Московский государственный университет
имени М.В.Ломоносова
Механико-математический факультет

На правах рукописи

Габдуллин Михаил Рашидович

Суммы характеров: оценки и приложения

01.01.06 — математическая логика, алгебра и теория чисел

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата физико-математических наук

Научный руководитель
академик РАН, профессор С.В.Конягин

Москва, 2019

Содержание

Введение **3**
Краткое содержание **6**
Глава 1. Оценки сумм характеров в конечных полях порядка p^2 и p^3 . . **18**
Глава 2. Нижние оценки винеровской нормы в $\mathbb{Z}_p^d$ **34**
Глава 3. Пропущенные цифры в конечных полях **49**
Глава 4. Множества, разность которых не содержит квадратов **70**
Заключение **79**
Литература **79**

Введение

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 др.) 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 (см., например, [1], [4], [11]).

Цель работы.

Получение новых оценок сумм характеров по параллелепипедам в 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, 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, 2019 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 диссертации.

Структура и объём работы.

Диссертация состоит из четырёх глав, заключения и списка литературы из 63 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 при работе в лаборатории «Многомерная аппроксимация и приложения» МГУ им. М.В.Ломоносова (проект 14.W03.31.0031).

Краткое содержание диссертации

В диссертации получены следующие результаты (перечисляем их соответственно главам; для каждого утверждения указан его номер в основном тексте).

Глава 1.
Оценки сумм характеров в конечных полях порядка p^2 и p^3

В конечных полях различают аддитивные и мультипликативные характеры (характеры аддитивной и мультипликативной групп поля соответственно); при этом для мультипликативных характеров полагают $\chi(0) = 0$. 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» $B \subseteq \mathbb{F}_{p^n}$:

$$B = \left\{ \sum_{i=1}^{n} x_i \omega_i \,:\, N_i + 1 \leqslant x_i \leqslant N_i + H_i,\ \ 1 \leqslant i \leqslant n \right\}. \tag{0.1}$$

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 [19]: для любого $\varepsilon > 0$ 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 [20] также получил аналог этого неравества для базисов специального вида в случае $n = 2$, а Карацуба [5], [6] обобщил его оценки на произвольные конечные поля; так, например, в работе [6] рассматривается 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 Дэвенпортом и Льюисом [29].

Теорема А ([29]). *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 [27].

Теорема B ([27]). *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

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

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 [28] были получены нетривиальные оценки сумм характеров в случае $n = 2$, $H_1, H_2 > p^{1/4+\varepsilon}$. Конягин [8] обобщил последний результат на произвольные конечные поля.

Теорема C ([8]). *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 $\{\omega_1, \dots, \omega_n\}$ — 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, 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.
Нижние оценки винеровской нормы в $\mathbb{Z}_p^d$

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 [7] в 1981 году. В чуть более поздней работе [43] получен более общий результат: если $B = \{b_1 < \dots < b_n\}$ и $c(b_j) \in \mathbb{C}$ — произвольные комплексные числа, то

$$\int_0^1 \left| \sum_{b \in B} c(b) e(bx) \right| dx \gg \sum_{j=1}^{n} \frac{|c(b_j)|}{j} \tag{0.2}$$

Хорошо известно (см., например, [52], с.19), 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 [38], а также в ряде последующих работ [48], [9], [10], [47], [49] 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 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 $\|g\|_q:=(\sum_{x\in supp\, g}|g(x)|^q)^{1/q}$). Имеет место неравенство

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

откуда сразу следует, что

$$\|\widehat{fg}\|_1\leqslant\|\widehat{f}\|_1\|\widehat{g}\|_1. \tag{0.3}$$

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 $e_p(u)=e^{2\pi iu/p}$.

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

$$\|\widehat{A}\|_1\gg\log|A|, \tag{0.4}$$

аналогичная оценке (0.2) в непрерывном случае. Кроме того, применяя теорему Марцинкевича о дискретизации L_1-норм тригонометрических многочленов (см., например, [52], теорема 1.10), 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 (0.4) доказано Конягиным и Шкредовым для множеств малого размера.

Теорема D [9]. *Пусть* $A \subset \mathbb{Z}_p$ *и*

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

Тогда справедлива оценка (0.4).

Ими же получены следующие результаты.

Теорема E [10]. *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, в работе [9] было показано, что из результатов Сандерса [48] вытекает следующая оценка.

Теорема F [9]. *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 $\delta \asymp (\log p)^{-1}$ работает лишь теорема D и даёт слабые оценки снизу (порядка $(\log\log p)^{1/3}$). Шоен [47] 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 вытекает более сильная оценка $\|\widehat{A}\|_1 \gg (\log|A|)^{1/4-o(1)}$.

Теорема G [49]. *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* $x \in S := supp f$. *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* $x \in S := supp\, f$. *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

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

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 $\delta = |supp\, h|p^{-1}$. *Тогда для любой функции* $f\colon \mathbb{Z}_p^d \to E \cup \{0\}$ *такой, что* $|supp\, f| = \delta p^d$, $\delta \geqslant Cp^{-1}$, *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 [49] изучаются целозначные функции, в то время как в [9] и [10] 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 $|supp\, h| = \delta p < (2p)^{1/2}$, 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 $|supp f| = \delta p < (2p)^{1/2}$, 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.
Пропущенные цифры в конечных полях

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 (см., например, [15], [16], [22]-[26], [30], [31], [35], [36], [41]) изучались арифметические свойства чисел с "пропущенными" цифрами, т.е. тех чисел, b-ичная запись которых состоит из заданных цифр.

В [32] C. Dartyge и A. Sárközy 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.

В недавней работе C. Dartyge, C. Mauduit, A. Sárközy [33] 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* $\mathcal{D} = \{0, \dots, t-1\}$, *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 $t \gg \sqrt{p}\log p$.

Автором 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*

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

Кроме того, если $r \geqslant 20$, $C(r) = \exp\left(\frac{4\log r + 8}{r}\right)$ и $|\mathcal{D}| \geqslant C(r) p^{\frac{1}{2}} \exp\left(\frac{\log p + 4\log\log p}{r}\right)$, 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 (см., например, начало доказательства теоремы 3.1), 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 R.Dietmann, C.Elsholtz, I.E.Shaprlinski [34], была рассмотрена более общая задача. Пусть $D_1, \ldots, D_r$ – подмножества $\mathbb{F}_p$. Положим

$$W = W(D_1, \ldots, D_r) = \{x_1 a_1 + \ldots + x_r a_r \,|\, x_i \in D_i\}.$$

Авторы работы [34] отмечают, что доказательство теоремы H [33] 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 ([34], теорема 3.5). *Для любого $\varepsilon > 0$ существует $\delta > 0$ такое, что для любых множеств $D_1, \ldots, D_r$, удовлетворяющих условиям*

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

и

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

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

По аналогии с работой [34], 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.
Множества, разность которых не содержит квадратов

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

Л.Ловас предположил, что если последовательность $S \subset \mathbb{N}$ имеет положительную асимптотическую верхнюю плотность, то множество $S - S$ содержит точный квадрат. А. Шаркози [50] доказал это, показав, что если множество $B \subset [N] = \{1, \ldots, N\}$ 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 Я. Пинца, В.Л. Штайгера и Э. Семереди [44]. Метод этой работы также позволяет получить верхнюю оценку на размер множества, разность с собой которого не содержит k-х степеней; см. [13]. С другой стороны, И. Ружи [45] построил пример множества $B \subset [N]$, разность которого не содержит квадратов, и такого, что $|B| \gg N^{\gamma}$, где $\gamma = \frac{1}{2}(1 + \frac{\log 7}{\log 65}) = 0.733077\ldots$. 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 И. Ружи и М. Матолчи в их работе [42]. Напомним, что натуральное число m называется бесквадратным (или свободным от квадратов), если оно имеет вид $m = p_1 \cdot \ldots \cdot p_s$, где $p_1, \ldots, p_s$ — различные простые числа. В работе [42] 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 $\delta = 0.119\ldots$. Далее, авторы доказали, что если $A - A$ не содержит ненулевых квадратичных вычетов, то

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

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

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

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. С. Коэн [21] 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, С. Грэхем и С. Рингроуз [37] 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.

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 [42] о квадратичных вычетах для общего случая бесквадратных модулей; при этом мы доказываем «почти корневую оценку» для почти всех модулей.

Глава 1

Оценки сумм характеров в конечных полях порядка p^2 и p^3

В этой главе мы докажем следующую теорему.

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.

Ключевым моментом в доказательстве теорем B и C и теоремы 1.1 является оценка величины

$$E(B) = \#\{(x,y,w,t)\in B^4 : xy = wt\},$$

которую называют мультипликативной энергией множества B. В работе [27] методами аддитивной комбинаторики была доказана оценка $E(B) \ll_n |B|^{11/4}\log p$ для параллелепипедов с условием $H_i < \frac{1}{2}(\sqrt{p}-1)$ (см. [27], предложение 1), а в работе [8] с помощью соображений из геометрической теории чисел была получена оценка $E(B) \ll_n |B|^2\log p$ для параллелепипедов с условием $H_1 = \ldots = H_n \leqslant \sqrt{p}$ (см. [8], лемма 1). Обобщая рассуждения леммы 1 из [8] для случаев $n=2$ и $n=3$ и параллелепипедов с различными рёбрами, мы доказываем следующее утверждение.

Основная лемма. *Пусть* $n \in \{2,3\}$ *и* $H_1 \leqslant \ldots \leqslant H_n < \sqrt{p/2}$. *Тогда справедлива оценка*

$$E(B) \ll |B|^2 \log^3 p.$$

При доказательстве теоремы мы почти полностью следуем работе [27]; сначала мы доказываем требуемую оценку в случае, когда все рёбра параллелепипеда меньше $\sqrt{p/2}$ (эта часть рассуждений является ныне стандартной и использовалась в работах [27], [8], а впервые появилась в [5]); отсюда сразу вытекает утверждение теоремы и для случая, когда все рёбра не превосходят $p^{1/2+\varepsilon/2}$. После мы доказываем теорему в случае, когда $H_n > p^{1/2+\varepsilon/2}$. Отметим, что из доказательства теоремы видно, что в последнем случае на самом деле можно написать чуть лучшую оценку на сумму характеров, а именно, $\sum_{x\in B}\chi(x) \ll_\varepsilon |B|p^{-\varepsilon/3} + |B\cap \omega_n \mathbb{F}_p|$.

Мы доказываем теорему 1.1 и основную лемму в технически более сложном случае $n = 3$ (случай $n = 2$ аналогичен). В разделе 1.1 мы доказываем основную лемму, в разделе 1.2 — теорему 1.1.

1.1 Доказательство основной леммы

Сначала сведём оценку энергии произвольного параллелепипеда к оценке энергии симметричного параллелепипеда. Следующая лемма будет использоваться в главе 3, поэтому удобства дальнейшего изложения мы формулируем её сразу в общем в случае поля $\mathbb{F}_{p^n}$.

Лемма 1.2. *Пусть параллелепипед* $B \subset \mathbb{F}_{p^n}$ *определён как в (0.1) и*

$$B_0 = \left\{ \sum_{i=1}^n x_i\omega_i \,:\, -H_i \leqslant x_i \leqslant H_i,\ 1 \leqslant i \leqslant n \right\}.$$

Положим $Z = \frac{B_0\setminus\{0\}}{B_0\setminus\{0\}}$ *и* $f_0(z) = \#\{(x,y)\in B_0^2 : xz = y\}$. *Тогда*

$$E(B) \leqslant 3|B|^2 + \sum_{z\in Z} f_0^2(z).$$

Доказательство. Положим

$$Z' = \frac{B\setminus\{0\}}{B\setminus\{0\}} = \{z\in\mathbb{F}_{p^n} : \exists x,y\in B\setminus\{0\},\ xz = y\}.$$

Если $x^1,x^2,x^3,x^4 \in B$ таковы, что $x^1x^2 = x^3x^4$, причём $(x^1,x^4)\neq(0,0)$ и $(x^2,x^3)\neq(0,0)$, то для некоторого $z\in Z'$ имеем $x^1z = x^3$, $x^4z = x^2$. Поэтому

$$E(B) \leqslant 2|B|^2 + \sum_{z\in Z'} f^2(z), \tag{1.1}$$

где $f(z)$ — число решений уравнения $xz = y$ в переменных $x,y\in B$. Заметим, что если $(x_1,y_1),\ldots,(x_k,y_k)\in B^2$ — различные решения уравнения

$xz = y$, то $(0,0), (x_2 - x_1, y_2 - y_1), \ldots, (x_k - x_1, y_k - y_1)$ — различные решения того же уравнения в B_0^2. Поэтому $f(z) \leqslant f_0(z)$; кроме того, $f_0(z) = 1$ при $z \in \mathbb{F}_{p^3}^* \setminus Z$. Значит,

$$\sum_{z \in Z'} f^2(z) \leqslant \sum_{z \in Z} f_0^2(z) + |Z' \setminus Z|.$$

Так как $|Z'| \leqslant |B|^2$, то из неравества (1.1), получаем

$$E(B) \leqslant 3|B|^2 + \sum_{z \in Z} f_0^2(z).$$

Лемма доказана. $\square$

Таким образом, для доказательства основной леммы нам достаточно оценить сумму

$$S = \sum_{z \in Z} f_0^2(z)$$

(где B_0 определено как в лемме 1.2, но $n = 3$). Запишем S в виде

$$S = S_1 + S_2,$$

где

$$S_1 = \sum_{z \in Z \setminus \mathbb{F}_p} f_0^2(z). \tag{1.2}$$

и

$$S_2 = \sum_{z \in \mathbb{F}_p^*} f_0^2(z) \tag{1.3}$$

Утверждение основной леммы теперь вытекает из следующих двух лемм.

Лемма 1.3. *Справедлива оценка*

$$S_1 \ll |B|^2 \log p.$$

Лемма 1.4. *Справедлива оценка*

$$S_2 \ll |B|^2 \log^3 p.$$

1.1.1 Доказательство леммы 1.3

Для фиксированного $z \in Z$ определим решётку $\Gamma_z \subset \mathbb{Z}^6$:

$$\Gamma_z = \{(x_1, x_2, x_3, y_1, y_2, y_3) \in \mathbb{Z}^6 : z \sum_{i=1}^{3} x_i \omega_i = \sum_{i=1}^{3} y_i \omega_i\}.$$

При фиксированных $x_1, x_2, x_3 \in \mathbb{Z}$ условие $(x_1, x_2, x_3, y_1, y_2, y_3) \in \Gamma_z$ определяет вычет каждого из чисел y_1, y_2, y_3 по модулю p. Значит,

$$|\{(x_1,x_2,x_3,y_1,y_2,y_3)\in\Gamma_z : |x_i|,|y_i|\leqslant M, 1\leqslant i\leqslant 3\}| = \frac{(2M)^6}{p^3}(1+o(1)), \quad M\to\infty.$$

Следовательно,

$$\mathsf{mes}\ (\mathbb{R}^6/\Gamma_z) = p^3.$$

Пусть

$$D = \{(x_1,x_2,x_3,y_1,y_2,y_3)\in\mathbb{R}^6 : |x_i|,|y_i|\leqslant H_i,\ 1\leqslant i\leqslant 3\};$$

в этих обозначениях имеем $f_0(z) = |\Gamma_z\cap D|$. Напомним, что i-й последовательный минимум

$$\lambda_i = \lambda_i(z) = \lambda_i(D,\Gamma_z)$$

множества D относительно Γ_z определяется как минимальное число λ, при котором множество λD содержит i линейно независимых векторов решётки Γ_z. Очевидно, что $\lambda_1(z)\leqslant\ldots\leqslant\lambda_6(z)$, причём условие $\lambda_1(z)\leqslant 1$ равносильно тому, что $z\in Z$. Согласно второй теореме Минковского (см., например, [51], теорема 3.30)

$$\prod_{i=1}^{6}\lambda_i \gg \frac{\mathsf{mes}(\mathbb{R}^6/\Gamma_z)}{\mathsf{mes}D} \gg p^3|B|^{-2}. \tag{1.4}$$

Далее, хорошо известно (см. [17], предложение 2.1, а также [51], упражнение 3.5.6), что число $f_0(z)$ точек решётки Γ_z во множестве D удовлетворяет неравенству

$$f_0(z)\ll\prod_{i=1}^{6}\max\{1,\lambda_i^{-1}\}. \tag{1.5}$$

Получим теперь нижние оценки на величины $\lambda_1(z)$, $\lambda_2(z)$, $\lambda_3(z)$ для $z\in Z\setminus\mathbb{F}_p$.

Прежде всего, так как $z\in Z$, то $\lambda_1(z)\leqslant 1$. Кроме того, $H_2^{-1}\leqslant\lambda_1(z)$ (так как иначе найдётся ненулевой вектор $(0,0,u_3,0,0,u_6)\in\Gamma_z$ такой, что $|u_3|$, $|u_6|<H_3H_2^{-1}$ и $zu_3\omega_3 = u_6\omega_3$, но тогда $z\in\mathbb{F}_p$).

Далее, покажем, что $\lambda_2(z)\geqslant H_1^{-1}$. Если это не так, то найдутся два линейно независимых над $\mathbb{R}$ вектора $\mathbf{u} = (0,u_2,u_3,0,u_5,u_6)$, $\mathbf{v} = (0,v_2,v_3,0,v_5,v_6)\in\Gamma_z$ таких, что $|u_2|,|u_5|,|v_2|,|v_5|<H_2H_1^{-1}<\sqrt{p/2}$, $|u_3|,|u_6|,|v_3|,|v_6|<H_3H_1^{-1}<\sqrt{p/2}$, и

$$\begin{cases}(u_2\omega_2+u_3\omega_3)z = u_5\omega_2+u_6\omega_3\,,\\ (v_2\omega_2+v_3\omega_3)z = v_5\omega_2+v_6\omega_3.\end{cases} \tag{1.6}$$

Предположим, что векторы (u_2,u_3) и (v_2,v_3) линейно независимы над $\mathbb{F}_p$. Обозначим через $\mathsf{Lin}\{\omega_2,\omega_3\}$ подпространство, натянутое на векторы ω_2 и ω_3. Тогда равенства (1.6) означают, что умножение на элемент z биективно отображает $\mathsf{Lin}\{\omega_2,\omega_3\}$ на себя. Пусть

$$z\omega_1 = a_1\omega_1+a_2\omega_2+a_3\omega_3;$$

мы утверждаем, что $z = a_1$. Действительно, иначе умножение на элемент $z - a_1$ также биективно отображает подпространство $\mathsf{Lin}\{\omega_2, \omega_3\}$ на себя, откуда $\omega_1 \in \mathsf{Lin}\{\omega_2, \omega_3\}$, что неверно. Таким образом, $z = a_1$; но тогда мы получаем противоречие с тем, что $z \notin \mathbb{F}_p$.

