ФГБОУ ВО
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА»

На правах рукописи
УДК 511.321

Габдуллин Михаил Рашидович

Суммы характеров: оценки и приложения

01.01.06 — математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2019

Работа выполнена на кафедре общих проблем управления механико-математического факультета МГУ им. М.В.Ломоносова.

Научный руководитель:

КОНЯГИН Сергей Владимирович — доктор физико-математических наук, академик РАН, профессор, заведующий отделом теории чисел, главный научный сотрудник Федерального государственного учреждения науки Математический институт им. В.А. Стеклова Российской академии наук (специальность 01.01.06).

Официальные оппоненты:

ДОБРОВОЛЬСКИЙ Николай Михайлович — доктор физико-математических наук, профессор, заведующий кафедрой алгебры, математического анализа и геометрии факультета математики, физики и информатики Федерального государственного бюджетного образовательного учреждения высшего образования «Тульский государственный педагогический университет им. Л.Н. Толстого» (специальность — 01.01.06).

ЧАНГА Марис Евгеньевич — кандидат физико-математических наук, доцент кафедры высшей математики геодезического факультета Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет геодезии и картографии» (специальность — 01.01.06).

Ведущая организация:

Хабаровское отделение Федерального государственного бюджетного учреждения науки Института прикладной математики ДВО РАН.

Защита диссертации состоится 3 октября 2019 г. в 15:00 на заседании диссертационного совета Д002.022.03 при МИАН по адресу: 119991, Москва, ул. Губкина, д. 8, конференц-зал (9 этаж).

Ознакомиться с диссертацией можно можно в библиотеке МИАН и на сайте http://www.mi-ras.ru/dis/ref19/gabdullin/dis.pdf

Автореферат разослан “ ” августа 2019 г.

Учёный секретарь
диссертационного совета
Д002.022.03 при МИАН,
доктор физ.мат наук  Королёв М.А.

Общая характеристика работы

Актуальность темы.

Характерами на конечной абелевой группе называют гомоморфизмы последней в единичную окружность комплексной плоскости. Первый и, пожалуй, самый известный пример характеров — это характеры Дирихле, являющиеся характерами мультипликативных групп обратимых элементов колец вычетов. С помощью таких характеров и соответствующих им L-функций П.Г.Л. Дирихле доказал свою знаменитую теорему о том, что в арифметической прогрессии, первый член и разность которой взаимно просты, существует бесконечно много простых чисел.

Суммы характеров тесно связаны с тригонометрическими суммами, то есть суммами вида $\sum_{n\in A} e^{2\pi i f(n)}$, где $f(n)$ — вещественная функция, а A — некоторое множество. Работы многих крупных математиков прошлого столетия (таких как И.М.Виноградов, Г.Вейль, Й. ван дер Корпут, А.А.Карацуба, Н.М.Коробов, и другие) были посвящены оценкам тригонометрических сумм и сумм характеров. Во многих задачах теории чисел такие суммы возникают естественным образом, и их оценки позволяют получать нетривиальные результаты в самых разных аналитических и комбинаторных задачах. Так, например, с помощью оценок линейных тригонометрических сумм по простым числам (в сочетании с круговым методом) И.М.Виноградов в 1937 году доказал, что любое достаточно большое нечетное число представимо в виде суммы трех простых чисел, решив тем самым тернарную проблему Гольдбаха. Многие открытые проблемы теории чисел следуют из достаточно сильных (неизвестных на сегодняшний день) оценок сумм характеров или тригонометрических сумм: к числу таких примеров можно отнести гипотезу Линделёфа об оценке дзета-функции на критической прямой и гипотезу И.М.Виноградова о наименьшем квадратичном невычете по простому модулю.

Оценкам сумм характеров и тригонометрических сумм посвящен ряд монографий[1] [2] [3].

Цель работы.

Получение новых оценок сумм характеров по параллелепипедам в

[1] Архипов Г.И., Карацуба А.А., Чубариков В.Н., Кратные тригонометрические суммы, Тр. МИАН СССР, 151, ред. С. М. Никольский, 1980, 128 с.

[2] Виноградов И. М., Приложение 1 к книге: Хуа Ло-Ген “Метод тригонометрических сумм и его применения в теории чисел”, М., Мир, 1964.

[3] Коробов Н.М., Оценки тригонометрических сумм и их приложения, УМН, 13:4(82) (1958), 185–192.

конечных полях, нижних оценок винеровской нормы функций в $\mathbb{Z}_p^d$, применение различных оценок сумм характеров к современным комбинаторным задачам теории чисел.

Научная новизна. В диссертации получены следующие результаты.

1) Доказаны нетривиальные оценки сумм характеров по параллелепипедам достаточно большого объёма в конечных полях порядка p^2 и p^3.

2) Получены нижние оценки винеровской нормы функций в дискретном многомерном случае (для группы $\mathbb{Z}_p^d$).

3) Изучена задача о распределении квадратов во множестве конечного поля с ограничениями на коэффициенты при разложении по базису.

4) Для почти всех модулей получены нетривиальные оценки на размер подмножества кольца вычетов, разность которого с собой не содержит квадратичных вычетов.

Методы исследования.

Основные методы исследования лежат в русле аналитической теории чисел. Используются также методы геометрии чисел и теории графов, а также ряд разработанных автором приёмов, позволивших преодолеть конкретные технические трудности в каждой из упомянутых задач.

Теоретическая и практическая ценность.

Диссертация имеет теоретический характер. Полученные в диссертации результаты представляют интерес для специалистов в области теории чисел.

Апробация диссертации.

