \gg \log \frac{p}{|A|} \left(\log \log \frac{p}{|A|} \right)^{-3-\varepsilon}.$$

Таким образом, неравенство (18) не согласуется с (16). Теорема доказана. □

Первый автор поддержан грантом РФФИ 14-01-00332 и грантом поддержки ведущих научных школ, грант НШ-3082.2014.1. Второй автор поддержан грантом мол_а_вед 12-01-33080.

Литература

[1] Зигмунд А. Тригонометрические ряды. Т. 2. — М.: Мир, 1965.

[2] Конягин С. В. О проблеме Литтлвуда // Изв. АН СССР. Сер. матем. — 1981. — Т. 45, № 2. — С. 243—265.

[3] Конягин С. В., Шкредов И. Д. Количественный вариант теоремы Берлинга—Хелсона. — В печати.

[4] Лебедев В. В. Абсолютно сходящиеся ряды Фурье. Усиление теоремы Берлинга—Хелсона // Функц. анализ и его прил. — 2012. — Т. 46, № 2. — С. 52—65.

[5] Bourgain J., Garaev M. Z. On a variant of sum-product estimates and explicit exponential sum bounds in prime fields // Math. Proc. Cambridge Philos. Soc. — 2009. — Vol. 146, no. 1. — P. 1—21.

[6] Green B. J., Konyagin S. V. On the Littlewood problem modulo a prime // Can. J. Math. — 2009. — Vol. 61, no. 1. — P. 141—164.

[7] McGehee O. C., Pigno L., Smith B. Hardy's inequality and the L^1 norm of exponential sums // Ann. Math. — 1981. — Vol. 113. — P. 613—618.

[8] Sanders T. The Littlewood—Gowers problem // J. Anal. Math. — 2007. — Vol. 101. — P. 123—162.

[9] Sanders T. The structure theory of set addition revisited // Bull. Am. Math. Soc. — 2013. — Vol. 50, no. 1. — P. 93—127.

[10] Schoen T. New bounds in Balog—Szemerédi—Gowers theorem // Combinatorica. — Accepted.

[11] Tao T., Vu V. Additive Combinatorics. — Cambridge: Cambridge Univ. Press, 2006.