Итак, векторы (u_2, u_3) и (v_2, v_3) линейно зависимы над $\mathbb{F}_p$. Это означает, что определитель матрицы $\begin{pmatrix} u_2 & u_3 \\ v_2 & v_3 \end{pmatrix}$ делится на p. С другой стороны, так как все её элементы по модулю меньше $\sqrt{p/2}$, то его модуль меньше p, откуда он равен нулю, то есть векторы (u_2, u_3) и (v_2, v_3) линейно зависимы над $\mathbb{Z}$.

Вектор $\mathbf{v} = (0, v_2, v_3, 0, v_5, v_6)$ ненулевой; предположим сначала, что $(v_2, v_3) \neq (0, 0)$, и пусть $v_2 \neq 0$. Умножая второе уравнение системы (1.6) на u_2/v_2 и вычитая его из первого, получим

$$(u_5 - v_5 u_2/v_2)\omega_2 + (u_6 - v_6 u_2/v_2)\omega_3 = 0.$$

Так как $\{\omega_1, \omega_2, \omega_3\}$ — базис, и $|u_5 v_2 - v_5 u_2| < p$, $|u_6 v_2 - v_6 u_2| < p$, то $u_5 u_2 - v_5 v_2 = u_6 u_2 - v_6 v_2 = 0$, откуда $\mathbf{u} = \frac{u_2}{v_2}\mathbf{v}$. Противоречие с тем, что векторы $\mathbf{u}$ и $\mathbf{v}$ линейно независимы над $\mathbb{R}$. Аналогичные рассуждения имеют место в случае $v_3 \neq 0$.

Если же $v_2 = v_3 = 0$, то $(v_5, v_6) \neq (0, 0)$ и, повторяя рассуждения выше с заменой z на $1/z$, получим, что векторы (v_5, v_6) и (u_5, u_6) линейно зависимы и точно так же получим противоречие.

Итак, для $z \in Z \setminus \mathbb{F}_p$ имеем $1 \geqslant \lambda_1(z) \geqslant H_2^{-1}$ и $\lambda_3(z) \geqslant \lambda_2(z) \geqslant H_1^{-1}$. Положим

$$Z_j = \{z \in Z \setminus \mathbb{F}_p : 2^{j-1} \leqslant H_2\lambda_1 < 2^j\}, \;\; 1 \leqslant j \leqslant J := \log_2 H_2 + 1.$$

Вектор $\mathbf{u} \in \lambda_1(z)D \cap \Gamma_z$, соответствующий элементу $z \in Z_j$, однозначно определяет элемент z: действительно, если $\mathbf{u} = (u_1, u_2, u_3, u_4, u_5, u_6)$, то, определив элементы $x, y \in \mathbb{F}_{p^3}$ равенствами $x = u_1\omega_1 + u_2\omega_2 + u_3\omega_3$, $y = u_4\omega_1 + u_5\omega_2 + u_6\omega_3$, будем иметь $z = xy^{-1}$. Следовательно, $|Z_j|$ не превосходит числа целых точек в параллелепипеде $2^j H_2^{-1} D$. Поэтому, полагая $j_1 = \log_2(H_2/H_1)$, имеем

$$|Z_j| \leqslant |2^j H_2^{-1} D \cap \mathbb{Z}^6| \ll \prod_{i=1}^{3} \max\{1, H_i 2^j H_2^{-1}\}^2 \leqslant \begin{cases} 2^{4j} H_3^2 H_2^{-2}, & \text{если } 1 \leqslant j < j_1; \\ |B|^2 2^{6j} H_2^{-6}, & \text{если } j_1 \leqslant j \leqslant J. \end{cases} \quad (1.7)$$

Положим $s = s(z) = \max\{j : \lambda_j \leqslant 1\}$ и $Z^s = \{z \in Z \setminus \mathbb{F}_p : s(z) = s\}$. Вспоминая определение (1.2) суммы S_1, имеем

$$S_1 \leqslant \sum_{s=1}^{6} \sum_{z \in Z^s} f_0^2(z).$$

Для $s \leqslant 3$ положим $Z_j^s = Z^s \cap Z_j$. Тогда

$$\sum_{z\in Z^s} f_0^2(z) \leqslant \sum_j \sum_{z\in Z_j^s} f_0^2(z).$$

Ниже мы часто будем пользоваться тривиальной оценкой $|Z_j^s| \leqslant |Z_j|$.

Пусть $s = 1$. Тогда в силу (1.5) имеем $f_0(z) \ll \lambda_1^{-1}$. Учитывая оценки (1.7) и, то, что при $z \in Z_j$ справедлива оценка $\lambda_1^{-1}(z) \ll 2^{-j}H_2$, получаем

$$\sum_j \sum_{z\in Z_j^1} f_0^2(z) \ll \sum_j \sum_{z\in Z_j^1} \lambda_1^{-2} \ll \sum_j |Z_j^1| 2^{-2j} H_2^2 \ll$$
$$\sum_{1\leqslant j<j_1} 2^{4j} H_3^2 H_2^{-2} 2^{-2j} H_2^2 + \sum_{j_1\leqslant j\leqslant J} |B|^2 2^{6j} H_2^{-6} 2^{-2j} H_2^2 \ll$$
$$H_3^2 \sum_{j\leqslant j_1} 2^{2j} + |B|^2 H_2^{-4} \sum_{j\leqslant J} 2^{4j} \ll |B|^2. \quad (1.8)$$

Пусть $s = 2$; тогда в силу (1.5) имеем $f_0(z) \leqslant \lambda_1^{-1}\lambda_2^{-1}$. Пусть $z \in Z_j$; при $j < j_1$ будем пользоваться оценками $\lambda_1^{-1} \ll 2^{-j}H_2$ и $\lambda_2^{-1} \leqslant H_1$, а при $j \geqslant j_1$ — оценкой $\lambda_2^{-1} \leqslant \lambda_1^{-1} \ll 2^{-j}H_2$. Учитывая также (1.7), получим

$$\sum_j \sum_{z\in Z_j^2} f_0^2(z) \ll \sum_j \sum_{z\in Z_j^2} \lambda_1^{-2}\lambda_2^{-2} \ll$$
$$\sum_{1\leqslant j<j_1} |Z_j^2| 2^{-2j} H_2^2 H_1^2 + \sum_{j_1\leqslant j\leqslant J} |Z_j^2| 2^{-4j} H_2^4 \ll$$
$$\sum_{j\leqslant j_1} 2^{4j} H_3^2 H_2^{-2} 2^{-2j} H_2^2 H_1^2 + \sum_{j\leqslant J} |B|^2 2^{6j} H_2^{-6} 2^{-4j} H_2^4 \ll |B|^2. \quad (1.9)$$

Пусть $s = 3$; тогда в силу (1.5) справедливо $f_0(z) \ll \lambda_1^{-1}\lambda_2^{-1}\lambda_3^{-1}$. Пусть $z \in Z_j$; при $j < j_1$ будем пользоваться оценками $\lambda_1^{-1} \ll 2^{-j}H_2$ и $\lambda_3^{-1} \leqslant \lambda_2^{-1} \leqslant H_1$, а при $j \geqslant j_1$ — оценкой $\lambda_3^{-1} \leqslant \lambda_2^{-1} \leqslant \lambda_1^{-1} \ll 2^{-j}H_2$.

Вновь используя (1.7), имеем

$$\sum_j \sum_{z\in Z_j^3} f_0^2(z) \ll \sum_j \sum_{z\in Z_j^3} \lambda_1^{-2}\lambda_2^{-2}\lambda_3^{-2} \ll$$
$$\sum_{1\leqslant j<j_1} 2^{4j} H_3^2 H_2^{-2} 2^{-2j} H_2^2 H_1^4 + \sum_{j_1\leqslant j\leqslant J} |B|^2 2^{6j} H_2^{-6} 2^{-6j} H_2^6 \ll |B|^2 \log p. \quad (1.10)$$

Пусть $s = 6$. Тогда, учитывая (1.4) и (1.5), получаем

$$\sum_{z\in Z^6} f_0^2(z) \ll \sum_{z\in Z} |B|^4 p^{-6} \leqslant |B|^2 |B|^4 p^{-6} \leqslant |B|^2 p^{4\cdot 1.5-6} = |B|^2 \quad (1.11)$$

(здесь $|B| \leqslant p^{1.5}$, так как $H_1 \leqslant H_2 \leqslant H_3 < \sqrt{p/2}$).

Разберём, наконец, случаи $s = 4$ и $s = 5$. Определим сопряженную решетку Γ_z^* следующим образом:

$$\Gamma_z^* = \left\{ (u_1, \dots, u_6) \in \mathbb{R}^6 : \sum_{i=1}^{3} u_i x_i + \sum_{i=1}^{3} u_{i+3} y_i \in \mathbb{Z} \quad \forall (x_1, \dots, y_3) \in \Gamma_z \right\}.$$

Так как $\Gamma_z \supseteq p\mathbb{Z}^6$, то $\Gamma_z^* \subseteq p^{-1}\mathbb{Z}^6$. Определим множество

$$D^* = \{(u_1, \dots, v_3) \in \mathbb{R}^6 : \sum_{i=1}^{3} |u_i x_i| + \sum_{i=1}^{3} |v_i y_i| \leqslant 1 \text{ при всех } (x_1, \dots, y_3) \in D\}$$

Ясно, что

$$D^* = \{(u_1, \dots, v_3) \in \mathbb{R}^6 : \sum_{i=1}^{3} (|u_i| + |v_i|) H_i \leqslant 1\}.$$

Пусть $\lambda_1^* = \lambda_1^*(z)$ — первый последовательный минимум множества D^* относительно Γ_z^*. Согласно предложению 3.6 из [14] имеем

$$\lambda_1^* \lambda_6 \ll 1. \tag{1.12}$$

Поэтому, учитывая (1.4) и (1.5), при $s = 5$ имеем

$$f_0(z) \ll \prod_{i=1}^{5} \lambda_i^{-1}(z) = \lambda_6(z) \prod_{i=1}^{6} \lambda_i^{-1}(z) \ll \lambda_6 |B|^2 p^{-3} \ll (\lambda_1^*)^{-1} |B|^2 p^{-3}, \tag{1.13}$$

а при $s = 4$ —

$$f_0(z) \ll \prod_{i=1}^{4} \lambda_i^{-1}(z) \leqslant \lambda_6^2 \prod_{i=1}^{6} \lambda_i^{-1}(z) \ll \lambda_6^2 |B|^2 p^{-3} \ll (\lambda_1^*)^{-2} |B|^2 p^{-3}. \tag{1.14}$$

Вклад в суммы $\sum_{z \in Z^5} f_0^2(z)$ (или $\sum_{z \in Z^4} f_0^2(z)$) от тех $z \in Z^5$ (соответственно $z \in Z^4$), для которых $\lambda_1^*(z) \geqslant 1$, оценивается так же, как в случае $s = 6$ (см. (1.11)). Поэтому можно считать, что $\lambda_1^*(z) \leqslant 1$. При этом легко видеть, что $\lambda_1^* \geqslant H_1 p^{-1}$ (так как если $\lambda < H_1 p^{-1}$, то в силу $\Gamma_z^* \subseteq p^{-1}\mathbb{Z}^6$ имеем $\lambda D^* \cap \Gamma_z^* = \{0\}$). Положим

$$Z_j' = \{z \in Z : 2^{j-1} \leqslant \frac{p\lambda_1^*(z)}{H_1} < 2^j\}, \ j = 1, ..., \log_2(p/H_1) + 1\}.$$

Покажем, что вектор $\mathbf{u} \in \lambda_1^*(z) D^* \cap \Gamma_z^*$, соответствующий элементу $z \in Z_j'$, однозначно определяет этот элемент z. Предположим противное: пусть нашелся ненулевой вектор $\mathbf{u} = (u_1/p, ..., v_3/p) \in \Gamma_{z'}^* \cap \Gamma_{z''}^*$, где $z' \neq z''$ и $u_i, v_i \in \mathbb{Z}$; при этом $\sum_{i=1}^3 |u_i| + \sum_{i=1}^3 |v_i| < 2^j$. Возьмём произвольный элемент $x = \sum_{i=1}^3 x_i \omega_i \in \mathbb{F}_{p^3}$ и положим $y' = xz' = \sum_{i=1}^3 y_i' \omega_i$, $y'' = xz'' = \sum_{i=1}^3 y_i'' \omega_i$; тогда

$$(x_1, x_2, x_3, y_1', y_2', y_3') \in \Gamma_{z'}, \ (x_1, x_2, x_3, y_1'', y_2'', y_3'') \in \Gamma_{z''},$$

а потому в силу определения сопряженной решетки имеем

$$\sum_{i=1}^{3} x_i u_i/p + \sum_{i=1}^{3} y_i' v_i/p \in \mathbb{Z},\ \sum_{i=1}^{3} x_i u_i/p + \sum_{i=1}^{3} y_i'' v_i/p \in \mathbb{Z}.$$

Но тогда

$$\sum_{i=1}^{3} (y_i' - y_i'') v_i \equiv 0 \pmod{p}.$$

Заметим, что числа $y_i' - y_i''$ могут быть произвольными (они суть коэффициенты разложения по базису элемента $y' - y''$, который равен $x(z' - z'')$ и который можно сделать произвольным за счет выбора x, так как $z' - z'' \neq 0$). Поэтому $v_i \equiv 0 \pmod{p}$, и так как $|v_i| < 2^j \leqslant p$, то $v_i = 0$. Но тогда

$$\sum_{i=1}^{3} x_i u_i = 0$$

при всех $(x_1, x_2, x_3) \in \mathbb{Z}^3$, откуда $u_i = 0$. Получаем противоречие с тем, что вектор $(u_1, \ldots, v_3)$ ненулевой. Таким образом, вектор $\mathbf{u} \in \lambda_1^*(z) D^* \cap \Gamma_z^*$, соответствующий элементу $z \in Z_j'$, действительно однозначно определяет этот элемент z.

Так как вектор $(u_1, \ldots, v_3) \in \frac{2^j H_1}{p} D^* \cap \Gamma_z^*$ удовлетворяет неравенству $\sum_{i=1}^{3} (|u_i| + |v_i|) H_i \leqslant 2^j H_1$, а следовательно, и неравенствам $|u_i|, |v_i| \leqslant 2^j H_1 H_i^{-1}$, то отсюда следует, что $|Z_j'| \leqslant \prod_{i=1}^{3} \max(1, 2^j H_1 H_i^{-1})^2$. Более точно, полагая $j_2 = \log_2(H_3/H_1)$ и $j_3 = \log_2(p/H_1) + 1$, имеем

$$|Z_j'| \leqslant \begin{cases} 2^{2j}, \text{ если } 1 \leqslant j < j_1; \\ 2^{4j} H_1^2 H_2^{-2}, \text{ если } j_1 \leqslant j < j_2; \\ 2^{6j} H_1^6 |B|^{-2}, \text{ если } j_2 \leqslant j \leqslant j_3. \end{cases} \tag{1.15}$$

Для $s = 4$ и $s = 5$ положим

$$Z_j^s = Z^s \cap Z_j';$$

ниже мы будем использовать тривиальную оценку $|Z_j^s| \leqslant |Z_j'|$ и затем применять неравенства (1.15). Вспоминая для случая $s = 5$ оценку (1.13) и

учитывая, что $\lambda_1^*(z) \asymp 2^j H_1/p$ при $z \in Z_j'$, имеем

$$\sum_{z\in Z^5} f_0^2(z) \leqslant |B|^4 p^{-6} \sum_j \sum_{z\in Z_j^5} (\lambda_1^*(z))^{-2} \leqslant$$
$$|B|^4 p^{-6} \sum_{1\leqslant j<j_1} 2^{2j-2j} H_1^{-2} p^2 + |B|^4 p^{-6} \sum_{j_1\leqslant j<j_2} H_1^2 H_2^{-2} 2^{4j-2j} H_1^{-2} p^2 +$$
$$|B|^4 p^{-6} \sum_{j_2\leqslant j\leqslant j_3} H_1^6 |B|^{-2} 2^{6j-2j} H_1^{-2} p^2 \leqslant$$
$$|B|^4 p^{-4} H_1^{-2} \log p + |B|^4 p^{-4} H_2^{-2} \sum_{j\leqslant j_2} 2^{2j} + |B|^2 p^{-4} H_1^4 \sum_{j\leqslant j_3} 2^{4j} \ll$$
$$|B|^2 (1 + |B|^2 p^{-4} H_3^4 |B|^{-2} + |B|^2 p^{-4} H_1^{-2} \log p) \ll |B|^2. \quad (1.16)$$

В случае $s = 4$ из оценки (1.14) аналогично получаем

$$\sum_{z\in Z^5} f_0^2(z) \leqslant |B|^4 p^{-6} \sum_j \sum_{z\in Z_j^5} (\lambda_1^*(z))^{-4} \leqslant$$
$$|B|^4 p^{-6} \sum_{1\leqslant j<j_1} 2^{2j-4j} H_1^{-4} p^4 + |B|^4 p^{-6} \sum_{j_1\leqslant j<j_2} H_1^2 H_2^{-2} 2^{4j-4j} H_1^{-4} p^4 +$$
$$|B|^4 p^{-6} \sum_{j_2\leqslant j\leqslant j_3} H_1^6 |B|^{-2} 2^{6j-4j} H_1^{-4} p^4 \leqslant$$
$$|B|^4 p^{-2} H_1^{-4} + |B|^4 p^{-2} H_1^{-2} H_2^{-2} \sum_{j\leqslant j_2} 1 + |B|^2 p^{-2} H_1^2 \sum_{j\leqslant j_3} 2^{2j} \ll$$
$$|B|^2 (1 + |B|^2 p^{-2} H_3^2 (\log p) |B|^{-2} + |B|^2 p^{-2} H_1^{-4}) \ll |B|^2. \quad (1.17)$$

Собирая оценки (1.8)-(1.11) и (1.16)-(1.17), получаем, что

$$S_1 \ll |B|^2 \log p.$$

Лемма 1.3 доказана. $\square$

1.1.2 Доказательство леммы 1.4

Пусть $z \in \mathbb{F}_p$. Если $x = \sum_{i=1}^3 x_i\omega_i$, $y = \sum_{i=1}^3 y_i\omega_i$, то равенство $xz = y$ равносильно равенствам $zx_i \equiv y_i \pmod p$, $1 \leqslant i \leqslant 3$. Поэтому

$$f_0(z) = f_1(z) f_2(z) f_3(z),$$

где

$$f_i(z) = \#\{(x_i, y_i) \in [-H_i, H_i]^2 : x_i z \equiv y_i \pmod p\}.$$

Вспоминая определение (1.3) суммы S_2, имеем

$$S_2 = \sum_{z\in\mathbb{F}_p^*} f_0^2(z) = \sum_{z\in\mathbb{F}_p^*} f_1^2(z) f_2^2(z) f_3^2(z) \leqslant \prod_{i=1}^3 \left(\sum_{z\in\mathbb{F}_p^*} f_i^2(z) \right). \quad (1.18)$$

Суммы $\sum_{z\in\mathbb{F}_p^*} f_i^2(z)$ оцениваются по аналогии с суммой S_1. Повторим эти рассуждения. Зафиксируем $i\in\{1,2,3\}$, и пусть $H=H_i$,

$$D=[-H,H]^2,\qquad Z=\frac{[-H,H]\setminus 0}{[-H,H]\setminus 0},$$

$$\Gamma_z=\{(x,y)\in\mathbb{Z}^2:\ xz\equiv y\pmod p\},$$

и $\lambda_l=\lambda_l(z)$ — l-й последовательный минимум D относительно Γ_z, $l=1,2$. Тогда для всех $z\in\mathbb{F}_p^*$ имеем

$$\mathsf{mes}(\mathbb{R}^2/\Gamma_z)=p,$$

и потому в силу теоремы Минковского

$$\lambda_1\lambda_2\gg pH^{-2}. \tag{1.19}$$

Во введённых обозначениях $f_i(z)=|D\cap\Gamma_z|$, так что в силу предложения 2.1 из [17] имеем

$$f_i(z)\ll\prod_{l=1}^{2}\max\{1,\lambda_l^{-1}(z)\}.$$

Кроме того, ясно, что $H^{-1}\leqslant\lambda_1\leqslant 1$ при $z\in Z$. Положим

$$Z_j=\{z\in Z:2^{j-1}\leqslant H\lambda_1(z)<2^j\},\ j=1,\dots,[\log_2 H]+1,$$

$s(z)=\max\{l:\lambda_l(z)\leqslant 1\}$, и $Z^s=\{z\in Z:\ s(z)=s\}$. Так как вектор $(u_1,u_2)\in\lambda_1(z)D\cap\Gamma_z$, соответствующий элементу $z\in Z_j$, однозначно определяет этот элемент, то

$$|Z_j|\ll\left|\frac{2^j}{H}D\cap\mathbb{Z}^2\right|\ll 2^{2j}.$$

Поэтому

$$\sum_{z\in Z^1}f_i^2(z)\ll\sum_j\sum_{z\in Z^1\cap Z_j}\lambda_1^{-2}(z)\ll\sum_{j=1}^{[\log_2 H]+1}2^{2j}H^2 2^{-2j}\ll H^2\log p. \tag{1.20}$$

Далее, в силу (1.19) и того, что $H\leqslant\sqrt{p}$, имеем

$$\sum_{z\in Z^2}f_i^2(z)\ll|Z^2|p^{-2}H^4\leqslant H^6p^{-2}\leqslant H^2. \tag{1.21}$$

Собирая оценки (1.20) и (1.21), получаем

$$\sum_{z\in\mathbb{F}_p^*}f_i^2(z)\ll H^2\log p.$$

Подставляя эту оценку в (1.18), получаем

$$S_2\ll\prod_{i=1}^{3}(H_i^2\log p)=|B|^2\log^3 p.$$

Тем самым лемма 1.4 и основная лемма доказаны. $\square$

1.2 Доказательство теоремы 1.1.