Результаты диссертации неоднократно докладывались и обсуждались на научно-исследовательском семинаре “Современные проблемы теории чисел” в Математическом Институте им. Стеклова под руководством С.В.Конягина и И.Д.Шкредова (многократно), на Московском семинаре по теории чисел под руководством Н.Г.Мощевитина и Ю.В.Нестеренко, на семинаре по теории функций действительного переменного под руководством Б.С.Кашина, С.В.Конягина, Б.И.Голубова, и М.И.Дьяченко, на семинаре ”Геометрическая теория приближений” под руководством П.А.Бородина, и на международных конференциях “Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории” (Тула, 2019 г.), Воронежская зимняя математическая школа ”Современные методы теории функций и смежные проблемы” (Воронеж, 2019г.), Саратовская зимняя школа “Современные проблемы тео-

рии функций и их приложения" (Саратов, 2016 г.), "Uniform Distribution Theory" (Шопрон, Венгрия, 2016 г., и Марсель, Франция, 2018 г.), "Journées Arithmétiques" (Кан, Франция, 2017 г.), а также во время визитов автора в Математический Институт им. Альфреда Реньи, Будапешт, 2016 г., и Математический Исследовательский Институт в Беркли (2017 г.).

Публикации.

Результаты диссертации опубликованы в 4 работах автора в журналах из баз данных Web of Science и Scopus и представлены также в тезисах нескольких международных конференций. Список этих работ приведён в конце автореферата.

Структура и объём работы.

Диссертация состоит из четырёх глав, заключения и списка литературы из 64 наименований. Общий объём диссертации составляет 84 страницы.

В диссертацию вошли результаты, полученные при работе над проектом 14-11-00702 Российского научного фонда, выполнявшегося при ИММ УрО РАН г. Екатеринбурга, и работе в лаборатории «Многомерная аппроксимация и приложения» МГУ им. М.В.Ломоносова (проект 14.W03.31.0031).

Краткое содержание диссертации

Глава 1. В этой главе получены нетривиальные оценки сумм мультипликативных характеров в конечных полях размера p^2 и p^3 по параллелепипедам достаточно большого объёма.

Пусть p — простое число, $\mathbb{F}_{p^n}$ — конечное поле из p^n элементов, $\{\omega_1, \dots \omega_n\}$ — базис $\mathbb{F}_{p^n}$ над $\mathbb{F}_p$, N_i, H_i — целые числа, $1 \leqslant H_i \leqslant p$, $i = 1, \dots, n$. Определим n-мерный «параллелепипед» $B \subseteq \mathbb{F}_{p^n}$:

$$B = \left\{ \sum_{i=1}^{n} x_i \omega_i \, : \, N_i + 1 \leqslant x_i \leqslant N_i + H_i, \;\; 1 \leqslant i \leqslant n \right\}. \qquad (1)$$

Нас будут интересовать оценки сумм вида $\sum_{x \in B} \chi(x)$, где χ — нетривиальный мультипликативный характер в $\mathbb{F}_{p^n}$, при возможно более слабых ограничениях на B. Дадим обзор известных в этом направлении результатов. В случае $n = 1$ на протяжении более чем полувека сильнейшим остаётся знаменитый результат Бёрджеса[4]: для любого $\varepsilon > 0$

[4]Burgess D. A., "On character sums and primitive roots", Proc. London Math. Society (3), 12 (1962), 179-192.

существует $\delta > 0$ такое, что при $H \geqslant p^{1/4+\varepsilon}$ справедлива оценка

$$\left| \sum_{x=N+1}^{N+H} \chi(x) \right| \ll_\varepsilon p^{-\delta} H.$$

Бёрджес[5] также получил аналог этого неравества для базисов специального вида в случае $n = 2$, а Карацуба[6] [7] обобщил его оценки на произвольные конечные поля, рассматривая случай базиса вида $\omega_i = g^i$, где g — корень неприводимого многочлена степени n над $\mathbb{F}_p$. Представляют интерес оценки сумм характеров по параллелепипедам, построенным по произвольным базисам. Первый такой результат был получен в работе Дэвенпорта и Льюиса[8].

Теорема A. *Для любого $\varepsilon > 0$ существует $\delta > 0$ такое, что при*

$$H_1 = \ldots = H_n = H > p^{\frac{n}{2n+2}+\varepsilon}$$

выполнена оценка

$$\left| \sum_{x \in B} \chi(x) \right| \leqslant (p^{-\delta} H)^n.$$

Заметим, что в теореме A показатель $\frac{n}{2n+2}$ стремится к $1/2$ при $n \to \infty$. Это ограничение было ослаблено Чанг[9].

Теорема B. *Пусть $\varepsilon > 0$ и параллелепипед B удовлетворяет условию $\prod_{i=1}^n H_i > p^{(\frac{2}{5}+\varepsilon)n}$. Тогда*

$$\left| \sum_{x \in B} \chi(x) \right| \ll_{n,\varepsilon} p^{-\varepsilon^2/4} |B|$$

в случае, если n нечётно или если n чётно и сужение $\chi|_{\mathbb{F}_{p^{n/2}}}$ характера χ на подполе $\mathbb{F}_{p^{n/2}}$ является нетривиальным характером, и

$$\left| \sum_{x \in B} \chi(x) \right| \leqslant \max_\xi |B \cap \xi \mathbb{F}_{p^{n/2}}| + O_{n,\varepsilon}(p^{-\varepsilon^2/4}|B|)$$

---

[5] Burgess D. A., "Character sums and primitive roots in finite fields", Proc. London Math. Society (3), 17 (1967), 11-25.

[6] Карацуба А. А., Суммы характеров и первообразные корни в конечных полях, ДАН СССР, 180:6, (1968), 1287-1289.

[7] Карацуба А. А., Об оценках сумм характеров, Изв. АН СССР Сер. матем., 34:1, (1970), 20-30.

[8] Davenport H., Lewis D. J., "Characters sums and primitive roots in finite fields", Rend. Circ. Mat. Palermo(2), 12 (2), 129-136 (1963).

[9] Chang M.-Ch., "On a question of Davenport and Lewis and new character sums bounds in finite fields", Duke Math. J. 145 (3), 409-442 (2008).

иначе.

Отметим, что при условии $|B| = \prod_{i=1}^{n} H_i > p^{(2/5+\varepsilon)n}$, вообще говоря, нельзя получить нетривиальные оценки суммы значений нетривиального характера, так как возможен случай, когда B совпадает с подполем $\mathbb{F}_{p^{n/2}}$, а χ — нетривиальный характер, тождественный на $\mathbb{F}_{p^{n/2}}$. Отсюда возникает необходимость рассматривать случаи, описанные в теореме B.