В этом разделе мы почти полностью следуем работе [27]. Отметим, однако, что рассуждения в случае $H_3 < \sqrt{p/2}$ («аддитивный сдвиг» переменной суммирования вида $x \mapsto x + yz$ с последующим двукратным применением неравенства Гёльдера) являются ныне стандартными и использовались в [27], [8], а впервые появились в работе Карацубы [5]. Сам же аддитивный сдвиг использовался и ранее в работах Виноградова (см. [2], [3], [4]) и восходит, вероятно, к идеям ван дер Корпута и Г.Вейля (см., например, [54], [57], [58]).

1.2.1 Случай $H_3 < \sqrt{p/2}$.

Разбивая B на меньшие параллелепипеды, можно считать, что $|B| \asymp p^{3(1/4+\varepsilon)}$. Пусть $\delta = \delta(\varepsilon) > 0$ — число, которое мы определим позже. Положим

$$I = [1, p^{\delta}] \cap \mathbb{Z}$$

и

$$B_0 = \left\{ \sum_{i=1}^{3} x_i \omega_i : \ x_i \in [0, p^{-2\delta} H_i] \cap \mathbb{Z}, \ 1 \leqslant i \leqslant 3 \right\}.$$

Заметим, что $\#([0, p^{-2\delta} H_i] \cap \mathbb{Z}) \asymp 1 + p^{-2\delta} H_i \gg p^{-2\delta} H_i$, и, значит, справедлива оценка

$$|B_0| \gg p^{-6\delta} |B|. \tag{1.22}$$

Так как $B_0 I \subseteq \left\{ \sum_{i=1}^{3} x_i \omega_i : \ x_i \in [0, p^{-\delta} H_i] \cap \mathbb{Z}, \ 1 \leqslant i \leqslant 3 \right\}$, то при всех $y \in B_0$, $z \in I$ имеем

$$\left| \sum_{x \in B} \chi(x) - \sum_{x \in B} \chi(x + yz) \right| \leqslant |B \setminus (B + yz)| + |(B + yz) \setminus B| \leqslant 6 p^{-\delta} |B|.$$

Поэтому

$$\sum_{x \in B} \chi(x) = \frac{1}{|B_0||I|} \sum_{x \in B, y \in B_0, z \in I} \chi(x + yz) + O(p^{-\delta} |B|). \tag{1.23}$$

Далее,

$$\left| \sum_{x \in B, y \in B_0, z \in I} \chi(x + yz) \right| \leqslant \sum_{x \in B, y \in B_0} \left| \sum_{z \in I} \chi(x + yz) \right| \leqslant$$

$$\sum_{x \in B, y \in B_0 \setminus \{0\}} \left| \sum_{z \in I} \chi(x y^{-1} + z) \right| + |B||I| =$$

$$\sum_{u \in \mathbb{F}_{p^3}} \tau(u) \left| \sum_{z \in I} \chi(u + z) \right| + |B||I|,$$

где

$$\tau(u) = \#\{(x,y) \in B \times (B_0 \setminus \{0\}) : xy^{-1} = u\}.$$

Пусть r — некоторое натуральное число. Дважды используя неравенство Гёльдера, имеем

$$\left|\sum_{x\in B, y\in B_0, z\in I} \chi(x+yz)\right| \leqslant$$

$$\left(\sum_{u\in\mathbb{F}_{p^3}} \tau(u)\right)^{1-1/r} \left(\sum_{u\in\mathbb{F}_{p^3}} \tau(u)\left|\sum_{z\in I}\chi(u+z)\right|^r\right)^{1/r} + |B||I| \leqslant$$

$$\left(\sum_{u\in\mathbb{F}_{p^3}} \tau(u)\right)^{1-1/r} \left(\sum_{u\in\mathbb{F}_{p^3}} \tau^2(u)\right)^{1/(2r)} \left(\sum_{u\in\mathbb{F}_{p^3}} \left|\sum_{z\in I}\chi(u+z)\right|^{2r}\right)^{1/(2r)} + |B||I|. \tag{1.24}$$

Оценим теперь каждую из трёх появившихся сумм. Прежде всего,

$$\sum_{u\in\mathbb{F}_{p^3}} \tau(u) = |B|(|B_0|-1) \leqslant |B||B_0|. \tag{1.25}$$

Далее, $\tau(0) \leqslant |B_0|$ и поэтому

$$\tau^2(0) \leqslant |B_0|^2 \leqslant |B||B_0|.$$

Пользуясь неравенством Коши-Буняковского и основной леммой, получаем

$$\sum_{u\in\mathbb{F}^*_{p^3}} \tau^2(u) = \#\{(x_1,x_2,y_1,y_2) \in B\times B\times B_0\times B_0 \,:\, x_1y_2 = x_2y_1 \neq 0\} =$$

$$\sum_{\nu\in\mathbb{F}^*_{p^3}} \#\{(x_1,x_2)\in B^2 : \frac{x_1}{x_2} = \nu\}\#\{(y_1,y_2)\in B_0^2 : \frac{y_1}{y_2} = \nu\} \leqslant$$

$$E(B)^{1/2}E(B_0)^{1/2} \ll |B||B_0|\log^3 p.$$

Собирая вместе два последних неравенства, получаем для второй суммы оценку

$$\sum_{u\in\mathbb{F}_{p^3}} \tau^2(u) \ll |B||B_0|\log^3 p. \tag{1.26}$$

Для оценки третьей суммы используем следующую теорему.

Теорема K ([46], теорема 2C', стр.43). *Пусть χ — мультипликативный характер в $\mathbb{F}_{p^n}$ порядка $d > 1$. Предположим, что многочлен $f \in \mathbb{F}_{p^n}[x]$ имеет m различных корней и не является d-й степенью. Тогда*

$$\left|\sum_{x\in\mathbb{F}_{p^n}} \chi(f(x))\right| \leqslant (m-1)p^{n/2}.$$

Имеем

$$\sum_{u\in\mathbb{F}_{p^3}}\left|\sum_{z\in I}\chi(u+z)\right|^{2r}\leqslant$$

$$\sum_{z_1,\dots,z_{2r}\in I}\left|\sum_{u\in\mathbb{F}_{p^3}}\chi\left((u+z_1)\dots(u+z_r)(u+z_{r+1})^{q-2}\dots(u+z_{2r})^{q-2}\right)\right|.$$

Назовём набор $(z_1,\dots,z_{2r})$ *хорошим*, если хотя бы один из его элементов встречается в нём ровно один раз, и *плохим* иначе. Согласно теореме K для любого хорошего набора $(z_1,\dots,z_{2r})$ имеет место оценка

$$\left|\sum_{u\in\mathbb{F}_{p^3}}\chi\left((u+z_1)\dots(u+z_r)(u+z_{r+1})^{q-2}\dots(u+z_{2r})^{q-2}\right)\right|<2rp^{3/2}.$$

Оценивая число хороших наборов тривиально величиной $|I|^{2r}$, видим, что вклад от них не превосходит $2rp^{3/2}|I|^{2r}$. Далее, в любом плохом наборе каждый элемент встретился по крайней мере дважды, то в нём заведомо не более r различных элементов; их можно выбрать не более $|I|^r$ способами, и поэтому количество плохих наборов не превосходит $|I|^r r^{2r}$. Оценивая вклад от каждого плохого набора тривиально числом p^3, видим, что вклад от плохих наборов не превосходит $p^3|I|^r r^{2r}$. Таким образом,

$$\sum_{u\in\mathbb{F}_{p^3}}\left|\sum_{z\in I}\chi(u+z)\right|^{2r}\leqslant 2rp^{3/2}|I|^{2r}+p^3|I|^r r^{2r},$$

откуда

$$\left(\sum_{u\in\mathbb{F}_{p^3}}\left|\sum_{z\in I}\chi(u+z)\right|^{2r}\right)^{1/(2r)}\ll p^{3/(4r)}|I|+p^{3/(2r)}|I|^{1/2}r. \qquad (1.27)$$

Подставляя оценки (1.25)-(1.27) в (1.24), получим

$$\frac{1}{|B_0||I|}\left|\sum_{x\in B,y\in B_0,z\in I}\chi(x+yz)\right|\ll$$

$$\frac{1}{|B_0||I|}\left(|B||B_0|\right)^{1-\frac{1}{r}}\left(|B||B_0|\log^3 p\right)^{\frac{1}{2r}}\left(p^{3/(4r)}|I|+rp^{3/(2r)}|I|^{1/2}\right)+|B||B_0|^{-1}$$

$$=|B|\left(|B||B_0|\right)^{-1/(2r)}(\log p)^{3/(2r)}\left(p^{3/(4r)}+rp^{3/(2r)}|I|^{-1/2}\right)+|B||B_0|^{-1}.$$

Вспоминая оценку (1.22) и предположение относительно величины $|B|$ и

учитывая, что $|I| \gg_\varepsilon p^\delta/2$ (напомним, что $\delta = \delta(\varepsilon)$), имеем

$$\frac{1}{|B_0||I|}\left|\sum_{x\in B, y\in B_0, z\in I}\chi(x+yz)\right| \ll_\varepsilon$$
$$|B|p^{-3/(4r)-3(\varepsilon-\delta)/r}(\log p)^{3/(2r)}\left(p^{3/(4r)}+rp^{3/(2r)-\delta/2}\right)+O(p^{6\delta}).$$

Положим $\delta = \frac{3}{2r}$. Тогда

$$\frac{1}{|B_0||I|}\left|\sum_{x\in B, y\in B_0, z\in I}\chi(x+yz)\right| \ll_\varepsilon |B|rp^{-3(\varepsilon-\delta)/r}(\log p)^{3/(2r)}+O(p^{6\delta}).$$

Вспоминая (1.23) и учитывая, что $3/r = 2\delta$, получаем

$$\left|\sum_{x\in B}\chi(x)\right| \ll_\varepsilon |B|rp^{-2\delta(\varepsilon-\delta)}(\log p)^\delta + p^{6\delta} + |B|p^{-\delta}. \qquad (1.28)$$

Выберем r так, чтобы $\delta = 3/(2r)$ было близко к $\varepsilon/2$. Пусть r — ближайшее целое к $3\varepsilon^{-1}$; тогда

$$\left|r - \frac{3}{\varepsilon}\right| \leqslant 1/2$$

и

$$r = 3\varepsilon^{-1} + 0.5\theta,$$

где $|\theta| \leqslant 1$. Поэтому

$$\delta = \frac{3}{2r} = \frac{3}{2(3\varepsilon^{-1}+0.5\theta)} = \frac{\varepsilon}{2+\theta\varepsilon/3},$$

откуда $\frac{1}{3}\varepsilon < \frac{6}{13}\varepsilon \leqslant \delta \leqslant \frac{6}{11}\varepsilon$ (ибо можно считать, что $\varepsilon < 1/2$). Так как $|B| \gg p^{3/4+3\varepsilon}$, то отсюда $p^{6\delta} \ll |B|p^{-\delta} \leqslant |B|p^{-\varepsilon/3}$ и мы можем переписать (1.28) в виде

$$\left|\sum_{x\in B}\chi(x)\right| \ll_\varepsilon |B|p^{-2\delta(\varepsilon-\delta)}(\log p)^\delta + |B|p^{-\varepsilon/3}.$$

Наконец,

$$2\delta(\varepsilon-\delta) \geqslant 2(6\varepsilon/13)(5\varepsilon/11) = 60\varepsilon^2/143 > \varepsilon^2/3.$$

Отсюда

$$\left|\sum_{x\in B}\chi(x)\right| \ll_\varepsilon |B|p^{-\varepsilon^2/3}.$$

Таким образом, в случае $H_3 \leqslant \sqrt{p/2}$ теорема доказана.

1.2.2 Случай $H_3 \leqslant p^{1/2+\varepsilon/2}$.

В этом случае можем разбить каждое ребро, имеющее длину больше, чем $\sqrt{p/2}$, на $O(p^{\varepsilon/2})$ «почти одинаковых» кусков длины меньше $\sqrt{p/2}$, но больше $\sqrt{p}/2$; тем самым B можно разбить на не более чем $O((p^{\varepsilon/2})^3)$ параллелепипедов B_α объема $\gg p^{-3\varepsilon/2}p^{3(1/4+\varepsilon)} = p^{3(1/4+\varepsilon/2)}$. По доказанному выше

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

при всех α, и потому

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

1.2.3 Случай $H_3 > p^{1/2+\varepsilon/2}$.

Будем пользоваться следующей теоремой, являющейся обобщением теоремы 1 из [40].

Теорема L([27]) *Пусть χ — нетривиальный мультипликативный характер в $\mathbb{F}_{p^n}$, и $g \in \mathbb{F}_{p^n}$ — примитивный элемент расширения $\mathbb{F}_{p^n}$ поля $\mathbb{F}_p$, то есть $\mathbb{F}_{p^n} = \mathbb{F}_p(g)$. Тогда для любого интервала $I \subseteq [1,p]\cap\mathbb{Z}$ справедлива оценка*

$$\left|\sum_{t\in I}\chi(g+t)\right| \leqslant c(n)\sqrt{p}\log p.$$

Заметим, что

$$\left|\sum_{x\in B}\chi(x)\right| = \left|\sum_{(x_1,x_2)\in I_1\times I_2}\sum_{x_3\in I_3}\chi(x_1\frac{\omega_1}{\omega_3}+x_2\frac{\omega_2}{\omega_3}+x_3)\right|. \qquad (1.29)$$

Пусть $I_i = [N_i+1, N_i+H_i]\cap\mathbb{Z}$ и

$$A = \left\{(x_1,x_2)\in I_1\times I_2 \,:\, \mathbb{F}_p(x_1\frac{\omega_1}{\omega_3}+x_2\frac{\omega_2}{\omega_3}) \neq \mathbb{F}_{p^3}\right\}.$$

Так как число 3 — простое, то у поля $\mathbb{F}_{p^3}$ нет нетривиальных подполей, кроме $\mathbb{F}_p$, и поэтому

$$A = \left\{(x_1,x_2)\in I_1\times I_2 \,:\, x_1\frac{\omega_1}{\omega_3}+x_2\frac{\omega_2}{\omega_3} \in \mathbb{F}_p\right\}.$$

Далее, элементы $1, \frac{\omega_1}{\omega_3}, \frac{\omega_2}{\omega_3}$ линейно независимы над $\mathbb{F}_p$, и, значит, $x_1\frac{\omega_1}{\omega_3} + x_2\frac{\omega_2}{\omega_3} \in \mathbb{F}_p$ только при $x_1 = x_2 = 0$. Таким образом,

$$A = \begin{cases}\varnothing, \text{ если } 0\notin I_1\cap I_2\\ \{(0,0)\}, \text{ если } 0\in I_1\cap I_2.\end{cases}$$

Вернемся теперь к равенству (1.29). Если пара (x_1, x_2) не попала в A, то в силу теоремы L и предположения на H_3 имеем

$$\left|\sum_{x_3\in I_3}\chi(x_1\frac{\omega_1}{\omega_3}+x_2\frac{\omega_2}{\omega_3}+x_3)\right|\ll\sqrt{p}\log p\leqslant H_3p^{-\varepsilon/2}\log p.$$

Отсюда, оценивая число пар (x_1, x_2), не попавших в A, тривиально величиной $|I_1||I_2|$, получаем

$$\left|\sum_{(x_1,x_2)\in(I_1\times I_2)\setminus D}\sum_{x_3\in I_3}\chi(x_1\omega_1+x_2\omega_2+x_3\omega_3)\right|\ll_\varepsilon|B|p^{-\varepsilon/3}.$$

Таким образом, в случае $0\notin I_1\cap I_2$ теорема доказана. Пусть теперь $0\in I_1\cap I_2$. В силу предыдущих рассуждений достаточно оценить сумму

$$S'=\sum_{x_3\in I_3}\chi(x).$$

Если $\chi|_{\mathbb{F}_p}$ — нетривиальный характер, то ввиду неравенства Пойя-Виноградова и предположения на H_3 имеем

$$|S'|\leqslant\sqrt{p}\log p\ll_\varepsilon H_3p^{-\varepsilon/3}\ll_\varepsilon|B|p^{-\varepsilon/3}.$$

Таким образом, теорема доказана и в случае, когда $0\in I_1\cap I_2$ и $\chi|_{\mathbb{F}_p}$ — нетривиальный характер.

Пусть, наконец, $\chi|_{\mathbb{F}_p}$ — тривиальный характер. Тогда

$$|S'|\leqslant H_3,$$

и, таким образом, в случае $H_3\geqslant p^{1/2+\varepsilon/2}$ всегда имеем

$$\left|\sum_{x\in B}\chi(x)\right|\ll_\varepsilon|B|p^{-\varepsilon/3}+H_3.$$

Теорема 1.1 полностью доказана. $\square$

Глава 2

Нижние оценки винеровской нормы

В этой главе мы доказываем следующие четыре теоремы. Первые две из них обобщают теоремы D и E соответственно.

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

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

Другие две теоремы настоящей главы посвящены перенесению одномерных результатов на многомерный случай.

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

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

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

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* $|supp\, h| = \delta p < (2p)^{1/2}$, *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* $|suppf| = \delta p < (2p)^{1/2}$, *справедливо*

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

Доказательства теорем 2.1 и 2.2 повторяют доказательства теорем D и E с некоторыми техническими изменениями.

Для доказательства теоремы 2.3 мы с помощью комбинаторных соображений находим в $\mathbb{Z}_p^d$ прямую, пересечение носителя функции f с которой имеет примерно ту же плотность в этой прямой, что и $supp\, f$ в $\mathbb{Z}_p^d$, а затем показываем, что винеровская норма функции в $\mathbb{Z}_p^d$ не меньше винеровской нормы своего сужения на любую прямую. При доказательстве теоремы 2.4 мы при помощи невырожденного линейного преобразования сводим всё к случаю, где первые координаты элементов множества $supp\, f$ различны, а затем применяем предположение на оценки в одномерном случае.

2.1 Доказательства теорем 2.1 и 2.2

Мы следуем работам [9] и [10].

Прежде всего, заметим, что из формулы обращения преобразования Фурье

$$f(x) = \sum_{\xi \in \mathbb{Z}_p} \widehat{f}(\xi) e_p(\xi x)$$

немедленно следует, что

$$M = \max_{x \in \mathbb{Z}_p} |f(x)| \leqslant \sum_{\xi \in \mathbb{Z}_p} |\widehat{f}(\xi)| = \|\widehat{f}\|_1, \tag{2.1}$$

и тем самым первые неравенства в утверждениях теорем 2.1 и 2.2 доказано. Кроме того, отсюда мы видим, что при получении нижних оценок на $\|\widehat{f}\|_1$ можно считать, что f принимает не слишком большие значения.

2.1.1 Доказательство теоремы 2.1

Напомним необходимые определения.

Пусть G — конечная абелева группа. Для произвольной функции $g\colon G \to \mathbb{C}$ определим величину

$$T_k(g) := \sum_{x_1+\ldots+x_k=x'_1+\ldots+x'_k} g(x_1)\ldots g(x_k)\overline{g(x'_1)}\ldots\overline{g(x'_k)}.$$

Нетрудно показать, что

$$T_k(g) = |G|^{2k-1}\sum_{\gamma}|\widehat{g}(\gamma)|^{2k}. \qquad (2.2)$$

Далее, множество $\Lambda = \{\lambda_1,\ldots,\lambda_\Lambda\} \subseteq G$ называется диссоциативным, если из того, что

$$\sum_{\lambda\in\Lambda}\varepsilon_\lambda\lambda = 0$$

для некоторых чисел $\varepsilon_\lambda \in \{-1,0,1\}$, вытекает, что все ε_λ равны нулю. Пусть $S \subseteq G$; размер максимального диссоциативного подмножества множества S называется *аддитивной размерностью* множества S и обозначается $\dim S$.

Лемма 2.5. *Пусть G — конечная абелева группа, $f\colon G \to \mathbb{C}$ и $\|\widehat{f}\|_1 \leqslant K$. Пусть, далее, множество $Q \subseteq S$ таково, что $|f(x)| \geqslant L$ при $x \in Q$, и $g(x) = Q(x)f(x)$. Тогда при всех $k \in \mathbb{N}$ справедливо*

$$T_k(g) \geqslant \frac{|Q|^{2k}L^{4k}}{\|f\|_2^2K^{2k-2}}\,.$$

Доказательство. Применяя поочередно оценку снизу на $|f(x)|$ при $x \in Q$, теорему Планшереля, и неравенство Гёльдера с показателями $2k$ и $2k/(2k-1)$, получаем

$$|Q|^{2k}L^{4k} \leqslant \left(\sum_x g(x)\overline{f(x)}\right)^{2k} \leqslant \left(|G|\sum_\gamma|\widehat{g}(\gamma)||\widehat{f}(\gamma)|\right)^{2k} \leqslant$$
$$\leqslant |G|^{2k}\sum_\gamma|\widehat{g}(\gamma)|^{2k}\left(\sum_\gamma|\widehat{f}(\gamma)|^{2k/(2k-1)}\right)^{2k-1}.$$

Записывая $|\widehat{f}(\gamma)|^{2k/(2k-1)}$ в виде $|\widehat{f}(\gamma)|^{(2k-2)/(2k-1)}|\widehat{f}(\gamma)|^{2/(2k-1)}$ и применяя неравенство Гёльдера с показателями $(2k-1)/(2k-2)$ и $2k-1$, а также пользуясь (2.2) и оценкой сверху на $|f(x)|$ при $x \in S$, имеем

$$|Q|^{2k}L^{4k} \leqslant |G|T_k(g)\left(\sum_\gamma|\widehat{f}(\gamma)|\right)^{2k-2}\sum_\gamma|\widehat{f}(\gamma)|^2 \leqslant$$
$$T_k(g)K^{2k-2}\sum_x|f(x)|^2 = T_k(g)K^{2k-2}\|f\|_2^2.$$

Лемма доказана. $\square$

Лемма 2.6. *Пусть G — конечная абелева группа, $S \subset G$ — произвольное множество и функция $f\colon G \to \mathbb{C}$ такова, что $|f(x)| \geqslant 1$ при $x \in S = supp f$ и $\|\widehat{f}\|_1 \leqslant K \leqslant \|f\|_2$. Тогда справедлива оценка*

$$\dim S \ll K^2 \left(1 + \log \frac{\|f\|_2}{K}\right).$$

Доказательство. Пусть Λ — максимальное диссоциативное подмножество множества S, и

$$\Lambda_j = \{x \in \Lambda : 2^{j-1} \leqslant |f(x)| < 2^j\}, \qquad j = 1, 2, \ldots.$$

Применим предыдущую лемму, взяв в качестве Q множество Λ_j; имеем (здесь $g_j(x) = \Lambda_j(x) f(x)$)

$$\frac{|\Lambda_j|^{2k} 2^{4(j-1)k}}{\|f\|_2^2 K^{2k-2}} \leqslant T_k(g_j) \leqslant T_k(|g_j|) \leqslant 2^{2jk} T_k(\Lambda_j).$$

Хорошо известное неравенство Рудина гласит, что для любого диссоциативного множества Λ справедлива оценка $T_k(\Lambda) \leqslant (Ck)^k |\Lambda|^k$, где $C > 0$ — абсолютная постоянная (см., например, [51]: нужное неравенство вытекает из оценки (4.34) и определения 4.26 $\Lambda(p)$-констант). Множества Λ_j, будучи подмножествами диссоциативного множества Λ, сами диссоциативны; поэтому

$$|\Lambda_j|^k \leqslant (2^{-2j+4} Ck)^k \|f\|_2^2 K^{2k-2},$$

откуда

$$|\Lambda_j| \ll 2^{-2j} K^2 \exp\left(\log k + \frac{2}{k} \log \frac{\|f\|_2}{K}\right).$$

Полагая $k := [2 \log \frac{\|f\|_2}{K}] + 1$, получаем

$$|\Lambda_j| \ll 2^{-2j} K^2 \left(1 + \log \frac{\|f\|_2}{K}\right).$$

Суммируя по всем $j \geqslant 1$ и вспоминая, что $|\Lambda| = \dim S$, получаем требуемое. $\square$

Замечание. *В силу неравенства Коши-Буняковского и равенства Парсеваля имеем*

$$\|\widehat{f}\|_1 \leqslant p^{1/2} \left(\sum_\gamma |\widehat{f}(\gamma)|^2\right)^{1/2} = \left(\sum_x |f(x)|^2\right)^{1/2} = \|f\|_2,$$

поэтому ограничение $K \leqslant \|f\|_2$ в предложении 1 не является обременительным.

Теперь докажем теорему 2.1. Неравенство (2.1) даёт первое неравенство в утверждении теоремы; кроме того, из него следует, что при доказательстве второго неравенства мы можем ограничиться случаем $M = \max_{x\in\mathbb{Z}_p} |f(x)| \leqslant \log|S|$.

Положим $K := \|\widehat{f}\|_1$. Пусть $c > 0$ — достаточно малая абсолютная постоянная. Можно считать, что $K^2 \log|S| \leqslant c\frac{\log p}{\log\log p}$, ибо в противном случае теорема доказана. Пусть Λ — максимальное диссоциативное подмножество S. В силу того, что $M \leqslant \log|S|$, имеем $\|f\|_2 \leqslant |S|^{1/2}M \leqslant |S|^{1/2}\log|S|$, и, значит, $\log\frac{\|f\|_2}{K} \ll \log|S|$. Тогда из леммы 2.6 получаем

$$d := \dim S = |\Lambda| \leqslant \frac{\log p}{\log\log p}\,. \tag{2.3}$$

Для элемента $x \in \mathbb{Z}_p$ через $|x|$ будем обозначать наименьший по абсолютной величине вычет По теореме Дирихле найдётся натуральное $q < p$ такое, что при всех $\lambda \in \Lambda$

$$|q\lambda| \leqslant p^{1-1/d} \leqslant \frac{p}{\log p}. \tag{2.4}$$

Возьмем произвольный элемент $x \in S$; по определению множества Λ имеем $x = \sum_{\lambda\in\Lambda}\varepsilon_\lambda\lambda$ для некоторых чисел $\varepsilon_\lambda \in \{-1,0,1\}$; в силу (2.3) и (2.4) видим, что при достаточно больших p

$$|qx| = |q\sum_{\lambda\in\Lambda}\varepsilon_\lambda\lambda| \leqslant \sum_{\lambda\in\Lambda}|q\lambda| \leqslant \frac{p}{\log\log p} \leqslant \frac{p}{3}.$$

Рассмотрим функцию $F(x) := f(qx)$; её носителем является множество $B := qS \subseteq [-p/3, p/3]$ и

$$\|\widehat{f}\|_1 = \|\widehat{F}\|_1 = \frac{1}{p}\sum_{\xi=1}^{p}\left|\sum_{x\in B}F(x)e_p(\xi x)\right|$$

Пусть $B = \{b_1 < \ldots b_n\}$. Рассмотрим тригонометрический полином $T(\xi) = \sum_{x\in B}F(x)e^{ix\xi} = \sum_{j=1}^{n}F(b_j)e^{ib_j\xi}$. В силу теоремы Марцинкевича, неравенства (0.2) и того, что $|F(b_j)| \geqslant 1$, имеем

$$\|\widehat{f}\|_1 = \|\widehat{F}\|_1 \gg \int_{\mathbb{T}}|F(y)|\,dy \gg \sum_{j=1}^{n}\frac{|F(b_j)|}{j} \gg \log|B| = \log|S|.$$

Тем самым теорема 2.1 доказана. $\square$

2.1.2 Доказательство теоремы 2.2

Докажем второе неравенство теоремы. Вначале сформулируем вспомогательные утверждения.

Лемма 2.7. *Пусть* $n \in \mathbb{N}$, $B \subset [-2n, 2n]$, $|B| \geqslant 2$, $0 < \eta < 1/2$, $|B \cap [-n, n]| \geqslant (1-\eta)|B|$, *и пусть* $c(b)$ $(b \in B)$ — *комплексные числа с условием* $|c(b)| \geqslant 1$ *при* $b \in B \cap [-n, n]$. *Тогда*

$$\int_0^1 \left| \sum_{b \in B} c(b) e(bu) \right| du \gg \min \left(\log \frac{1}{\eta}, \log |B| \right).$$

Лемма 2.7 доказана в работа [10] для случая, когда $c(b) = 1$ при $b \in B \cap [-n, n]$, но её доказательство проходит без изменений для сформулированного более общего случая.

Следуя работе [10], с помощью леммы 2.7 и многочленов Валле-Пуссена несложно доказать следующее утверждение.

Лемма 2.8. *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 для любой функции $F \colon \mathbb{Z}_p \to \mathbb{C}$ *такой, что* $|F(b)| \geqslant 1$ *при* $b \in B = \operatorname{supp} F$, *имеем*

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

Получим теперь аналог «структурной» леммы из [10]. Положим

$$S_j = \{x \in S : 2^{j-1} \leqslant |f(x)| < 2^j\}, \quad j = 1, 2, \ldots, [\log_2 M] + 1.$$

Лемма 2.5 при $k = 2$, $K = \|\widehat{f}\|_1$, $Q = S_j$ и $g_j(x) = S_j(x) f(x)$ даёт нам

$$\frac{|S_j|^4 2^{8(j-1)}}{\|f\|_2^2 \|\widehat{f}\|_1^2} \leqslant T_2(g) \leqslant 2^{4j} T_2(S_j),$$

откуда

$$T_2(S_j) \gg \frac{|S_j|^4 2^{4j}}{\|f\|_2^2 \|\widehat{f}\|_1^2}.$$

В силу того, что $T_2(S) = T_2(\sqcup_j S_j) \geqslant \sum_j T_2(S_j)$, имеем

$$T_2(S) \gg \frac{\sum_j |S_j|^4 2^{4j}}{\|f\|_2^2 \|\widehat{f}\|_1^2}. \tag{2.5}$$

Применяя неравенство Гёльдера, получаем

$$|S| = \sum_j |S_j| 2^j 2^{-j} \leqslant \left(\sum_j |S_j|^4 2^{4j} \right)^{1/4} \left(\sum_j 2^{-4j/3} \right)^{3/4} \ll \left(\sum_j |S_j|^4 2^{4j} \right)^{1/4}$$

и (так как $j \leqslant [\log_2 M] + 1$)

$$\|f\|_2^2 = \sum_{x\in S} |f(x)|^2 \asymp \sum_j |S_j| 2^j 2^j \ll$$
$$\left(\sum_j |S_j|^4 2^{4j}\right)^{1/4} \left(\sum_j 2^{4j/3}\right)^{3/4} \ll M \left(\sum_j |S_j|^4 2^{4j}\right)^{1/4}.$$

Из последних двух неравенств вытекает, что

$$\sum_j |S_j|^4 2^{4j} \gg |S|^3 \|f\|_2^2 M^{-1}.$$

Подставляя эту оценку в (2.5), находим

$$T_2(S) \gg \frac{|S|^3}{M\|\widehat{f}\|_1^2} \tag{2.6}$$

Повторяя аддитивно-комбинаторные рассуждения из работы [10], связанные с теоремами Балога-Семереди-Гауэрса и Фреймана, получим (по сути, меняя лишь величину $\|\widehat{\chi_A}\|_1$ на величину $O(M^{1/2}\|\widehat{f}\|_1)$) следующее утверждение.

Лемма 2.9. *Пусть $\varepsilon > 0$, $R > R(\varepsilon)$, $d_\varepsilon = \log^{3+\varepsilon} R$; пусть, далее, $f\colon \mathbb{Z}_p \to \mathbb{C}$ такова, что $1 \leqslant |f(x)|$ при $x \in S = supp f$, и $M = \max_{x\in\mathbb{Z}_p} |f(x)|$, $m = \left[d_\varepsilon p \left(\frac{|S|}{p}\right)^{1/d_\varepsilon}\right]$. Тогда если $M^{1/2}\|\widehat{f}\|_1 \leqslant R$, то найдутся $x_0 \in \mathbb{Z}_p$ и $q \in \mathbb{Z}_p^*$ такие, что для множества*

$$B = q(S - x_0)$$

выполнено

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

Наконец, сформулируем лемму из [10] об оценке величины $T_k(Q)$ для «разбросанных» множеств Q.

Лемма 2.10. *Пусть I, k, m, N — натуральные числа, и пусть $Q = \sqcup_{i=1}^I Q_i \subseteq \mathbb{Z}$, где $Q_i \subseteq [-4^i m, -\frac{4^i}{2} m) \cup (\frac{4^i}{2} m, 4^i m]$, $|Q_i| = N$, а i пробегает подмножество $\mathbb{Z}$ мощности I. Тогда*

$$T_k(Q) \leqslant 2^{8k} k^k I^k N^{2k-1}.$$

Теперь мы готовы доказать теорему 2.2. Можно считать, что $M \leqslant \log^{1/3}(p/|S|)$. Зафиксируем произвольное $\varepsilon > 0$ и предположим, что

$$M^{1/2}\|\widehat{f}\|_1 \leqslant R, \quad R(\varepsilon) \leqslant R \leqslant M^{1/2}(\log(p/|S|))^{1/3}(\log\log(p/|S|))^{-1-\varepsilon}. \tag{2.7}$$

Наша цель — доказать, что неравенства (2.7) не могут выполняться, если $p/|S|$ больше некоторой величины, зависящей от ε. Так как ε взято произвольным, то теорема 2.2 будет доказана.

Прежде всего, заметим, что так как всегда $\|\widehat{f}\|_1 \geqslant M$, то из (2.7) вытекает, что

$$M \leqslant R^{2/3}; \tag{2.8}$$

в частности, $RM^{-1/2} \geqslant R^{2/3}$.

Возьмем x_0, q, m и B в соответствии с леммой 2.9, и положим $F(x) = f(q(x - x_0))$. Тогда $\|\widehat{F}\|_1 = \|\widehat{f}\|_1$ и потому

$$M^{1/2}\|\widehat{F}\|_1 \leqslant R. \tag{2.9}$$

Пусть l_0 — максимальное целое такое, что $2^l m \leqslant p/3$, и

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

$$\eta = \exp(-CRM^{-1/2}),$$

где $C > 0$ — достаточно большая абсолютная постоянная (заметим, что $\eta \in (0, 1/2)$), и

$$N = [\eta|S|e^{-d_\varepsilon}].$$

В силу нижней оценки на $|S|$ и верхних оценок на M и R имеем $N \geqslant 1$ при достаточно большом p. Рассмотрим два случая.

I случай. Пусть $|D_l \setminus D_{l-1}| < N$ для некоторого l. В силу леммы 2.9 $|D_l| \geqslant |D_0| \geqslant |S|e^{-d_\varepsilon}$, и поэтому $|D_{l-1}| \geqslant |D_l| - N \geqslant |D_l|(1 - N|D_l|^{-1}) \geqslant (1 - \eta)|D_l|$. Применяя лемму 2.8 для множества B и $n = 2^{l-1}m$, найдём

$$\|\widehat{F}\|_1 \gg \min\left(\log\frac{1}{\eta}, \log|D_0|\right).$$

Учитывая, что $|S| \geqslant \exp((\log / \log\log p)^{1/3})$, (2.7) и то, что $p/|S|$ достаточно велико, имеем

$$\log|D_0| \geqslant \log|S| - d_\varepsilon \gg \log|S| \geqslant (\log p/\log\log p)^{1/3} \geqslant \log\frac{1}{\eta} = CRM^{-1/2},$$

откуда

$$\|\widehat{f}\|_1 = \|\widehat{F}\|_1 \gg CRM^{-1/2},$$

и мы получаем противоречие с (2.7) при достаточно большом C.