Далее, Чанг[10] были получены нетривиальные оценки сумм характеров в случае $n = 2$, $H_1, H_2 > p^{1/4+\varepsilon}$. Конягин[11] обобщил последний результат на произвольные конечные поля.

Теорема C. *Пусть $\varepsilon > 0$ и выполнено условие $H_i > p^{1/4+\varepsilon}$ при всех $1 \leqslant i \leqslant n$. Тогда*

$$\left|\sum_{x\in B} \chi(x)\right| \ll \frac{n^{O(1)}}{\varepsilon} p^{-\varepsilon^2/2}|B|.$$

В этой главе мы доказываем следующую оценку суммы характеров для случаев $n = 2$ и $n = 3$.

Теорема 1.1. *Пусть $n \in \{2, 3\}$, χ — нетривиальный мультипликативный характер в $\mathbb{F}_{p^n}$ и $|B| \geqslant p^{n(1/4+\varepsilon)}$, причём будем считать, что $H_1 \leqslant \ldots \leqslant H_n$. Тогда*

$$\left|\sum_{x\in B} \chi(x)\right| \ll_\varepsilon |B|p^{-\varepsilon^2/12},$$

если $\chi|_{\mathbb{F}_p}$ — нетривиальный характер, и

$$\left|\sum_{x\in B} \chi(x)\right| \ll_\varepsilon |B|p^{-\varepsilon^2/12} + |B \cap \omega_n\mathbb{F}_p|$$

иначе.

Заметим, что так как $\{\omega_1, \ldots, \omega_n\}$ — базис, то

$$|B \cap \omega_n\mathbb{F}_p| = \begin{cases} H_n, \text{ если } 0 \in \cap_{i=1}^{n-1}[N_i + 1, N_i + H_i], \\ 0, \text{ иначе,} \end{cases}$$

поэтому во втором случае теоремы можно написать оценку $\sum_{x\in B} \chi(x) \ll_\varepsilon |B|p^{-\varepsilon^2/12} + H_n$. Кроме того, по аналогии с замечанием к теореме B,

[10] Chang M.-Ch., "Burgess inequality in $\mathbb{F}_{p^2}$", Geom. Funct. Anal. Vol. 19 (2009), 1001-1016.

[11] Конягин С.В., Оценки сумм характеров в конечных полях, Матем. заметки, 2010, том 88 (4), 529-542.

в условиях теоремы ($|B| \geqslant p^{n(1/4+\varepsilon)}$), вообще говоря, нельзя получить нетривиальные оценки суммы характеров, так как возможен случай, когда $B = \mathbb{F}_p$ и χ — нетривиальный характер, тождественный на $\mathbb{F}_p$. Отметим, что в условиях теоремы C такая ситуация невозможна в силу условия $H_i > p^{1/4+\varepsilon}$, $1 \leqslant i \leqslant n$.

Глава 2. В данной главе получены нижние оценки винеровской нормы (l_1-нормы преобразования Фурье) функций в $\mathbb{Z}_p^d$. Начнём изложение с истории вопроса.

Пусть $B \subset \mathbb{Z}$ — конечное множество, $|B| \geqslant 2$ и $e(x) := \exp(2\pi i x)$. Знаменитая гипотеза Литтлвуда гласит, что

$$\int_0^1 \left|\sum_{b\in B} e(bx)\right| dx \gg \log|B|.$$

Впервые это неравенство было доказано Конягиным[12] в 1981 году. В чуть более поздней работе Мак-Ги, Пиньо и Смита[13] получен более общий результат: если $B = \{b_1 < \ldots < b_n\}$ и $c(b_j) \in \mathbb{C}$ — произвольные комплексные числа, то

$$\int_0^1 \left|\sum_{b\in B} c(b)e(bx)\right| dx \gg \sum_{j=1}^{n} \frac{|c(b_j)|}{j} \qquad (2)$$

Хорошо известно , что в случае, когда $B = [-n, n] \cap \mathbb{Z}$, тригонометрический полином $D_n(x) := \sum_{b\in B} e^{ibx} = \sum_{k=-n}^{n} e^{-ikx}$ (ядро Дирихле) имеет L_1-норму, по порядку равную $\log n = \log|B|$. Таким образом, оба упомянутых результата точны по порядку.

В работе Грина и Конягина[14], а также в ряде последующих работ изучался дискретный аналог гипотезы Литтлвуда для случая группы $\mathbb{Z}_p$. Напомним необходимые определения в более общем случае конечной абелевой группы G. Характером группы G называется гомоморфизм $\gamma\colon G \to S^1$, где $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. Через $\widehat{G}$ будем обозначать дуальную группу группы G, то есть группу всех характеров (с операцией поточечного умножения). Хорошо известно, что в случае конечных абелевых групп группы G и $\widehat{G}$ изоморфны; мы будем отождествлять их. Для

[12]Конягин С.В., О проблеме Литтлвуда, Известия РАН, 45 (1981), 243-265.

[13]McGehee O.C., Pigno L., Smith B., Hardy's inequality and the L_1 norm of exponential sums, Annals of Math. 113 (1981), 613-618.

[14]Green B.J., Konyagin S.V., On the Littlewood problem modulo prime, Canad. J.Math. 61 (2009), 141-164.

произвольной функции $f\colon G \to \mathbb{C}$ определим её преобразование Фурье $\widehat{f}\colon G \to \mathbb{C}$,

$$\widehat{f}(\gamma) = |G|^{-1} \sum_{x \in G} f(x)\overline{\gamma(x)}$$

и винеровскую норму

$$\|\widehat{f}\|_1 = \sum_{\gamma \in \widehat{G}} |\widehat{f}(\gamma)|$$

(здесь и везде далее для $q > 0$ мы полагаем $\|g\|_q := (\sum_{x \in \operatorname{supp} g} |g(x)|^q)^{1/q}$). Имеет место неравенство

$$\widehat{fg}(\xi) = \sum_{\eta \in \widehat{G}} \widehat{f}(\xi - \eta)\widehat{g}(\eta),$$

откуда сразу следует, что

$$\|\widehat{fg}\|_1 \leqslant \|\widehat{f}\|_1 \|\widehat{g}\|_1. \tag{3}$$

Таким образом, пространство всех функций на G, снабжённое винеровской нормой, является банаховой алгеброй относительно обычного поточечного умножения функций.

Для множества $A \subseteq G$ через $A(x)$ будем обозначать его характеристическую функцию. Положим также $e_p(u) = e^{2\pi i u/p}$.

В случае $G = \mathbb{Z}_p$ характерами являются отображения $\gamma_\xi(x) = e_p(\xi x)$, и винеровская норма характеристической функции множества $A \subset \mathbb{Z}_p$ представляет собой дискретизацию L_1-нормы тригполинома $T_A(y) = \sum_{x \in A} e(xy)$:

$$\|\widehat{A}\|_1 = \frac{1}{p} \sum_{\xi \in \mathbb{Z}_p} \left| \sum_{x \in A} \exp\left(\frac{2\pi i \xi x}{p}\right) \right| = \frac{1}{p} \sum_{\xi=1}^{p} \left| T_A\left(\frac{\xi}{p}\right) \right|.$$

Поэтому задачу об оценке винеровской нормы подмножеств $\mathbb{Z}_p$ естественно рассматривать как дискретную версию гипотезы Литтлвуда.

Легко видеть, что

$$\|\widehat{A}\|_1 = \|\widehat{(\mathbb{Z}_p \setminus A)}\|_1 + \frac{2|A|}{p} - 1 = \|\widehat{(\mathbb{Z}_p \setminus A)}\|_1 + O(1),$$

поэтому достаточно рассматривать случай $|A| < p/2$. Предполагается, что при всех таких A имеет место оценка

$$\|\widehat{A}\|_1 \gg \log |A|, \tag{4}$$

аналогичная оценке (2) в непрерывном случае. Кроме того, применяя теорему Марцинкевича о дискретизации L_1-норм тригонометрических многочленов , нетрудно видеть, что в случае, когда A — арифметическая прогрессия (и $|A| < p/2$), справедливо

$$\|\widehat{A}\|_1 \asymp \log |A|.$$

Обсудим теперь известные результаты. Неравенство (4) доказано Конягиным и Шкредовым[15] для множеств малого размера.

Теорема D. *Пусть $A \subset \mathbb{Z}_p$ и*

$$|A| \ll \exp((\log p/\log\log p)^{1/3}).$$

Тогда справедлива оценка (4).

Ими же[16] получены следующие результаты.

Теорема E. *Пусть $A \subset \mathbb{Z}_p$, $\exp((\log p/\log\log p)^{1/3}) \leqslant |A| \leqslant p/3$. Тогда, полагая $\delta = |A|/p$, будем иметь*

$$\|\widehat{A}\|_1 \gg (\log \delta^{-1})^{1/3}(\log\log \delta^{-1})^{-1-o(1)}, \quad \delta \to 0.$$

Кроме того, авторами было показано, что из результатов Сандерса[17] вытекает следующая оценка.

Теорема F. *Пусть $A \subset \mathbb{Z}_p$ и $\delta = |A|/p < 1/2$. Тогда*

$$\|\widehat{A}\|_1 \gg \delta^{3/2}(\log p)^{1/2-o(1)},$$

при $\delta \geqslant (\log p)^{-1/4}(\log\log p)^{1/2}$, и

$$\|\widehat{A}\|_1 \gg \delta^{1/2}(\log p)^{1/4-o(1)}$$

при $\delta < (\log p)^{-1/4}(\log\log p)^{1/2}$.

Из теорем D и E следуют оценки типа $\|\widehat{A}\|_1 \gg (\log p)^c$, $c > 0$, для плотных и и достаточно редких множеств, но, скажем, при $\delta \asymp$

[15]Конягин С.В., Шкредов И.Д., Количественный вариант теоремы Берлинга–Хелсона, Функц. анализ и его прил., 49:2 (2015), 39–53; Funct. Anal. Appl., 49:2 (2015), 110–121.

[16]Конягин С.В., Шкредов И.Д., О норме Винера подмножеств $\mathbb{Z}_p$ промежуточного размера, Фундамент. и прикл. матем., 19:5 (2014), 75–87; J. Math. Sci., 218:5 (2016), 599–608.

[17]Sanders T., The Littlewood-Gowers problem, J.Anal.Math. 101 (2007), 123-162

$(\log p)^{-1}$ работает лишь теорема D и даёт слабые оценки снизу (порядка $(\log\log p)^{1/3}$). Шоен[18] показал, что винеровскую норму подмножества $A \subset \mathbb{Z}_p$ (при $|A| < p/2$) всегда можно оценить снизу величиной $(\log|A|)^{1/16-o(1)}$. Из следующего результата Сандерса[19] вытекает более сильная оценка $\|\widehat{A}\|_1 \gg (\log|A|)^{1/4-o(1)}$.

Теорема G. *Пусть G — конечная абелева группа. Обозначим через $\mathcal{W}(G)$ множество смежных классов по всевозможным подгруппам группы G. Тогда для любой функции $f\colon G \to \mathbb{Z}$ такой, что $\|\widehat{f}\|_1 \leqslant K$, справедливо представление*

$$f = \sum_{W\in\mathcal{W}(G)} z(W)1_W,$$

где $z(W) \in \mathbb{Z}$ и $\sum_{W\in\mathcal{W}(G)} |z(W)| \leqslant \exp(K^{4+o(1)})$.

Настоящей главе посвящены следующие результаты. Во-первых, мы обобщаем теоремы D и E на случай, когда вместо характеристической функции множества заданного размера рассматривается функция f со значениями, больше или равными единицы по модулю, и носителем, имеющем аналогичный размер.