II случай. Пусть $|D_l \setminus D_{l-1}| \geqslant N$ при всех $l = 1, \ldots, l_0$. Тогда для каждого $l \equiv 0 \pmod 2$ мы можем выбрать множество $S_l \subseteq D_l \setminus D_{l-1}$ такое, что $|S_l| = N$. Положим

$$Q = \bigsqcup_l S_l;$$

к множеству Q можно применить лемму 2.10, где множества Q_i суть множества S_l и $I = [l_0/2]$. Имеем

$$T_k(Q) \leqslant (2^8 k)^k I^k N^{2k-1}. \tag{2.10}$$

Получим теперь нижнюю оценку на $T_k(Q)$. Пусть

$$Q_j = \{x \in Q : 2^{j-1} < |F(x)| \leqslant 2^j\}.$$

Применяя лемму 2.5 к множеству $Q_j \subseteq B$, числу $K = RM^{-1/2}$ и функциям $F(x)$ и $g_j(x) = Q_j(x)F(x)$, получаем

$$\frac{|Q_j|^{2k} 2^{4(j-1)k}}{\|F\|_2^2 K^{2k-2}} \leqslant T_k(g_j) \leqslant T_k(|g_j|) \leqslant 2^{2jk} T_k(Q_j),$$

откуда

$$T_k(Q_j) \geqslant \frac{|Q_j|^{2k} 2^{2jk-4k}}{\|F\|_2^2 K^{2k-2}}.$$

Суммируя по j, находим

$$T_k(Q) \geqslant \sum_j T_k(Q_j) \geqslant \frac{1}{2^{4k}\|F\|_2^2 K^{2k-2}} \sum_j |Q_j|^{2k} 2^{2jk};$$

далее, так как

$$|Q|^{2k} = \left(\sum_j |Q_j| 2^j 2^{-j}\right)^{2k} \leqslant \left(\sum_j |Q_j|^{2k} 2^{2jk}\right) \left(\sum_j 2^{-2jk/(2k-1)}\right)^{(2k-1)} \leqslant \sum_j |Q_j|^{2k} 2^{2jk},$$

то, в силу того, что $|Q| = IN$, имеем

$$T_k(Q) \geqslant \frac{|Q|^{2k}}{2^{4k}\|F\|_2^2 K^{2k-2}} = \frac{(IN)^{2k}}{2^{4k}\|F\|_2^2 K^{2k-2}}. \tag{2.11}$$

Сравним оценки (2.10) и (2.11). Получим

$$I \ll K^2 k \left(\frac{\|F\|_2^2}{NK^2}\right)^{1/k} \leqslant K^2 k \left(\frac{|S|M^2}{NK^2}\right)^{1/k}.$$

Вспоминая, что $K = RM^{-1/2}$, и пользуясь неравенством (2.8), найдём

$$I \ll R^2 M^{-1} k \left(\frac{|S|M^3}{NR^2}\right)^{1/k} \leqslant R^2 M^{-1} k \left(\frac{|S|}{N}\right)^{1/k} = R^2 M^{-1} \exp\left(\log k + \frac{1}{k} \log \frac{|S|}{N}\right). \tag{2.12}$$

Положим $k = [\log \frac{|S|}{N}] \geqslant 1$; тогда

$$I \ll R^2 M^{-1} \log \frac{|S|}{N}.$$

Наконец, так как $|S|N^{-1} \ll \eta^{-1} e^{d_\varepsilon} \leqslant \exp(CRM^{-1/2} + \log^{3+\varepsilon} R)$ и $RM^{-1/2} \geqslant R^{2/3}$, то $\log \frac{|S|}{N} \ll RM^{-1/2}$ и

$$I \ll R^3 M^{-3/2}. \tag{2.13}$$

Но

$$I \geqslant l_0/2 - 1 \gg \log(p/m) \gg d_\varepsilon^{-1} \log(p/|S|) - \log d_\varepsilon.$$

Вспоминая, что $d_\varepsilon = \log^{3+\varepsilon} R$, и учитывая верхнюю границу на R (предположение (2.7)), получаем

$$I \gg d_\varepsilon^{-1} \log(p/|S|) \gg \log(p/|S|)(\log\log(p/|S|))^{-3-\varepsilon}.$$

Отсюда и из (2.13) имеем

$$R^3 \gg M^{3/2} I \gg M^{3/2} \log(p/|S|)(\log\log(p/|S|))^{-3-\varepsilon}$$

что противоречит (2.7), если $p/|S|$ достаточно велико. Тем самым теорема 2.2 доказана. $\square$

2.2 Доказательство теоремы 2.3

Пусть $d \geqslant 1$. Для $x = (x_1, \dots, x_d), \xi = (\xi_1, \dots, \xi_d) \in \mathbb{Z}_p^d$ и $c \in \mathbb{Z}_p$ положим

$$x\xi := (x, \xi) = x_1\xi_1 + \dots + x_d\xi_d \in \mathbb{Z}_p$$

и

$$c\xi = (c\xi_1, \dots, c\xi_d) \in \mathbb{Z}_p^d.$$

Так как характеры группы $\mathbb{Z}_p^d$ суть функции

$$\gamma_\xi(x) = e_p(\xi x),$$

где $e_p(u) = \exp(2\pi i u/p)$ и $\xi \in \mathbb{Z}_p^d$, то преобразование Фурье функции $f\colon \mathbb{Z}_p^d \to \mathbb{C}$ может быть переписано в виде

$$\widehat{f}(\xi) := p^{-d} \sum_{x \in \mathbb{Z}_p^d} f(x) e_p(-\xi x),$$

а её винеровская норма — в виде

$$\|\widehat{f}\|_1 = \sum_{\xi \in \mathbb{Z}_p^d} |\widehat{f}(\xi)|.$$

Везде ниже в тексте через θ, θ', θ'' обозначены вещественные числа, по модулю не превосходящие единицы (в разных формулах, вообще говоря, разные).

Нам понадобятся следующие леммы.

Лемма 2.11. *Пусть $A \subset \mathbb{Z}_p^d$, $|A| = \delta p^d$. Тогда существует гиперплоскость $L \subset \mathbb{Z}_p^d$ такая, что*

$$|A \cap L| = p^{d-1}(\delta + \theta \delta^{1/2} p^{-(d-1)/2}),$$

где $|\theta| \leqslant 1$.

Доказательство. Будем использовать вероятностный метод. Рассмотрим всевозможные попарно не параллельные «направления» $\eta_1, \dots, \eta_r \in \mathbb{Z}_p^d$, то есть максимальный набор векторов из $\mathbb{Z}_p^d$, любые два из которых линейно независимы. Любой ненулевой вектор $\xi \in \mathbb{Z}_p^d$ параллелен ровно одному вектору η_j (то есть $\xi = \alpha \eta_j$ для некоторого $\alpha \in \mathbb{Z}_p$). Таким образом, каждому направлению соответствует ровно $p-1$ ненулевой вектор, и поэтому $r = \frac{p^d-1}{p-1} = 1 + p + \ldots + p^{d-1}$.

Любая гиперплоскость имеет вид

$$L = L_{\eta,u} = \{x \in \mathbb{Z}_p^d : x\eta = u\},$$

где $\eta \in \Lambda := \{\eta_1, \dots, \eta_r\}$ и $u \in \mathbb{Z}_p^d$. Будем случайно и равномерно выбирать упорядоченную пару $(\eta, u) \in \Lambda \times \mathbb{Z}_p$ (то есть гиперплоскость) и рассмотрим случайную величину

$$\xi = |A \cap L_{\eta,u}| = \sum_{x \in A} 1(x\eta = u).$$

Прежде всего,

$$\mathbb{E}\xi = \frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \Lambda} \sum_{u \in \mathbb{Z}_p} 1(x\eta = u) = \frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \Lambda} 1 = \frac{|A|}{p}.$$

Далее,

$$\mathbb{E}\xi^2 = \frac{1}{rp} \sum_{x_1, x_2 \in A} \sum_{\eta \in \Lambda} \sum_{u \in \mathbb{Z}_p} 1(x_1\eta = x_2\eta = u) =$$

$$\mathbb{E}\xi + \frac{1}{rp} \sum_{x_1, x_2 \in A, x_1 \neq x_2} \sum_{\eta \in \Lambda} \sum_{u \in \mathbb{Z}_p} 1(x_1\eta = x_2\eta = u).$$

Зафиксируем $x_1, x_2 \in A$, $x_1 \neq x_2$. Будем говорить, что векторы $a, b \in \mathbb{Z}_p^d$ ортогональны (и писать $a \perp b$), если $(a, b) = 0$. Заметим, что если $(x_1 - x_2, \eta) = 0$, то $\sum_{u \in \mathbb{Z}_p} 1(x_1\eta = x_2\eta = u) = 1$, а иначе $\sum_{u \in \mathbb{Z}_p} 1(x_1\eta = x_2\eta = u) = 0$. Далее, имеется ровно $p^{d-1} - 1$ ненулевых векторов $y \in \mathbb{Z}_p^d$, таких, что $(x_1 - x_2, y) = 0$. Так как векторы, параллельные конкретному η_j, одновременно ортогональны или неортогональны разности $x_1 - x_2$, то количество векторов $\eta_j \in \Lambda$, ортогональных $x_1 - x_2$, равно $\frac{p^{d-1}-1}{p-1}$. Вспоминая, что $r = \frac{p^d-1}{p-1}$,

получаем

$$\mathbb{E}\xi^2 = \mathbb{E}\xi + \frac{1}{rp}\sum_{x_1,x_2\in A, x_1\neq x_2}\sum_{\eta\in\Lambda,\eta\perp x_1-x_2} 1 = \mathbb{E}\xi + \frac{p^{d-1}-1}{rp(p-1)}|A|(|A|-1) =$$

$$\mathbb{E}\xi + \frac{1}{p^2}\frac{p^{d-1}-1}{p^{d-1}-1/p}|A|(|A|-1) < \mathbb{E}\xi + \frac{1}{p^2}|A|^2 = \mathbb{E}\xi + (\mathbb{E}\xi)^2.$$

Поэтому

$$Var\,\xi = \mathbb{E}\xi^2 - (\mathbb{E}\xi)^2 < \mathbb{E}\xi = \delta p^{d-1}.$$

и

$$\sigma := (Var\,\xi)^{1/2} = \frac{\delta^{1/2}p^{(d-1)/2}}{\lambda}$$

для некоторого $\lambda > 1$. Значит, по неравенству Чебышёва

$$\mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \delta^{1/2}p^{(d-1)/2}) = \mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \lambda\sigma) \leqslant \frac{1}{\lambda^2} < 1,$$

и, стало быть, найдётся гиперплоскость $L_{\eta,u}$ такая, что

$$|A\cap L_{\eta,u}| = \delta p^{d-1} + \theta\delta^{1/2}p^{(d-1)/2}$$

при некотором $\theta < 1$. Лемма доказана. $\square$

Многократное применение леммы 2.11 даёт нам прямую, на которой плотность множества A близка к δ.

Лемма 2.12. *Пусть $A \subset \mathbb{Z}_p^d$, $|A| = \delta p^d$ и $\delta \gg p^{-1}$. Тогда существует прямая $l \subset \mathbb{Z}_p^d$ такая, что*

$$|A\cap l| = p\left(\delta + \theta\delta^{1/2}p^{-1/2} + O(\delta^{1/2}p^{-1} + p^{-3/2})\right),$$

где $|\theta| \leqslant 1$.

Доказательство. Прежде всего, заметим, что если $T\colon \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ — невырожденное аффинное преобразование, а l — прямая в $\mathbb{Z}_p^d$, то $T^{-1}l$ — снова прямая и $|TA\cap l| = |A\cap T^{-1}l|$. Поэтому достаточно доказать лемму для произвольного образа множества A при невырожденном аффинном преобразовании.

Утверждение леммы при $d = 2$ непосредственно вытекает из леммы 2.11. Пусть $d \geqslant 3$. Покажем, что в этом случае можно считать, что

$$\delta_{d-3} := p^{-3}|A\cap\mathbb{Z}_p^3| = \delta + \theta\sum_{k=3}^{d-1}p^{-k/2}. \tag{2.14}$$

Действительно, при $d = 3$ мы имеем $p^{-3}|A\cap\mathbb{Z}_p^3| = p^{-3}|A| = \delta$. При $d \geqslant 4$, применяя лемму 1 к множеству A, найдём гиперплоскость $L_1 \subset \mathbb{Z}_p^d$ такую, что

$$p^{-(d-1)}|A\cap L_1| = \delta_1,$$

где $\delta_1 = \delta + \theta\delta^{1/2}p^{-(d-1)/2} = \delta + \theta' p^{-(d-1)/2}$. В силу сделанного выше замечания можно, не ограничивая общности, считать, что $L_1 = \mathbb{Z}_p^{d-1}$ (мы отождествляем подпространства $\{x \in \mathbb{Z}_p^d : x_{d-k+1} = \ldots = x_{d-1} = x_d = 0\}$, $k = 1, \ldots, d-1$, с $\mathbb{Z}_p^{d-k}$). Применяя лемму 2.11 к множеству $A \cap L_1 \subset \mathbb{Z}_p^{d-1}$, найдём гиперплоскость $L_2 \subset \mathbb{Z}_p^{d-1}$ со свойством

$$|A \cap L_2| = \delta_1 + \theta\delta_1^{1/2}p^{-(d-2)/2} = \delta_1 + \theta' p^{-(d-2)/2} = \delta + \theta'' \sum_{k=d-2}^{d-1} p^{-k/2}.$$

Вновь, не ограничивая общности, можно считать, что $L_2 = \mathbb{Z}_p^{d-2}$, и применить лемму к множеству $A \cap L_2 \subset \mathbb{Z}_p^{d-2}$. Рассуждая далее аналогично, мы придём к случаю, когда выполнено (2.14).

Итак, можно считать, что $|A \cap \mathbb{Z}_p^3| = \delta_{d-3}p^3$, где $\delta_{d-3} = \delta + \theta\sum_{k=3}^{d-1} p^{-k/2} = \delta + O(p^{-3/2})$. В этом случае будем иметь $\delta_{d-3}^{1/2} = \delta^{1/2} + O(\delta^{-1/2}p^{-3/2})$. Применяя к множеству $A \cap \mathbb{Z}_p^3$ лемму 2.11 и учитывая, что $\delta \gg p^{-1}$, найдем плоскость $L \subset \mathbb{Z}_p^3$ такую, что

$$\delta_{d-2} := p^{-2}|A \cap L| = \delta_{d-3} + \theta\delta_{d-3}^{1/2}p^{-1} = \\ \delta + O(p^{-3/2} + \delta^{1/2}p^{-1} + \delta^{-1/2}p^{-5/2}) = \delta + O(\delta^{1/2}p^{-1});$$

при этом

$$\delta_{d-2}^{1/2} = \delta^{1/2} + O(p^{-1}).$$

Как и ранее, можно считать, что $L = \mathbb{Z}_p^2$. Наконец, применяя лемму 2.11 к множеству $A \cap L \subset \mathbb{Z}_p^2$, найдём прямую $l \subset \mathbb{Z}_p^2$ со свойством

$$p^{-1}|A \cap l| = \delta_{d-2} + \theta\delta_{d-2}^{1/2}p^{-1/2} = \delta + \theta\delta^{1/2}p^{-1/2} + O(\delta^{1/2}p^{-1} + p^{-3/2}),$$

что и требовалось. $\square$

Пусть теперь

$$l = \{y \in \mathbb{Z}_p^d : y = ub + c \,|\, u \in \mathbb{Z}_p\} \tag{2.15}$$

где $c = (c_1, \ldots, c_d)$, $b = (b_1, \ldots, b_d) \in \mathbb{Z}_p^d$, $b \neq 0$, — прямая в $\mathbb{Z}_p^d$. Для произвольной функции $f\colon \mathbb{Z}_p^d \to \mathbb{C}$ определим её сужение на прямую l как функцию $f_l\colon \mathbb{Z}_p \to \mathbb{C}$,

$$f_l(u) = f(b_1u + c_1, \ldots, b_du + c_d).$$

Легко видеть, что абсолютные значения коэффициентов Фурье (а следовательно, и винеровская норма) функции f_l не зависят от параметризации прямой.

Покажем теперь, что винеровская норма функции f в $\mathbb{Z}_p^d$ не меньше, чем винеровская норма её сужения на любую прямую.

Лемма 2.13. *Пусть* $f\colon \mathbb{Z}_p^d \to \mathbb{C}$ *и* $l \subset \mathbb{Z}_p^d$ *— прямая. Тогда*

$$\|\widehat{f}\|_1 \geqslant \|\widehat{f}_l\|_1.$$

Доказательство. Пусть прямая l определена как в (2.15) и пусть $l(x)$ — её характеристическая функция. Так как прямая l является сдвигом одномерного подпространства, то $\|\widehat{l}\|_1 = 1$; тогда в силу неравенства (0.3) имеем

$$\|\widehat{f}\|_1 = \|\widehat{f}\|_1\|\widehat{l}\|_1 \geqslant \|\widehat{f}\widehat{l}\|_1 = \sum_{\xi\in\mathbb{Z}_p^d}\left|p^{-d}\sum_{x\in l} f(x)e_p(-\xi x)\right| = \sum_{\xi\in\mathbb{Z}_p^d}\left|p^{-d}\sum_{u\in\mathbb{Z}_p} f(ub+c)e_p(-\xi(ub+c))\right| =$$

$$p^{-(d-1)}\sum_{\xi\in\mathbb{Z}_p^d}\left|p^{-1}\sum_{u\in\mathbb{Z}_p} f_l(u)e_p(-u\xi b)\right|.$$

Так как $b \neq 0$, то для каждого $\eta \in \mathbb{Z}_p$ существует ровно p^{d-1} векторов $\xi \in \mathbb{Z}_p^d$ со свойством $\xi b = \eta$. Поэтому последняя сумма равна

$$\sum_{\eta\in\mathbb{Z}_p}\left|p^{-1}\sum_{u\in\mathbb{Z}_p} f_l(u)e_p(-u\eta)\right| = \|\widehat{f}_l\|_1.$$

Лемма доказана. □

Утверждение теоремы 2.3 теперь вытекает из лемм 2.12 и 2.13 и предположения на оценки в одномерном случае.