Теорема 2.1. *Пусть $f\colon \mathbb{Z}_p \to \mathbb{C}$ и $|f(x)| \geqslant 1$ при $x \in S := \operatorname{supp} f$. Тогда, полагая $M := \max_{x\in\mathbb{Z}_p} |f(x)|$, имеем*

$$\|\widehat{f}\|_1 \geqslant M$$

и

$$\|\widehat{f}\|_1 \gg \min\left(\log|S|, \left(\frac{\log p}{(\log\log p)(\log|S|)}\right)^{1/2}\right).$$

В частности, если $|S| \leqslant \exp((\log p/\log\log p)^{1/3})$, то $\|\widehat{f}\|_1 \gg \log|S|$.

Теорема 2.2. *Пусть $f\colon \mathbb{Z}_p \to \mathbb{C}$ и $|f(x)| \geqslant 1$ при $x \in S := \operatorname{supp} f$. Тогда, полагая $M := \max_{x\in\mathbb{Z}_p} |f(x)|$, при $\exp((\log p/\log\log p)^{1/3}) \leqslant |S| \leqslant p/3$ имеем*

$$\|\widehat{f}\|_1 \geqslant M$$

и

$$\|\widehat{f}\|_1 \gg (\log(p/|S|))^{1/3}(\log\log(p/|S|))^{-1-o(1)}, \quad p/|S| \to \infty.$$

[18]Schoen T., On the Littlewood conjecture modulo prime, Moscow Journal of Number Theory and Combinatorics, 1-5, 2016.

[19]Sanders T., Bounds in Cohen's idempotent theorem, preprint

Вторая цель настоящей главы — перенесение одномерных результатов на многомерный случай. В этом направлении получены два результата.

Теорема 2.3. *Пусть $E \subseteq \mathbb{C}$ — произвольное множество и число $C > 0$ достаточно велико. Предположим, что для любой функции $h\colon \mathbb{Z}_p \to E \cup \{0\}$ выполнена оценка*

$$\|\widehat{h}\|_1 \geqslant F(p, \delta),$$

где $\delta = |\operatorname{supp} h| p^{-1}$. Тогда для любой функции $f\colon \mathbb{Z}_p^d \to E \cup \{0\}$ такой, что $|\operatorname{supp} f| = \delta p^d$, $\delta \geqslant Cp^{-1}$, выполнено

$$\|\widehat{f}\|_1 \geqslant F(p, \delta'),$$

для некоторого $\delta' = \delta + O(\delta^{1/2} p^{-1/2})$, причём подразумеваемая постоянная абсолютна.

Замечание. *Не умаляя общности, в формулировке теоремы можно считать, что функция $F(p, \delta)$ равна $+\infty$, если $p\delta$ не равно целому числу. Это предположение не влияет на посылку теоремы и отсекает тривиальные случаи, связанные с тем, что мы не знаем точное значение δ'.*

В частности, с помощью теоремы 2.3 и теоремы F можно оценить винеровскую норму больших подмножеств $\mathbb{Z}_p^d$: если $A \subset \mathbb{Z}_p^d$ и $|A| \asymp p^d$ (и $|A| < p^d/2$), то $\|\widehat{A}\|_1 \gg (\log p)^{1/2 - o(1)}$.

Нам удобно формулировать теорему 2.3 в «условном» виде, чтобы не зависеть от наилучших на сегодня результатов в одномерном случае. Кроме того, как упоминалось выше, для разных классов функций имеются разные оценки: например, в работе Сандерса изучаются целозначные функции, в то время как в работах Конягина и Шкредова получены оценки винеровской нормы характеристических функций подмножеств $\mathbb{Z}_p$, а в настоящей работе — функций, со значениями, больше или равными единицы по модулю.

В аналогичном «условном» виде сформулируем результат об оценке снизу винеровской нормы малых подмножеств $\mathbb{Z}_p^d$.

Теорема 2.4. *Пусть $E \subseteq \mathbb{C}$ — произвольное множество, инвариантное относительно поворотов (то есть $e^{i\varphi} E = E$ при всех $\varphi \in \mathbb{R}$). Предположим, что для любой функции $h\colon \mathbb{Z}_p \to E \cup \{0\}$ такой, что $|\operatorname{supp} h| = \delta p < (2p)^{1/2}$, выполнена оценка*

$$\|\widehat{h}\|_1 \geqslant F(p, \delta).$$

Тогда для любой функции $f\colon \mathbb{Z}_p^d \to E \cup \{0\}$ *такой, что* $|\operatorname{supp} f| = \delta p < (2p)^{1/2}$, *справедливо*

$$\|\widehat{f}\|_1 \geqslant F(p,\delta).$$

В частности, с помощью теоремы 2.1 и теоремы 2.4 (используя их в случаях $M = 1$ и $E = \{z \in \mathbb{C} : |z| = 1\}$ соответственно) мы можем оценить винеровскую малых подмножеств $\mathbb{Z}_p^d$: при $A \subset \mathbb{Z}_p^d$, $|A| \leqslant \exp((\log p/\log\log p)^{1/3})$ получаем точную оценку $\|\widehat{A}\|_1 \gg \log|A|$.

При $d \geqslant 2$ мы, вообще говоря, не можем оценить $\|\widehat{A}\|_1$ снизу функцией, растущей по $|A|$, ибо, как нетрудно убедиться, для любого подпространства $V \subseteq \mathbb{Z}_p^d$ мы имеем $\|\widehat{V}\|_1 = 1$. Однако теорема G даёт нетривиальные оценки снизу в случаях, когда мы "отделены" от подпространств: например, если $G = \mathbb{Z}_p^d$, число $\eta \in (0,1)$ фиксировано, и $|A| \asymp p^{k+\eta}$, где $k \in \{0,1,\dots,d-1\}$, то мы получаем оценку $\|\widehat{A}\|_1 \gg (\log p)^{1/4-o(1)}$. Теоремы 2.3 и 2.4 усиливают эту оценку для малых и больших множеств A.

Глава 3. Эта глава посвящена результатам о множествах элементов конечного поля с "пропущенными цифрами". Перейдём к более точным формулировкам.

При любом фиксированном $b \in \mathbb{N}$, $b \geqslant 2$, каждое число $n \in \mathbb{N}$ единственным образом представимо в системе счисления с основанием b:

$$n = \sum_{j=0}^{r-1} c_j b^j, \qquad 0 \leqslant c_j \leqslant b-1, \quad c_{r-1} \geqslant 1.$$

Во многих работах изучались арифметические свойства чисел с пропущенными цифрами, т.е. тех чисел, b-ичная запись которых состоит из заданных цифр.

Дартидж и Шаркози[20] рассмотрели аналог этой задачи в конечных полях. Пусть $\mathbb{F}_q$ — поле из $q = p^r$ элементов, $\{a_1,\dots,a_r\}$ — базис $\mathbb{F}_q$ над $\mathbb{F}_p$. Для множества $\mathcal{D} \subset \mathbb{F}_p$ через $W_{\mathcal{D}}$ будем обозначать множество элементов поля $\mathbb{F}_q$, все коэффициенты которых при разложении по базису $\{a_1,\dots,a_r\}$ принадлежат множеству $\mathcal{D}$. Обозначим через Q множество ненулевых квадратов поля $\mathbb{F}_q$. Положим $Q_0 = Q \cup \{0\}$. Будем считать, что $p \geqslant 3$, так как в случае $p = 2$ мы имеем $\mathbb{F}_q = Q_0$. Кроме того, везде в дальнейшем будем считать, что $|\mathcal{D}| \geqslant 2$ и $r \geqslant 2$, ибо в противном случае задача также бессодержательна.

[20]Dartyge C., Sárközy A., The sum of digits function in the finite field. Proc. Amer. Math. Soc. 2013. Vol. 141, №12. P. 4119-4124.

В недавней работе Дартидж, Мадуи и Шаркози[21] было показано, что если множество $\mathcal{D}$ достаточно велико, то во множестве $W_{\mathcal{D}}$ имеются квадраты.

Теорема H. *Имеет место оценка*

$$\left||W_{\mathcal{D}} \cap Q_0| - \frac{|W_{\mathcal{D}}|}{2}\right| \leqslant \frac{1}{2\sqrt{q}} \left(|\mathcal{D}| + p\sqrt{p - |\mathcal{D}|}\right)^r .$$

Эта оценка нетривиальна, если $|\mathcal{D}| \geqslant \frac{(\sqrt{5}-1)p}{2}(1 + o(1))$, $p \to \infty$.

В случае, когда множество $\mathcal{D}$ состоит из последовательных чисел, в этой же работе был получен аналог предыдущей теоремы.

Теорема I. *Пусть* $\mathcal{D} = \{0, \ldots, t-1\}$, *где* $2 \leqslant t \leqslant p-1$. *Тогда*

$$\left||W_{\mathcal{D}} \cap Q_0| - \frac{|W_{\mathcal{D}}|}{2}\right| \leqslant \frac{1}{2} \left(C(p,t)t\sqrt{p}\right)^r ,$$

где

$$C(p,t) = \begin{cases} \frac{\log p}{t} + \frac{1}{t}\left(\frac{4}{3} - \frac{\log 3}{2}\right) + \frac{1}{p}, & \text{если } 2 \leqslant t < p-2, \\ \frac{2}{p} + \frac{2}{\pi(p-1)}(1 - \log(2\sin\frac{\pi}{2p})), & \text{если } t = p-2. \end{cases}$$

Эта оценка нетривиальна, если $t \gg \sqrt{p}\log p$.

Диссертантом доказаны следующие две оценки на количество квадратов во множестве $W_{\mathcal{D}}$, из которых вытекает существование квадратов при ограничениях на размер множества $\mathcal{D}$ более слабых, чем в теореме H.

Теорема 3.1. *Пусть* $2r - 1 \leqslant p^{1/2}$. *Тогда справедлива оценка*

$$\left||W_{\mathcal{D}} \cap Q| - \frac{|W_{\mathcal{D}}|}{2}\right| \leqslant \frac{1}{2}|\mathcal{D}|^{1/2} \left(p^{1/4}(2r-1)^{1/2}|\mathcal{D}|^{r-1} + \frac{1}{2}p^{3/4}r^{3/2}\right) .$$

Кроме того, если $\delta = \left(\sqrt{p}(2r-1)\right)^{2-r}$ *и* $|\mathcal{D}| \geqslant (1+\delta)(2r-1)p^{1/2}$, то $|W_{\mathcal{D}} \cap Q| \geqslant 1$.

Теорема 3.2. *При любых натуральных* ν *и* $1 \leqslant k \leqslant r-1$ *справедлива оценка*

$$\left||W_{\mathcal{D}} \cap Q| - \frac{|W_{\mathcal{D}}|}{2}\right| < |\mathcal{D}|^{(r-k)(1-1/2\nu)} \left(\nu|\mathcal{D}|^{k/2}q^{1/2\nu} + |\mathcal{D}|^k q^{1/4\nu}\right) .$$

[21] Dartyge C., Mauduit C., Sárközy A.Polynomial values and generators with missing digits in finite fields. Functiones et Approximatio. 2015. Vol. 52, №1. P. 65–74.

Кроме того, если $r \geqslant 20$ *и* $|\mathcal{D}| \geqslant C(r)p^{\frac{1}{2}} \exp\left(\frac{\log p + 4\log\log p}{r}\right)$, *где* $C(r) = \exp\left(\frac{4\log r + 8}{r}\right)$, *то* $|W_{\mathcal{D}} \cap Q| \geqslant 1$.

В частности, из теоремы 3.2 следует, что при $r \gg p^{1/2}\log p$ во множестве $W_{\mathcal{D}}$ есть квадраты уже при $|\mathcal{D}| > p^{1/2} + 1$. Отметим, что при $r \gg \frac{\log p}{\log\log p}$, более точный результат дает теорема 3.2, а иначе — теорема 3.1.

Отметим, что при малых r теорему I также можно усилить, пользуясь теоремой C. Действительно, рассуждая стандартным образом , из теоремы C нетрудно вывести следующий результат.