2.3 Доказательство теоремы 2.4

Пусть $\{e_1, \dots, e_d\}$ — стандартный базис $\mathbb{Z}_p^d$ над $\mathbb{Z}_p$ (везде ниже мы рассматриваем только его). Пусть $A = supp\, f$. Покажем, что существует невырожденное линейное преобразование преобразование $T\colon \mathbb{Z}_p^d \to \mathbb{Z}_p^d$, $T = \{t_{ij}\}_{i,j=1}^d$, такое, что первые координаты элементов множества TA различны. Пусть $A = \{a_1, \dots, a_n\}$ и $a_j = \sum_{i=1}^d \alpha_{ij}e_i$; тогда

$$Ta_j = \sum_{i=1}^d \beta_{ij}e_i,$$

где

$$\beta_{ij} = \sum_{k=1}^d t_{ik}\alpha_{kj}.$$

Мы хотим, чтобы величины $\beta_{1,j} = \sum_{k=1}^d t_{1,k}\alpha_{k,j}$, $j = 1, \dots, n$, были различны; это равносильно тому, что при всех $i < j$

$$\sum_{k=1}^d t_{1,k}(\alpha_{k,i} - \alpha_{k,j}) \neq 0. \tag{2.16}$$

Таким образом, нам нужно лишь найти вектор $\mathbf{t} = (t_{1,1}, \ldots, t_{1,d})$ (который будет первой строкой матрицы T) со свойством (2.16). Пар элементов $(a_i, a_j) \in A^2$, $i < j$, имеется ровно $|A|(|A|-1)/2$; так как $|A| < (2p)^{1/2}$, то таких пар менее, чем p штук. Для каждой из них существует ровно p^{d-1} векторов $\mathbf{t}$, при которых нарушается (2.16); так как всего векторов $\mathbf{t}$ имеется p^d, то найдётся $\mathbf{t}$ со свойством (2.16).

Итак, существует невырожденное линейное преобразование T такое, что первые координаты элементов множества TA различны. Пусть

$$A' = \{x \in \mathbb{Z}_p : x = \beta_{1,j} \text{ для некоторого } j\}$$

— «проекция» множества TA на прямую $x_2 = \ldots = x_d = 0$. Тогда любой элемент $a \in TA$ представляется в виде

$$a = a_x = xe_1 + y_2(x)e_2 + \ldots + y_d(x)e_d, \quad x \in A'. \tag{2.17}$$

Рассмотрим теперь функцию

$$h(x) := f(T^{-1}x).$$

Тогда

$$\widehat{h}(\xi) = p^{-d} \sum_x f(T^{-1}x) e_p(-\xi x) = p^{-d} \sum_x f(x) e_p(-\xi T x) = \widehat{h}(T^*\xi),$$

где T^* — сопряженный к T оператор, и потому $\|\widehat{h}\|_1 = \|\widehat{f}\|_1$. Кроме того, так как носителем h является множество TA, то в силу (2.17)

$$\|\widehat{h}\|_1 = p^{-d} \sum_{\xi_1,\ldots,\xi_d} \left| \sum_{x \in A'} h(a_x) e_p(-(y_2(x)\xi_2 + \ldots + y_d(x)\xi_d)) e_p(-x\xi_1) \right| \geqslant$$

$$p^{-(d-1)} \sum_{\xi_2,\ldots,\xi_d} p^{-1} \sum_{\xi_1} \left| \sum_{x \in A'} h(a_x) e_p(-(y_2(x)\xi_2 + \ldots + y_d(x)\xi_d)) e_p(-x\xi_1) \right|.$$

При фиксированных $\xi_2, \ldots, \xi_d$ к внутренней сумме, являющейся винеровской нормой одномерной функции со значениями, принадлежащими множеству E, можно применить предположение теоремы; так как $|A'| = |A|$, то каждая внутренняя сумма оценивается снизу величиной $F(p, |A|p^{-1})$. Отсюда следует утверждение теоремы 2.4. $\square$

Глава 3

Пропущенные цифры в конечных полях

В этой главе будут доказаны утверждения о размере множеств с пропущенными цифрами. Первые два из них относятся к случаю, когда множество допустимых цифр $\mathcal{D}$ общее для всех координат, то есть, когда

$$W_{\mathcal{D}} = \{x_1a_1 + \ldots + x_ra_r \,|\, x_i \in \mathcal{D}\}\,.$$

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*

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

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

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 $|W_{\mathcal{D}} \cap Q| = \left(\frac{1}{2} + O((\log p)^{-C})\right)|W_{\mathcal{D}}|$.

Следующая теорема и её следствия относятся к случаю, когда по каждой координате имеется своё множество допустимых цифр, то есть, когда

$$W = W(D_1, \dots, D_r) = \{x_1 a_1 + \dots + x_r a_r \,|\, x_i \in D_i\}.$$

Теорема 3.4. *Справедлива оценка*

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

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.

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

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 даёт достаточные условия существования квадратов во множестве W.

В разделе 3.1 мы приводим необходимые вспомогательные результаты. В разделах 3.2 и 3.3 приводятся доказательства теорем 3.1 и 3.2 соответственно. Теореме 3.3 посвящен раздел 3.4.1. Мы выводим её из теоремы C, однако, в работе [8] множитель $\frac{r^{O(1)}}{\varepsilon}$ не был выписан явно, поэтому далее мы доказываем теорему C в сформулированном виде. Теорема 3.4 доказывается в разделе 3.5, следствия 3.5 и 3.6 — в разделе 3.6.

3.1 Вспомогательные результаты

Нам потребуются оценки сумм характеров специального вида. Отметим, что лемма M была получена в работе [55] и сформулирована в удобном для нас виде в [56].

Лемма M ([55], следствие 2.4; [56], лемма 2.2). *Пусть χ – мультипликативный характер порядка s в $\mathbb{F}_q$ и $\alpha, \beta \in \mathbb{F}_q$ – несопряжённые порождающие элементы $\mathbb{F}_q$ над $\mathbb{F}_p$. Тогда*

$$\left|\sum_{\xi \in \mathbb{F}_p} \chi\left((\xi+\alpha)(\xi+\beta)^{s-1}\right)\right| \leqslant (2r-1)p^{1/2}.$$

Лемма N ([39], лемма 1). *Пусть t – целое число, $1 \leqslant t < q$, $\chi_1, \dots, \chi_t$ – мультипликативные характеры в $\mathbb{F}_q$, причём для некоторого i $\chi_i \neq \chi_0$,*

где χ_0 – главный характер. Пусть, далее, $h_1, \dots, h_t$ – различные элементы $\mathbb{F}_q$ и

$$S = \sum_{a \in F_q} \chi_1(a+h_1)\chi_2(a+h_2)\cdots\chi_t(a+h_t).$$

Тогда

$$|S| < tq^{1/2}.$$

Хорошо известны оценки сумм характеров по суммам множеств (см., например, [18], лемма 2). Нам будет удобно использовать оценку следующего вида.

Лемма 3.7. *Для любых $\nu \in \mathbb{N}$, $U, V \subset \mathbb{F}_q$ и квадратичного характера χ на $\mathbb{F}_q$ справедливо*

$$\left|\sum_{u\in U}\sum_{v\in V}\chi(u+v)\right| < |U|^{1-1/2\nu}\left((2\nu)!|V|^{\nu}q + |V|^{2\nu}2\nu q^{1/2}\right)^{1/2\nu}.$$

Доказательство. Имеем

$$\left|\sum_{u\in U}\sum_{v\in V}\chi(u+v)\right| \leqslant \sum_{u\in U}\left|\sum_{v\in V}\chi(u+v)\right| \leqslant |U|^{1-1/2\nu}S^{1/2\nu},$$

где

$$S = \sum_{u\in U}\left|\sum_{v\in V}\chi(u+v)\right|^{2\nu} \leqslant \sum_{(v_1,\dots,v_{2\nu})\in V^{2\nu}}\left|\sum_{a\in\mathbb{F}_q}\chi(a+v_1)\cdots\chi(a+v_{2\nu})\right|.$$

Последнюю сумму разобьем на две: на сумму S_1 по тем наборам $(v_1, \dots, v_{2\nu})$, в которых значение каждой компоненты встречается чётное число раз, и на сумму S_2 по всем остальным наборам. Ясно, что $S_1 \leqslant (2\nu)!|V|^{\nu}q$. Для оценки внутренней суммы для наборов из суммы S_2 воспользуемся леммой N; каждая полученная оценка будет меньше, чем $2\nu q^{1/2}$. Поэтому

$$S \leqslant S_1 + S_2 < (2\nu)!|V|^{\nu}q + |V|^{2\nu}2\nu q^{1/2}.$$

Лемма доказана. □

3.2 Доказательство теоремы 3.1

Через χ обозначим квадратичный характер на $\mathbb{F}_q$; считаем, что $\chi(0) = 0$. Пусть 0 не принадлежит $\mathcal{D}$. Тогда

$$|W_{\mathcal{D}} \cap Q| = \frac{1}{2}\sum_{x\in W_{\mathcal{D}}}(1+\chi(x)) = \frac{1}{2}|W_{\mathcal{D}}| + \frac{1}{2}\sum_{x\in W_{\mathcal{D}}}\chi(x).$$

Если же $0 \in \mathcal{D}$, то

$$|W_{\mathcal{D}} \cap Q| = \frac{1}{2} \sum_{x \in W_{\mathcal{D}} \setminus \{0\}} (1 + \chi(x)) = \frac{1}{2}(|W_{\mathcal{D}}| - 1) + \frac{1}{2} \sum_{x \in W_{\mathcal{D}}} \chi(x).$$

Таким образом, всегда справедлива оценка

$$\left| |W_{\mathcal{D}} \cap Q| - \frac{|W_{\mathcal{D}}|}{2} \right| \leqslant \frac{1}{2} \left| \sum_{x \in W_{\mathcal{D}}} \chi(x) \right| + \frac{1}{2}, \tag{3.1}$$

и нужно для доказательства теоремы нужно оценить сумму характеров. Положим $b_j = a_j/a_1$. Тогда $b_1 = 1$ и $\{1, b_2, \ldots, b_r\}$ — базис. Имеем

$$\left| \sum_{x \in W_{\mathcal{D}}} \chi(x) \right| \leqslant \sum_{c_1 \in \mathcal{D}} \left| \sum_{c_2, \ldots, c_r \in \mathcal{D}} \chi(c_1 a_1 + \ldots + c_r a_r) \right| \leqslant |\mathcal{D}|^{1/2} A^{1/2}, \tag{3.2}$$

где

$$A = \sum_{c_1 \in \mathcal{D}} \left| \sum_{c_2, \ldots, c_r \in \mathcal{D}} \chi(c_1 a_1 + \ldots + c_r a_r) \right|^2 = \sum_{c_1 \in \mathcal{D}} \left| \sum_{(c_2, \ldots, c_r) \in \mathcal{D}^{r-1}} \chi(c_1 + c_2 b_2 \ldots + c_r b_r) \right|^2.$$

Пусть $\mathcal{D}_d$ — множество тех наборов $(c_2, \ldots, c_r) \in \mathcal{D}^{r-1}$, для которых элемент $c_2 b_2 + \ldots + c_r b_r$ лежит в подполе порядка p^d и не лежит ни в каком подполе меньшего порядка. Ясно, что $\mathcal{D}^{r-1} = \bigsqcup_{d|r} \mathcal{D}_d$, причем $\mathcal{D}_1 = \{0\}$, если $0 \in \mathcal{D}$, и $\mathcal{D}_1 = \emptyset$ иначе. Для $d|r$ определим функцию $f_d(x) \colon \mathcal{D} \to \mathbb{C}$, $f_d(c) = \sum_{(c_2, \ldots, c_r) \in \mathcal{D}_d} \chi(c + c_2 b_2 + \ldots + c_r b_r)$. Напомним, что l_2-норма функции $g \colon \mathcal{D} \to \mathbb{C}$ определяется как $\|g\|_2 = \left(\sum_{x \in \mathcal{D}} |g(x)|^2 \right)^{1/2}$. Тогда в силу неравенства треугольника

$$A^{1/2} = \left\| \sum_{d|r} f_d \right\|_2 \leqslant \sum_{d|r} \|f_d\|_2 = \sum_{d|r} A_d^{1/2}. \tag{3.3}$$

где

$$A_d = \sum_{x \in \mathcal{D}} \left| \sum_{(c_2, \ldots, c_r) \in \mathcal{D}_d} \chi(x + c_2 b_2 + \ldots + c_r b_r) \right|^2.$$

По определению множества $\mathcal{D}_d$ при любом $(c_2, \ldots, c_r) \in \mathcal{D}_d$ элемент $c_2 b_2 + \ldots + c_r b_r$ порождает подполе порядка p^d. Учитывая, что каждый такой

элемент имеет не более d сопряженных, и применяя лемму М к парам несопряженных элементов, при $d > 1$ имеем

$$A_d \leqslant \sum_{(c_2,\ldots,c_r),(c_2',\ldots,c_r')\in\mathcal{D}_d} \left| \sum_{x\in F_p} \chi(x + c_2b_2 + \ldots + c_rb_r)\overline{\chi}(x + c_2'b_2 + \ldots + c_r'b_r) \right| \leqslant$$
$$\sum_{(c_2,\ldots,c_r)\in\mathcal{D}_d} \Big(dp + (|\mathcal{D}_d| - d)(2d-1)p^{1/2} \Big) \leqslant (2d-1)p^{1/2}|\mathcal{D}_d|^2 + dp|\mathcal{D}_d|.$$

Кроме того, $A_1 \leqslant |\mathcal{D}| \leqslant p$. Обозначим $\mathcal{J} = \{d | r : d > 1 \text{ и } \mathcal{D}_d \neq \emptyset\}$. Тогда при $d \in \mathcal{J}$ в силу неравенства $\sqrt{A+B} \leqslant \sqrt{A}\,(1 + \frac{B}{2A})$, верного при всех положительных A, B, получаем

$$A_d^{1/2} \leqslant (2d-1)^{1/2}p^{1/4}|\mathcal{D}_d| + \frac{dp^{3/4}}{2(2d-1)^{1/2}}.$$

Из этой оценки и неравенства (3.3) имеем

$$A^{1/2} \leqslant p^{1/4}S_1 + \frac{1}{2}p^{3/4}S_2 + p^{1/2},$$

где

$$S_1 = \sum_{d\in\mathcal{J}} (2d-1)^{1/2}|\mathcal{D}_d|, \quad S_2 = \sum_{d\in\mathcal{J}} \frac{d}{(2d-1)^{1/2}}.$$

Учитывая, что $\sum\limits_{d|r} |\mathcal{D}_d| = |\mathcal{D}|^{r-1}$, получаем

$$S_1 \leqslant (2r-1)^{1/2}|\Delta|^{r-1}, \quad S_2 \leqslant \sum_{d\in\mathcal{J}} d^{1/2} \leqslant \frac{1}{2}r^{3/2}.$$

(Последняя оценка проверяется непосредственно при $2 \leqslant r \leqslant 7$, а при $r \geqslant 8$ вытекает из неравенств $r^{1/2} \leqslant \frac{1}{6}r^{3/2}$ и $\sum\limits_{d\leqslant r/2} d^{1/2} \leqslant \frac{2}{3}(r/2+1)^{3/2} \leqslant \frac{1}{3}r^{3/2}$.)
Значит,

$$A^{1/2} \leqslant p^{1/4}(2r-1)^{1/2}|\mathcal{D}|^{r-1} + \frac{1}{4}p^{3/4}r^{3/2} + p^{1/2}.$$

Подставляя последнее неравенство в (3.2), получим

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

Отсюда и из (3.1) вытекает первое утверждение теоремы. Далее, во множестве $W_{\mathcal{D}}$ есть квадраты, если правая часть последнего неравенства меньше, чем $|\mathcal{D}|^r - 1$. Это равносильно условию

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

Покажем теперь, что последнее неравенство выполнено при $|\mathcal{D}| \geqslant (1+\delta)(2r-1)p^{1/2}$, где $\delta = \left(\sqrt{p}(2r-1)\right)^{2-r}$. В силу того, что $\sqrt{1+\delta}-1 \geqslant \frac{\delta}{2\sqrt{2}}$ при $\delta \in (0,1]$, а также $2r-1 \geqslant \frac{3}{2}r$ при $r \geqslant 2$, имеем

$$|\mathcal{D}|^{r-1}\left(|\mathcal{D}|^{1/2}-(2r-1)^{1/2}p^{1/4}\right) \geqslant (1+\delta)^{r-1}(2r-1)^{r-1/2}(p^{1/2})^{r-1/2}\frac{\delta}{2\sqrt{2}} =$$
$$\frac{(1+\delta)^{r-1}}{2\sqrt{2}}(2r-1)^{3/2}p^{3/4} \geqslant \frac{3\sqrt{3}}{8}p^{3/4}r^{3/2} > \frac{1}{4}p^{3/4}r^{3/2}+p^{1/2}+|\mathcal{D}|^{-1/2}.$$

Теорема доказана. $\square$

3.3 Доказательство теоремы 3.2

Введём натуральные параметры k и ν, которые выберем позже. Положим

$$U = \left\{\sum_{j=1}^{r-k} c_j a_j : c_j \in \mathcal{D}\right\}, \quad V = \left\{\sum_{j=r-k+1}^{r} c_j a_j : c_j \in \mathcal{D}\right\},$$

где $1 \leqslant k \leqslant r-1$. Тогда $W_{\mathcal{D}} = U+V$ и по лемме 3.7

$$\left|\sum_{x\in W_{\mathcal{D}}}\chi(x)\right| < |\mathcal{D}|^{(r-k)(1-1/2\nu)}\left((2\nu)!|\mathcal{D}|^{k\nu}q+|\mathcal{D}|^{2k\nu}2\nu q^{1/2}\right)^{1/2\nu}. \qquad (3.4)$$

Подставляя последнее неравенство в (3.1), получим

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

Отсюда вытекает первое утверждение теоремы. Далее, положим $a = |\mathcal{D}|^{-r}$. Во множестве $W_{\mathcal{D}}$ есть квадраты, если оценка (3.4) нетривиальна, т.е. если правая часть $\leqslant |\mathcal{D}|^r - 1$. Это равносильно условию

$$(2\nu)^{2\nu}|\mathcal{D}|^{k\nu}q+|\mathcal{D}|^{2k\nu}2\nu q^{1/2} \leqslant |\mathcal{D}|^{2k\nu+r-k}(1-a)^{2\nu},$$

или

$$|\mathcal{D}|^{k\nu}\left(|\mathcal{D}|^{r-k}(1-a)^{2\nu}-2\nu q^{1/2}\right) \geqslant (2\nu)^{2\nu}q.$$

Пусть $|\mathcal{D}|^{r-k} \geqslant 3\nu q^{1/2}(1-a)^{-2\nu}$, или

$$|\mathcal{D}| \geqslant (3\nu)^{\frac{1}{r-k}} p^{\frac{r}{2(r-k)}} (1-a)^{-\frac{2\nu}{r-k}} = (3\nu)^{\frac{1}{r-k}} p^{\frac{1}{2}+\frac{k}{2(r-k)}} (1-a)^{-\frac{2\nu}{r-k}} = p^{1/2} \exp\left(\frac{1}{r-k}(\log 3\nu + \frac{1}{2}k\log p + 2\nu \log(1-a)^{-1})\right). \quad (3.5)$$

Тогда $|\mathcal{D}|^k \geqslant \left(3\nu q^{1/2}\right)^{\frac{k}{r-k}} (1-a)^{-\frac{2\nu k}{r-k}}$ и

$$|\mathcal{D}|^{k\nu}\left(|\mathcal{D}|^{r-k}(1-a)^{2\nu} - 2\nu q^{1/2}\right) \geqslant \nu q^{1/2}\left(3\nu q^{1/2}\right)^{\frac{k\nu}{r-k}} (1-a)^{-\frac{2k\nu^2}{r-k}}.$$

Значит, во множестве $W_{\mathcal{D}}$ имеются квадраты, если выполнено условие (3.5) и неравенство

$$\nu\left(3\nu q^{1/2}\right)^{\frac{k\nu}{r-k}} (1-a)^{-\frac{2k\nu^2}{r-k}} \geqslant (2\nu)^{2\nu} q^{1/2}. \quad (3.6)$$

Вместо (3.6) потребуем условие

$$\left(q^{1/2}\right)^{\frac{k\nu}{r-k}-1} \geqslant (2\nu)^{2\nu} \quad (3.7)$$

(Так как $a \in (0,1)$, то это условие является более сильным, чем (3.6)). Запишем (3.7) в виде

$$\exp\left(\frac{1}{2}r(k\nu+k-r)\log p\right) \geqslant \exp\left((r-k)2\nu\log 2\nu\right),$$

то есть

$$r(k\nu+k-r)\log p \geqslant 4\nu(r-k)\log 2\nu,$$

или

$$\left(k + \frac{k}{\nu} - \frac{r}{\nu}\right)\log p \geqslant 4\left(1-\frac{k}{r}\right)\log 2\nu.$$

Последнее выполнено, если

$$\left(k - \frac{r}{\nu}\right)\log p \geqslant 4\log 2\nu,$$

то есть, если

$$k\log p \geqslant 4\log 2\nu + \frac{r}{\nu}\log p. \quad (3.8)$$

Таким образом, если выполнены (3.5) и (3.8), то $|W_{\mathcal{D}} \cap Q| \geqslant 1$.