Теорема 3.3. *Пусть* $a \in \mathbb{Z}_p$, $\varepsilon > 0$, $t \geqslant p^{1/4+\varepsilon}$, $\mathcal{D} = \{a, a+1, \ldots, a+t-1\}$. *Тогда справедлива оценка*

$$\left||W_{\mathcal{D}} \cap Q| - \frac{|W_{\mathcal{D}}|}{2}\right| \ll \frac{r^{O(1)}}{\varepsilon} p^{-\varepsilon^2/2}|W_{\mathcal{D}}|.$$

В частности, существует абсолютная $C > 0$ *такая, что если* $r > \log p$ *и* $\varepsilon \gg \sqrt{\frac{\log r}{\log p}}$, *то* $|W_{\mathcal{D}} \cap Q| = \left(\frac{1}{2} + O(r^{-C})\right)|W_{\mathcal{D}}|$; *если* $r < \log p$ *и* $\varepsilon \gg \sqrt{\frac{\log\log p}{\log p}}$, *то* $|W_{\mathcal{D}} \cap Q| = \left(\frac{1}{2} + O((\log p)^{-C})\right)|W_{\mathcal{D}}|$.

Далее, в работе Дитмана, Элсхолтца и Шпарлинского[22] была рассмотрена более общая задача. Пусть $D_1, \ldots, D_r$ – подмножества $\mathbb{F}_p$. Положим

$$W = W(D_1, \ldots, D_r) = \{x_1a_1 + \ldots + x_ra_r \,|\, x_i \in D_i\}.$$

Авторы отмечают, что доказательство теоремы H переносится на случай, когда множества D_i различны, а именно, при $\min\limits_{1\leqslant i\leqslant r} |D_i| \geqslant \frac{(\sqrt{5}-1)p}{2}(1 + o_p(1))$ справедливо $|W \cap Q_0| \geqslant 1$, и доказывают более сильное утверждение.

Теорема J. *Для любого* $\varepsilon > 0$ *существует* $\delta > 0$ *такое, что для любых множеств* $D_1, \ldots, D_r$, *удовлетворяющих условиям*

$$\prod_{i=1}^{r} |D_i| \geqslant p^{(1/2+\varepsilon)r^2/(r-1)}$$

[22]Dietmann R., Elsholtz C., Shparlinski I. E. Prescribing the binary digits of squarefree numbers and quadratic residues. arXiv: 1601.04754v1.

и

$$\min_{1\leqslant i\leqslant r}|D_i|\geqslant p^{\varepsilon}$$

справедливо $|W\cap Q_0|=\left(\frac{1}{2}+O(p^{-\delta})\right)|W|$.

Теорема 3.1 также может быть перенесена на случай различных множеств D_i. Доказана следующая

Теорема 3.4. *Справедлива оценка*

$$\left||W\cap Q|-\frac{|W|}{2}\right|\leqslant$$
$$\frac{1}{2}\left(|W|^{1-1/(2r)}p^{1/4}(2r-1)^{1/2}+|W|^{1/(2r)}(\frac{1}{4}p^{3/4}r^{3/2}+p^{1/2})+1\right).$$

Из этой теоремы вытекает аналог теоремы J, а также теорема о достаточных условиях существования квадратов во множестве W.

Следствие 3.5. *Пусть для некоторого* $\varepsilon>0$ *выполнено*

$$\prod_{i=1}^{r}|D_i|\geqslant(2r-1)^r p^{r(1/2+\varepsilon)}.$$

Тогда $|W\cap Q|=|W|\left(\frac{1}{2}+O(p^{-\varepsilon/2})\right)$, *причем постоянная в знаке* O *абсолютна.*

Отметим, что следствие 3.5 усиливает теорему J при фиксированном r (так как в нём отсутствует требование $\min\limits_{1\leqslant i\leqslant r}|D_i|\geqslant p^{\varepsilon}$).

Следствие 3.6. *Пусть* $\prod\limits_{i=1}^{r}|D_i|\geqslant 8(2r-1)^r p^{r/2}$. *Тогда* $|W\cap Q|\geqslant 1$.

Глава 4. Данная глава посвящена оценкам на размер подмножеств колец вычетов, разность которых не содержит ненулевых квадратичных вычетов. Начнём с истории вопроса.

Ловас предположил, что если последовательность $S\subset\mathbb{N}$ имеет положительную асимптотическую верхнюю плотность, то множество $S-S$ содержит точный квадрат. Шаркози[23] доказал это, показав, что если

[23] A. Sárközy, On difference sets of integers, I, Acta Math. Acad. Sci. Hungar. 31, 125-149 (1978)

множество $B \subset [N] = \{1, \dots, N\}$ таково, что $B - B$ не содержит ненулевых квадратов, то справедлива оценка

$$|B| \ll N(\log N)^{-1/3+\varepsilon}.$$

Наилучшая на сегодня оценка

$$|B| \ll \frac{N}{(\log N)^{\log\log\log\log N/12}},$$

получена в работе Пинца, Штайгера и Семереди[24]. Метод этой работы также позволяет получить верхнюю оценку на размер множества, разность с собой которого не содержит k-х степеней. С другой стороны, Ружи[25] построил пример множества $B \subset [N]$, разность которого не содержит квадратов, и такого, что $|B| \gg N^{\gamma}$, где $\gamma = \frac{1}{2}(1 + \frac{\log 7}{\log 65}) = 0.733077\dots$. Построение такого множества основывается на примере семиэлементного множества в кольце $\mathbb{Z}_{65}$, разность которого не содержит квадратичных вычетов по модулю 65.

Последний пример стимулировал рассмотрение аналогичной задачи в кольце вычетов $\mathbb{Z}_m$. Этот вопрос изучался в работе Ружи и Матолчи[26] Напомним, что натуральное число m называется бесквадратным (или свободным от квадратов), если оно имеет вид $m = p_1 \cdot \ldots \cdot p_s$, где $p_1, \dots, p_s$ — различные простые числа. Авторами было показано, что для множеств $A \subset \mathbb{Z}_m$ с тем свойством, что $A - A$ не содержит ненулевых кубических вычетов, доказана оценка

$$|A| \leqslant m^{1/2} 2^n$$

в случае, когда число m свободно от квадратов (здесь n обозначает количество простых делителей m вида $3k+1$), а также для произвольного m получена оценка

$$|A| \leqslant m^{1-\delta},$$

где $\delta = 0.119\dots$. Далее, авторы доказали, что если $A - A$ не содержит ненулевых квадратичных вычетов, то

$$|A| \leqslant m^{1/2}$$

[24]Pintz J., Steiger W.L., Szemerédi E., On sets of natural numbers whose difference set contains no squares J. London Math. Soc. s2-37, 2, 219-231 (1988).

[25]Ruzsa I., Difference sets without squares, Periodica Mathematica Hungarica, 15, 3, 205-209, 1984.

[26]Matolcsi M., Ruzsa I., Difference sets and positive exponential sums II: Quadratic and cubic residues in cyclic groups, preprint

для всех бесквадратных чисел m, все простые делители которых имеют вид $4l+1$, и

$$|A| \leqslant me^{-c\sqrt{\log m}},$$

где $c > 0$, при всех m.

В данной главе мы изучаем множества в кольце вычетов по бесквадратному модулю, разность которых избегает ненулевых квадратичных вычетов. Прежде всего, обсудим известные нижние оценки. Коэн[27] показал, что для модулей m, все простые делители которых имеют вид $4l+1$, найдётся такое множество размера по крайней мере $\prod_{p|m} \frac{\log_2 p}{2}$. Кроме того, Грэхем и Рингроуз[28] доказали существование таких множеств размера не менее $\log p \log\log\log p$ для бесконечного множества простых модулей $m = p$.

Основным результатом настоящей главы является

Теорема 4.1. *Для всех бесквадратных m и множеств $A \subset \mathbb{Z}_m$ таких, что $A-A$ не содержит квадратичных вычетов, справедлива оценка*

$$|A| \leqslant m^{1/2}(3n)^{1.5n},$$

где n обозначает количество нечётных простых делителей числа m.

Из этой общей оценки вытекают следующие утверждения.

Следствие 4.2. *Пусть m и A как в условиях теоремы 4.1. Тогда если $n = o(\frac{\log m}{\log\log m})$, то*

$$|A| \leqslant m^{1/2+o(1)};$$

если $n \leqslant (\frac{1}{3} - \varepsilon)\frac{\log m}{\log\log m}$, то

$$|A| \leqslant m^{1-1.5\varepsilon+o(1)}.$$

Следствие 4.3. *Существует абсолютная постоянная $c > 0$ такая, что*

$$|A| \leqslant me^{-c\log m/\log\log m}$$

для всех m и A, удовлетворяющим условиям теоремы 4.1.

[27] Cohen S.D., Clique numbers of Paley graphs, Quaestions Math., 11, 2, 225-231 (1998)

[28] Graham S., Ringrose C., Lower bounds for least quadratic non-residues, Analytic number theory (Allterton Park, IL), 269-309 (1989).

Следствие 4.4. *Существует множество $M \subset \mathbb{N}$ плотности 1 такое, что при всех $m \in M$ и любых $A \subset \mathbb{Z}_m$ таких, что $A - A$ не содержит квадратичных вычетов, справедлива оценка*

$$|A| \leqslant m^{1/2+o(1)}, \quad m \to \infty,\ m \in M.$$

Таким образом, мы усиливаем результат работы Ружи и Матолчи о квадратичных вычетах для общего случая бесквадратных модулей; при этом мы доказываем «почти корневую оценку» для почти всех модулей.

Заключение

В диссертации рассмотрены различные оценки сумм характеров и их приложения. Доказаны нетривиальные оценки сумм характеров по параллелепипедам достаточно большого объёма в конечных полях порядка p^2 и p^3. Получены нижние оценки винеровской нормы функций в дискретном многомерном случае (для группы $\mathbb{Z}_p^d$). Изучена задача о распределении квадратов во множестве конечного поля с ограничениями на коэффициенты при разложении по базису. Для почти всех модулей получены нетривиальные оценки на размер подмножества кольца вычетов, разность которого с собой не содержит квадратичных вычетов.

Дальнейшее развитие методов диссертации имеет перспективы в аналитической теории чисел и аддитивной комбинаторике.

Благодарности

Автор глубоко признателен своему научному руководителю Конягину Сергею Владимировичу за постановку задач и поддержку на протяжении всего научного пути.

Работы автора по теме диссертации:

Статьи в научных журналах Web of Science, Scopus

[1] М. Р. Габдуллин, “О подмножествах $\mathbb{Z}_m$, разность которых не содержит квадратов”, Матем. сб., 209:11 (2018), 60–68; M. R. Gabdullin, “Sets in $\mathbb{Z}_m$ whose difference sets avoid squares”, Sb. Math., 209:11 (2018), 1603–1610.

[2] М. Р. Габдуллин, “Оценки сумм характеров в конечных полях порядка p^2 и p^3”, Тр. МИАН, 303 (2018), 45–58; M. R. Gabdullin, “Estimates for character sums in finite fields of order p^2 and p^3”, Proc. Steklov Inst. Math., 303 (2018), 36–49.

[3] М. Р. Габдуллин, “О квадратах в специальных множествах конечного поля”, Чебышевский сб., 17:2 (2016), 56–63.

[4] М. Р. Габдуллин, “О квадратах во множестве элементов конечного поля с ограничениями на коэффициенты при разложении по базису”, Матем. заметки, 100:6 (2016), 807–824; M. R. Gabdullin, “On the Squares in the Set of Elements of a Finite Field with Constraints on the Coefficients of Its Basis Expansion”, Math. Notes, 101:2 (2017), 234–249.

Тезисы конференций:

М. Р. Габдуллин, Оценки винеровской нормы в $\mathbb{Z}_p^d$, Сборник тезисов Международной конференции ”Современные методы теории функций и смежные проблемы ”, Воронеж, 2019, с. 96-97.

М. Р. Габдуллин, “Нижние оценки винеровской нормы в $\mathbb{Z}_p^d$”, Сборник тезисов Международной конференции “Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории”, Тула, 2019, с. 183-184.