В наших интересах выбрать k как можно меньше. Минимум в правой части (3.8) достигается при $\nu = \frac{1}{2}r\log p$. Положим $\nu = \left[\frac{1}{2}r\log p\right]$. Тогда для выполнения (3.8) достаточно брать $k \geqslant (\log p)^{-1}(2\log r + 2\log\log p + 4)$. Положим

$$k = \left[\frac{2\log r + 2\log\log p + 4}{\log p}\right] + 1.$$

Так как при $u \geqslant 3$ функция $\frac{2\log\log u+4}{\log u}$ убывает, то $k \leqslant \left[\frac{2\log r+2\log\log 3+4}{\log 3}\right] + 1 \leqslant r/2$ при $r \geqslant 20$. Далее, имеем $\log(1-a)^{-1} \leqslant \frac{a}{1-a} \leqslant \frac{4}{3}a = \frac{4}{3}|\Delta|^{-r} \leqslant \frac{4}{3}p^{-r/2}$. Поэтому при выбранных ν и k показатель экспоненты в последней строке (3.5) будет не больше, чем

$$\frac{2}{r}\left(\log(5/2)+\log(r\log p)+\log r+\log\log p+2+\frac{1}{2}\log p+\frac{4}{3}p^{-r/2}r\log p\right) = \frac{2}{r}\left(2\log r+\frac{1}{2}\log p+2\log\log p+2+\log(5/2)+\frac{4}{3}p^{-r/2}r\log p\right) \leqslant \frac{1}{r}\left(4\log r+\log p+4\log\log p+8\right).$$

Отсюда вытекает второе утверждение теоремы. $\square$

3.4 Доказательство теоремы 3.3

Применяя соотношение 3.1 и теорему C, мы видим, что

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

далее, заявленные в теореме асимптотические равенства вытекают из предположений и простых оценок на остаток $\frac{r^{O(1)}}{\varepsilon}p^{-\varepsilon^2/2}$. Таким образом, остаётся доказать теорему C в нужном нам виде.

3.4.1 Доказательство теоремы C

Мы полностью следуем работе [8], лишь отслеживая зависимость констант от параметров r и ε.

Напомним, что для множества $A \subset \mathbb{F}_{p^r}$ через $E(A)$ мы обозначаем мультипликативную энергию множества A, то есть число решений уравнения $x^1x^2 = x^3x^4$, где $x^1, x^2, x^3, x^4 \in A$.

Лемма 3.8. *Пусть множество B определено соотношением (0.1), где $N_i, H_i > 0$ – целые числа, причем $H_1 = \ldots = H_r \leqslant p^{1/2}$. Тогда*

$$E(B) \ll r^{O(r)}|B|^2\log p.$$

Доказательство. Положим $H = H_1 = \ldots = H_r$,

$$B_0 = \{x_1a_1+\ldots+x_ra_r : -H \leqslant x_j \leqslant H\},$$

$$Z = \frac{B_0\setminus\{0\}}{B_0\setminus\{0\}}, \qquad f_0(z) = |\{(x,y)\in B_0^2 : xz = y\}|.$$

По лемме 1.2

$$E(B) \leqslant 3|B|^2 + \sum_{z\in Z} f_0^2(z). \tag{3.9}$$

Оценим последнюю сумму. Для фиксированного $z \in Z$ определим решетку Γ в $\mathbb{Z}^{2r}$:

$$\Gamma = \Gamma_z = \left\{ (x_1, \dots, x_r, y_1, \dots, y_r) \in \mathbb{Z}^{2r} : z \sum_{i=1}^{r} x_i a_i = \sum_{i=1}^{r} y_i a_i \right\}.$$

Для фиксированных $x_1, \dots, x_r \in \mathbb{Z}$ условие $(x_1, \dots, x_r, y_1, \dots, y_r) \in \Gamma$ определяет вычет по модулю p каждого из чисел $y_1, \dots, y_r$. Значит, количество точек решетки Γ в большом кубе имеет следующую асимптотику при $M \to \infty$:

$$|\{(x_1, \dots, y_r) \in \Gamma : |x_i| \leqslant M, |y_i| \leqslant M, i = 1, \dots, r\}| = \frac{(2M)^{2r}}{p^r}(1 + o(1)).$$

Поэтому

$$\mathrm{mes}(\mathbb{R}^{2r}/\Gamma) = p^r. \tag{3.10}$$

Определим куб $D \subset \mathbb{R}^{2r}$:

$$D = \{(x_1, \dots, y_r) \in \mathbb{R}^{2r} : |x_i| \leqslant H, |y_i| \leqslant H, i = 1, \dots, r\}.$$

Отметим, что

$$f_0(z) = |D \cap \Gamma_z|. \tag{3.11}$$

Напомним, что *i-й последовательный минимум*

$$\lambda_i = \lambda_i(z) = \lambda_i(D, \Gamma_z)$$

множества D по отношению к Γ_z определяется как минимальное число λ, при котором множество λD содержит i линейно независимых векторов решетки Γ_z, $i = 1, \dots, 2r$. Очевидно, $\lambda_1(z) \leqslant \dots \leqslant \lambda_{2r}(z)$, причем условие $\lambda_1(z) \leqslant 1$ равносильно тому, что $z \in Z$. Вторая теорема Минковского (см., например, [51], теорема 3.30) утверждает, что

$$\frac{2^{2r}}{(2r)!} \leqslant \frac{\lambda_1 \dots \lambda_{2r} \mathrm{mes} D}{\mathrm{mes}(\mathbb{R}^{2r}/\Gamma)}.$$

Учитывая (3.10), получим

$$\lambda_1 \dots \lambda_{2r} \geqslant \frac{p^r}{(2r)! H^{2r}}. \tag{3.12}$$

Хорошо известно (см. [17], предложение 2.1), что число $f_0(z)$ точек решетки Γ в кубе D удовлетворяет неравенству

$$f_0(z) \leqslant \prod_{i=1}^{2r} \left(\frac{2i}{\lambda_i} + 1 \right) \leqslant 2^{2r}(2r)! \prod_{i=1}^{2r} \left(\frac{1}{\lambda_i} + \frac{1}{2i} \right) \leqslant r^{O(r)} \prod_{i=1}^{2r} \max\left(\frac{1}{\lambda_i}, 1 \right). \tag{3.13}$$

Определим полярную решетку $\Gamma^* = \Gamma_z^*$ как множество векторов $(u_1, \dots, u_{2r}) \in \mathbb{R}^{2r}$ таких, что

$$\sum_{i=1}^{r} u_i x_i + \sum_{i=1}^{r} u_{r+i} y_i \in \mathbb{Z}$$

для всех $(x_1, \dots, x_r, y_1, \dots, y_r) \in \Gamma$. Заметим, что $\Gamma_z^* \subset p^{-1}\mathbb{Z}^{2r}$, так как $p\mathbb{Z}^{2r} \subset \Gamma_z$. Обозначим через $\lambda_1^* = \lambda_1^*(z)$ первый последовательный минимум решетки Γ_z^* по отношению к множеству

$$D^* = \left\{ (u_1, \dots, u_{2r}) : \sum_{i=1}^{2r} |u_i| \leqslant \frac{1}{H} \right\}$$

Согласно предложению 3.6 из [14], имеем

$$\lambda_{2r}\lambda_1^* \ll r(1 + \log r)^{1/2} = r^{O(1)}. \tag{3.14}$$

Обозначим

$$\nu = \nu(z) = \min\left(\lambda_1 H, \frac{p\lambda_1^*}{H}\right), \qquad s = \max\{j : \lambda_j \leqslant 1\}.$$

Если $z \in Z$, то $\lambda_1 \leqslant 1$ и число s определено корректно. Заметим также, что $\nu(z) \geqslant 1$.

В случае $s \leqslant r$ получаем

$$\prod_{i=1}^{2r} \max\left(1, \frac{1}{\lambda_i}\right) = \prod_{i=1}^{s} (\lambda_i)^{-1} \leqslant (\lambda_1)^{-r} \leqslant \nu^{-r} H^r.$$

Если же $s > r$, то ввиду (3.12) и (3.14) имеем

$$\prod_{i=1}^{2r} \max\left(1, \frac{1}{\lambda_i}\right) = \prod_{i=1}^{s} (\lambda_i)^{-1} \leqslant (\lambda_{2r})^{2r-s} \prod_{i=1}^{2r} (\lambda_i)^{-1} \leqslant r^{O(r)} (\lambda_1^*)^{s-2r} \prod_{i=1}^{2r} (\lambda_i)^{-1} \leqslant$$
$$r^{O(r)} \left(\frac{p}{H\nu}\right)^{2r-s} \frac{(2r)! H^{2r}}{p^r} = r^{O(r)} \nu^{-r} H^r \left(\frac{H\nu}{p}\right)^{s-r}.$$

Но

$$\frac{H\nu}{p} \leqslant \frac{H^2\lambda_1}{p} \leqslant \frac{H^2}{p} \leqslant 1,$$

и, значит, в обоих случаях справедливо

$$\prod_{i=1}^{2r} \max\left(1, \frac{1}{\lambda_i}\right) \leqslant r^{O(r)} \nu^{-r} H^r.$$

Учитывая (3.13), получаем

$$f_0(z) \leqslant r^{O(r)} \nu(z)^{-r} H^r. \tag{3.15}$$

Положим $J := [\log_2 H]+1$ и разобьем множество Z на подмножества Z_j, $\quad j = 1, \dots, J$, где

$$Z_j = \{z \in Z_0 : 2^{j-1} \leqslant \nu(z) < 2^j\}.$$

Заметим, что $Z_j \subset Z_j^1 \cup Z_j^2$, где

$$Z_j^1 = \{z \in Z : \lambda_1(z)H < 2^j\}, \qquad Z_j^2 = \{z \in Z : p\lambda_1^*(z)/H < 2^j\}.$$

Если $z \in Z_j^1$, то найдется ненулевой вектор $v = (v_1, \dots, v_{2r}) \in \Gamma_z$ такой, что $\max_i |v_i| < 2^j$. Вектор v однозначно определяет z, так как

$$z = \sum_{i=r+1}^{2r} v_i a_{i-r} \left(\sum_{i=1}^{r} v_i a_i \right)^{-1}.$$

(Случай, когда оба вектора

$$\sum_{i=r+1}^{2r} v_i a_{i-r} \quad \text{и} \quad \sum_{i=1}^{r} v_i a_i$$

равны нулю в $\mathbb{F}_{p^r}$ невозможен, так как $\max_i |v_i| < 2^J \leqslant p$). Поэтому $\left|Z_1^j\right| < (2^{j+1})^{2r}$. Аналогично, для $z \in Z_j^2$ найдется ненулевой вектор $u = (u_1, \dots, u_{2r}) \in p\Gamma_z^*$ такой, что $\sum_i |u_i| < 2^j$. Вектор u однозначно определяет z. В самом деле, предположим противное. Тогда найдутся различные z' и z'' такие, что $u \in p\Gamma_{z'}^*$ и $u \in p\Gamma_{z''}^*$. Возьмем произвольный элемент $x \in \mathbb{F}_{p^r}$, $x = \sum\limits_{i=1}^{r} x_i a_i$. Пусть

$$y' = xz' = \sum_{i=1}^{r} y_i' a_i, \qquad y'' = xz'' = \sum_{i=1}^{r} y_i'' a_i.$$

Тогда $(x_1, \dots, x_r, y_1', \dots, y_r') \in \Gamma_{z'}$, $\quad (x_1, \dots, x_r, y_1'', \dots, y_r'') \in \Gamma_{z''}$, и мы имеем

$$\sum_{i=1}^{r} y_i u_{i+r} \equiv 0 \pmod{p}, \tag{3.16}$$

где $y_i = y_i' - y_i''$. Так как уравнение $xz' - xz'' = y$ разрешимо (относительно x) для любого $y \in \mathbb{F}_{p^r}$, то сравнение (3.16) выполнено при всех $(y_1, \dots, y_r) \in \mathbb{Z}^r$. Значит,

$$u_{r+1} \equiv \dots \equiv u_{2r} \equiv 0 \pmod{p},$$

и в силу того, что $\max_i |u_i| < 2^J \leqslant p$, мы получаем

$$u_{r+1} = \dots = u_{2r} = 0.$$

Отсюда следует, что

$$\sum_{i=1}^{r} x_i u_i \equiv 0 \pmod{p}$$

при всех $(x_1, \dots, x_r) \in \mathbb{Z}^r$, и, стало быть, $u_1 = \dots = u_{2r} = 0$, что противоречит выбору вектора u. Итак, значит, вектор u однозначно определяет z, а поэтому $|Z_j^2| < (2^{j+1})^{2r}$.

Объединяя полученные выше оценки, имеем

$$|Z_j| \leqslant |Z_j^1| + |Z_j^2| < 2^{2r+1} 2^{2jr},$$

$$\sum_{z \in Z_j} f_0(z)^2 \leqslant r^{O(r)} (2^{j-1})^{-2r} H^{2r} |Z_j| \leqslant r^{O(r)} H^{2r}$$

$$\sum_{z \in Z} f_0(z)^2 = \sum_{j=1}^{J} \sum_{z \in Z_j} f_0(z)^2 \leqslant r^{O(r)} H^{2r} \log p.$$

Применяя (3.9), получаем утверждение леммы. $\square$

Для натурального $H \leqslant p/2$ и мультипликативного характера χ на $\mathbb{F}_{p^r}$ положим

$$\Delta(H, \chi) = \max_B \left| \sum_{x \in B} \chi(x) \right| |B|^{-1},$$

где максимум берется по всем параллелепипедам вида (0.1) таким, что

$$H \leqslant H_i \leqslant 2H, \qquad i = 1, \dots, r. \tag{3.17}$$

Заметим, что если рёбра параллелепипеда B удовлетворяют более слабым, чем (3.17), условиям, а именно,

$$H \leqslant H_i \leqslant p, \qquad i = 1, \dots, r,$$

то его можно разбить на параллелепипеды, рёбра которых удовлетворяют условиям (3.17). Поэтому

$$\left| \sum_{x \in B} \chi(x) \right| \leqslant \Delta(H, \chi) |B|,$$

и для того, чтобы доказать теорему C, достаточно проверить, что при всех $0 < \varepsilon \leqslant 1/4$ справедливо

$$\Delta([p^{1/4+\varepsilon}], \chi) \ll \frac{1}{\varepsilon} r^{O(1)} p^{-\varepsilon^2/2}. \tag{3.18}$$

Приведем еще один вспомогательный результат.

Лемма 3.9. *[[8], лемма 2] Пусть множество B определено соотношением (0.1), где $N_i, H_i > 0$ — целые числа, удовлетворяющие (3.17). Предположим, что $H, \widetilde{H}$ — натуральные числа, $\widetilde{H} \leqslant H/2$, и элемент $u = \sum_{i=1}^{r} u_i a_i$ удовлетворяет условию*

$$1 \leqslant u_i \leqslant \widetilde{H}, \qquad i = 1, \dots, r.$$

Пусть, далее, χ — мультипликативный характер в $\mathbb{F}_{p^r}$. Тогда

$$\left| \sum_{x \in B} \chi(x) - \sum_{x \in B} \chi(x+u) \right| \leqslant 6r\Delta(\widetilde{H}, \chi)|B|\frac{\widetilde{H}}{H}.$$

Следующая лемма основана на хорошо известном методе, разработанным Карацубой ([5], [6]), который позволяет получить оценку сумм характеров через лемму 3.8 и лемму N.

Лемма 3.10. *Пусть $s, H, \widetilde{H}$ — натуральные числа, и*

$$G := [p^{r/(2s)}] \leqslant \widetilde{H} \leqslant \frac{H}{2}, \qquad H \leqslant p^{1/2}.$$

Пусть также χ — нетривиальный мультипликативный характер на $\mathbb{F}_{p^r}$. Тогда имеет место следующее неравенство:

$$\Delta(H, \chi) \leqslant 6r\Delta(\widetilde{H}, \chi)\frac{\widetilde{H}}{H} + O(sr^{O(r/s)}(\log p)^{1/(2s)}(H\widetilde{H}G^{-1}p^{-1/2})^{-r/(2s)}).$$

Доказательство. Положим $I = [1, G] \cap \mathbb{Z}$, $H_0 = [\widetilde{H}/G]$, и

$$B_0' = \left\{ \sum_{i=1}^{r} x_i a_i : 1 \leqslant x_i \leqslant H_0,\ i = 1, \dots, r \right\}.$$

Заметим, что любой элемент $x = yz$, $y \in B_0'$, $z \in I$, может быть представлен в виде

$$x = \sum_{i=1}^{r} x_i a_i \,,$$

где $1 \leqslant x_i \leqslant \widetilde{H}$ для всех $i = 1, \dots, r$. Согласно лемме 3, для всех $y \in B_0'$, $z \in I$ справедливо

$$\left| \sum_{x \in B} \chi(x + yz) - \sum_{x \in B} \chi(x) \right| \leqslant 6r\Delta(\widetilde{H}, \chi)|B|\frac{\widetilde{H}}{H}.$$

Поэтому

$$\left| \sum_{x \in B} \chi(x) - \frac{1}{|B_0'|G} \sum_{x \in B, y \in B_0', z \in I} \chi(x + yz) \right| \leqslant 6r\Delta(\widetilde{H}, \chi)|B|\frac{\widetilde{H}}{H}. \qquad (3.19)$$

Далее,

$$\left|\sum_{x\in B,y\in B_0',z\in I}\chi(x+yz)\right| \leqslant \sum_{x\in B,y\in B_0'}\left|\sum_{z\in I}\chi(x+yz)\right|$$
$$= \sum_{x\in B,y\in B_0'}\left|\sum_{z\in I}\chi(xy^{-1}+z)\right| = \sum_{u\in\mathbb{F}_{p^r}}\omega(u)\left|\sum_{z\in I}\chi(u+z)\right|,$$

где

$$\omega(u) = \left|\left\{(x,y)\in B\times B_0' : \frac{x}{y}=u\right\}\right|.$$

Дважды используя неравенство Гёльдера, получаем

$$\left|\sum_{x\in B,y\in B_0',z\in I}\chi(x+yz)\right| \leqslant$$
$$\left(\sum_{u\in\mathbb{F}_{p^r}}\omega(u)\right)^{1-1/s}\left(\sum_{u\in\mathbb{F}_{p^r}}\omega(u)^2\right)^{1/(2s)}\left(\sum_{u\in\mathbb{F}_{p^r}}\left|\sum_{z\in I}\chi(u+z)\right|^{2s}\right)^{1/(2s)}. \tag{3.20}$$

Очевидно,

$$\sum_{u\in\mathbb{F}_{p^r}}\omega(u) = |B||B_0'|. \tag{3.21}$$

Оценим теперь сумму $\sum\limits_{u\in\mathbb{F}_{p^r}}\omega(u)^2$. Положим $B^* = B\setminus\{0\}$. Имеем

$$\sum_{u\in\mathbb{F}_{p^r}}\omega(u)^2 = \omega(0)^2 + \sum_{u\in\mathbb{F}_{p^r}^*}\omega(u)^2$$
$$= \omega(0)^2 + |\{(x_1,x_2,y_1,y_2)\in B^*\times B^*\times B_0'\times B_0' : x_1y_2 = x_2y_1\}|$$
$$\leqslant |B_0'|^2 + \sum_{\nu\in\mathbb{F}_{p^r}^*}\left|\left\{(x_1,x_2)\in B^*\times B^* : \frac{x_1}{x_2}=\nu\right\}\right|\left|\left\{B_0'\times B_0' : \frac{y_1}{y_2}=\nu\right\}\right|$$
$$\leqslant |B_0'|^2 + E(B)^{1/2}E(B_0')^{1/2}.$$

Используя лемму 3.8, и принимая во внимание, что $|B_0'|\leqslant|B|$, получим

$$\sum_{u\in\mathbb{F}_{p^r}}\omega(u)^2 \leqslant r^{O(r)}|B||B_0'|\log p. \tag{3.22}$$

Далее, мы используем оценку последней суммы в (3.20), полученную в [28].

Для полноты мы воспроизводим здесь доказательство.

$$\sum_{u\in\mathbb{F}_{p^r}}\left|\sum_{z\in I}\chi(u+z)\right|^{2s}=$$

$$\sum_{z_1,\dots,z_{2s}\in I}\left|\sum_{u\in\mathbb{F}_q}\chi\left((u+z_1)\dots(u+z_s)(u+z_{s+1})^{q-2}\dots(u+z_{2s})^{q-2}\right)\right|.$$

Последняя сумма уже оценивалась нами в частном случае, когда $\chi-$квадратичный характер, при доказательстве леммы 3.7. В общем случае работают аналогичные рассуждения. Мы можем применить лемму N для тех наборов $(z_1,\dots,z_{2s})$, в которых хотя бы один элемент встретился ровно один раз. Для таких наборов получим (см. оценку на сумму)

$$\left|\sum_{u\in\mathbb{F}_q}\chi\left((u+z_1)\dots(u+z_s)(u+z_{s+1})^{q-2}\dots(u+z_{2s})^{q-2}\right)\right|<2sp^{r/2}.$$

Сумму по наборам $(z_1,\dots,z_{2s})$, в которых каждый элемент встретился как минимум дважды, оценим произведением p^r на количество таких наборов. Так как все элементы $z_1,\dots,z_{2s}$ лежат в некотором подмножестве множества I, содержащем $\min(s,G)$ элементов, и для конкретного такого подмножества есть не более s способов выбрать каждый элемент, то количество интересующих нас наборов не превосходит $G^s s^{2s}$. Поэтому

$$\sum_{u\in\mathbb{F}_{p^r}}\left|\sum_{z\in I}\chi(u+z)\right|^{2s}\leqslant G^s s^{2s}p^r+2sG^{2s}p^{r/2},$$

$$\left(\sum_{u\in\mathbb{F}_{p^r}}\left|\sum_{z\in I}\chi(u+z)\right|^{2s}\right)^{1/(2s)}\leqslant sG^{1/2}p^{r/(2s)}+2Gp^{r/(4s)}.$$

По определению числа G имеем

$$\left(\sum_{u\in\mathbb{F}_{p^r}}\left|\sum_{z\in I}\chi(u+z)\right|^{2s}\right)^{1/(2s)}\leqslant(2s+2)Gp^{r/(4s)}. \tag{3.23}$$

Подставляя (3.21)–(3.23) в (3.20), получаем

$$\left|\sum_{x\in B,y\in B_0',z\in I}\chi(x+yz)\right| \ll sr^{O(r/s)}\left(|B||B_0'|\right)^{1-1/(2s)}(\log p)^{1/(2s)}Gp^{r/(4s)}$$
$$= sr^{O(r/s)}(\log p)^{1/(2s)}|B||B_0'|G\left(|B||B_0'|\right)^{-1/(2s)}p^{r/(4s)}$$
$$\leqslant sr^{O(r/s)}(\log p)^{1/(2s)}|B||B_0'|G\left(H\left[\frac{\widetilde{H}}{G}\right]p^{-1/2}\right)^{-r/(2s)}$$
$$\leqslant 2^{r/(2s)}sr^{O(r/s)}(\log p)^{1/(2s)}|B||B_0'|G\left(H\widetilde{H}G^{-1}p^{-1/2}\right)^{-r/(2s)}. \quad (3.24)$$

Из последнего неравенства и (3.19) следует, что

$$\left|\sum_{x\in B}\chi(x)\right| \leqslant 6r\Delta(\widetilde{H},\chi)|B|\frac{\widetilde{H}}{H}+O\left(sr^{O(r/s)}(\log p)^{1/(2s)}|B|\left(H\widetilde{H}G^{-1}p^{-1/2}\right)^{-r/(2s)}\right).$$

Так как выбор B был произвольным, то лемма доказана. $\square$

Предположим в лемме 3.10, что

$$s \geqslant 2r. \quad (3.25)$$

Введем параметр α, удовлетворяющий условию

$$0 < \alpha \leqslant \frac{1}{(12r)^2}. \quad (3.26)$$

Предположим также, что

$$0 < \varepsilon \leqslant \frac{1}{4}, \qquad H = [p^{1/4+\varepsilon}]. \quad (3.27)$$

Положим

$$H_i = [\alpha^i H], \qquad i \geqslant 0$$

и будем для краткости писать $\Delta(H)$ вместо $\Delta(H,\chi)$ и $\Delta(H_i)$ вместо $\Delta(H_i,\chi)$. Пусть I – наибольшее целое число такое, что $H_i \geqslant G$, где G определено в лемме 3.10. Так как $H \geqslant G$ в силу (3.25) и (3.27), то число I определено корректно.

Применяя лемму 3.10 к H_i и H_{i+1}, мы можем последовательно оценить $\Delta(H_i)$ через $\Delta(H_{i+1})$, $i = 0,\dots,I-1$:

$$\Delta(H_i) \leqslant 6r\Delta(H_{i+1})\frac{H_{i+1}}{H_i}+O\left(sr^{O(r/s)}(\log p)^{1/(2s)}(H_iH_{i+1}G^{-1}p^{-1/2})^{-r/(2s)}\right).$$

Поэтому

$$\Delta(H) \leqslant (6r)^I \Delta(H_I)\frac{H_I}{H} + \\ sr^{O(r/s)}(\log p)^{1/(2s)}(Gp^{1/2})^{r/(2s)} \sum_{i=0}^{I-1} O\left((6r)^i \frac{H_i}{H}(H_i H_{i+1})^{-r/(2s)}\right). \quad (3.28)$$

Далее,

$$(6r)^I \Delta(H_I)\frac{H_I}{H} \leqslant (6r)^{\log H/(-\log\alpha)}\frac{H_I}{H} \\ \leqslant (6r)^{\log p/(-2\log\alpha)}\alpha^{-1}\frac{2G}{H} = 2p^{\log(6r)/(-2\log\alpha)}\alpha^{-1}\frac{G}{H} \quad . \quad (3.29)$$

Принимая во внимание (3.25) и (3.26), получим

$$\sum_{i=0}^{I-1}(6r)^i \frac{H_i}{H}(H_i H_{i+1})^{-r/(2s)} \leqslant \sum_{i=0}^{I-1}(6r)^i \alpha^i \left(\frac{H^2\alpha^{2i+1}}{4}\right)^{-r/(2s)} \\ \leqslant 2H^{-r/s}\alpha^{-r/(2s)}\sum_{i=0}^{I-1}(6r)^i\alpha^{i(1-r/s)} \leqslant 2H^{-r/s}\alpha^{-r/(2s)}\sum_{i=0}^{I-1}(6r)^i\alpha^{i/2} \\ \leqslant 2H^{-r/s}\alpha^{-r/(2s)}\sum_{i=0}^{I-1}2^{-i} \leqslant 4H^{-r/s}\alpha^{-r/(2s)}. \quad (3.30)$$

Подставляя (3.29) и (3.30) в (3.28), находим

$$\Delta(H) \leqslant 2p^{\log 6r/(-2\log\alpha)}\alpha^{-1}\frac{G}{H} + O\left(sr^{O(r/s)}(\log p)^{1/(2s)}(Gp^{1/2})^{r/(2s)}H^{-r/s}\alpha^{-r/(2s)}\right) \\ \leqslant 4p^{\log 6r/(-2\log\alpha)}\alpha^{-1}p^{r/(2s)-1/4-\varepsilon} + O\left(sr^{O(r/s)}(\log p)^{1/(2s)}\alpha^{-1}p^{-(r/s)(\varepsilon-r/(4s))}\right). \quad (3.31)$$

Для завершения доказательства теоремы C выберем параметры s и α следующим образом:

$$s = \left[\frac{r}{2\varepsilon}\right] + 1, \qquad \alpha = (6r)^{-3}.$$

Легко видеть, что при этом условия (3.25) и (3.26) выполнены. Так как

$$\frac{4\varepsilon}{3} \leqslant \frac{r}{s} \leqslant 2\varepsilon,$$

то

$$\frac{r}{s}\left(\varepsilon - \frac{r}{4s}\right) \geqslant \frac{2}{3}\varepsilon^2;$$

следовательно,

$$(\log p)^{1/(2s)}\alpha^{-1}p^{-(r/s)(\varepsilon-r/(4s))} \leqslant (6r)^3(\log p)^{\varepsilon/r}p^{-2\varepsilon^2/3} \\ = (6r)^3\exp\left(\frac{\varepsilon}{r}\log\log p - \frac{\varepsilon^2}{6}\log p\right)p^{-\frac{\varepsilon^2}{2}} \ll r^3 p^{-\frac{\varepsilon^2}{2}}.$$

Наконец,

$$p^{\log 6r/(-2\log\alpha)}\alpha^{-1}p^{r/(2s)-1/4-\varepsilon} \leqslant (6r)^3 p^{1/6}p^{-1/4} \ll r^3 p^{-1/12}.$$

Значит, неравенство (3.31) дает нам

$$\Delta(H) \ll r^3 p^{-1/12} + \frac{r}{\varepsilon} r^{3+O(\varepsilon)} p^{-\varepsilon^2/2} \leqslant \frac{r^{4+O(\varepsilon)} p^{-\varepsilon^2/2}}{\varepsilon}.$$

Таким образом, неравенство (3.31) влечет неравенство (3.18), и теорема C доказана. $\square$

3.5 Доказательство теоремы 3.4.

Доказательство аналогично доказательству теоремы 3.1.

Через χ обозначим квадратичный характер на $\mathbb{F}_q$; считаем, что $\chi(0) = 0$. Пусть 0 не принадлежит некоторому D_i. Тогда

$$|W \cap Q| = \frac{1}{2}\sum_{x\in W}(1+\chi(x)) = \frac{1}{2}|W| + \frac{1}{2}\sum_{x\in W}\chi(x) = \frac{1}{2}|W| + \frac{1}{2}\sum_{x\in W}\chi(x).$$

Если же $0 \in D_i$ при всех i, то

$$|W \cap Q| = \frac{1}{2}\sum_{x\in W\setminus\{0\}}(1+\chi(x)) = \frac{1}{2}(|W|-1) + \frac{1}{2}\sum_{x\in W}\chi(x).$$

Таким образом, всегда справедливо неравенство

$$\left||W\cap Q| - \frac{|W|}{2}\right| \leqslant \frac{1}{2} + \frac{1}{2}\left|\sum_{x\in W}\chi(x)\right|, \tag{3.32}$$

и для доказательства теоремы нужно оценить сумму характеров $\left|\sum\limits_{x\in W}\chi(x)\right|$. Положим $D = D_2 \times \ldots \times D_r$ и $b_j = a_j/a_1$. Тогда $b_1 = 1$ и $\{1, b_2, \ldots, b_r\}$ — базис. Имеем

$$\left|\sum_{x\in W}\chi(x)\right| \leqslant \sum_{c_1\in D_1}\left|\sum_{c_j\in D_j,\, j\geqslant 2}\chi(c_1a_1+\ldots+c_ra_r)\right| \leqslant |D_1|^{1/2}A^{1/2}, \tag{3.33}$$

где

$$A = \sum_{c_1\in D_1}\left|\sum_{(c_2,\ldots,c_r)\in D}\chi(c_1+c_2b_2\ldots+c_rb_r)\right|^2.$$

Пусть L_d — множество тех наборов $(c_2,\ldots,c_r) \in D$, для которых элемент $c_2b_2+\ldots+c_rb_r$ лежит в подполе порядка p^d и не лежит ни в каком подполе

меньшего порядка. Ясно, что $D = \bigsqcup_{d|r} L_d$, причем $L_1 = \{0\}$, если $0 \in D_i$ при всех $2 \leqslant i \leqslant r$, и $L_1 = \varnothing$ иначе. Для $d|r$ определим функцию $f_d(x)\colon D_1 \to \mathbb{C}$, $f_d(c) = \sum\limits_{(c_2,\ldots,c_r)\in L_d} \chi(c + c_2b_2 + \ldots + c_rb_r)$. Напомним, что l_2-норма функции $g\colon D_1 \to \mathbb{C}$ определяется как $\|g\|_2 = \left(\sum\limits_{x\in D_1} |g(x)|^2\right)^{1/2}$. Тогда в силу неравенства треугольника

$$A^{1/2} = \left\|\sum_{d|r} f_d\right\|_2 \leqslant \sum_{d|r} \|f_d\|_2 = \sum_{d|r} A_d^{1/2}. \tag{3.34}$$

где

$$A_d = \sum_{x\in D_1} \left|\sum_{(c_2,\ldots,c_r)\in L_d} \chi(x + c_2b_2 + \ldots + c_rb_r)\right|^2.$$

По определению множества L_d при любом наборе $(c_2,\ldots,c_r) \in L_d$ элемент $c_2b_2 + \ldots + c_rb_r$ порождает подполе порядка p^d. Учитывая, что каждый такой элемент имеет не более d сопряженных, и применяя лемму М к парам несопряженных элементов, при $d > 1$ имеем

$$A_d \leqslant \sum_{(c_2,\ldots,c_r),(c_2',\ldots,c_r')\in L_d} \left|\sum_{x\in F_p} \chi(x + c_2b_2 + \ldots + c_rb_r)\overline{\chi}(x + c_2'b_2 + \ldots + c_r'b_r)\right| \leqslant$$
$$\sum_{(c_2,\ldots,c_r)\in L_d} \Big(dp + (|L_d| - d)(2d-1)p^{1/2}\Big) \leqslant (2d-1)p^{1/2}|L_d|^2 + dp|L_d|.$$

Кроме того, $A_1 \leqslant |D_1| \leqslant p$. Обозначим $\mathcal{J} = \{d|r : d > 1 \text{ и } L_d \neq \emptyset\}$. Тогда при $d \in \mathcal{J}$ в силу неравенства $\sqrt{A+B} \leqslant \sqrt{A}\left(1 + \frac{B}{2A}\right)$, верного при всех положительных A и B, получаем

$$A_d^{1/2} \leqslant (2d-1)^{1/2}p^{1/4}|L_d| + \frac{dp^{3/4}}{2(2d-1)^{1/2}}.$$

Из этой оценки и неравенства (3.34) имеем

$$A^{1/2} \leqslant p^{1/4}S_1 + \frac{1}{2}p^{3/4}S_2 + p^{1/2},$$

где

$$S_1 = \sum_{d\in\mathcal{J}} (2d-1)^{1/2}|L_d|, \quad S_2 = \sum_{d\in\mathcal{J}} \frac{d}{(2d-1)^{1/2}}.$$

Учитывая, что $\sum\limits_{d|r} |L_d| = |D_2|\ldots|D_r|$, получаем

$$S_1 \leqslant (2r-1)^{1/2}|D_2|\ldots|D_r|, \quad S_2 \leqslant \sum_{d\in\mathcal{J}} d^{1/2} \leqslant \frac{1}{2}r^{3/2}.$$

(Последняя оценка проверяется непосредственно при $2 \leqslant r \leqslant 7$, а при $r \geqslant 8$ вытекает из неравенств $r^{1/2} \leqslant \frac{1}{6} r^{3/2}$ и $\sum\limits_{d \leqslant r/2} d^{1/2} \leqslant \frac{2}{3}(r/2+1)^{3/2} \leqslant \frac{1}{3} r^{3/2}$.)

Значит,

$$A^{1/2} \leqslant p^{1/4}(2r-1)^{1/2}|D_2|\dots|D_r| + \frac{1}{4}p^{3/4}r^{3/2} + p^{1/2}.$$

Подставляя последнее неравенство в (3.33), получим

$$\left|\sum_{x\in W}\chi(x)\right| \leqslant |D_1|^{1/2}\left(p^{1/4}(2r-1)^{1/2}|D_2|\dots|D_r| + \frac{1}{4}p^{3/4}r^{3/2} + p^{1/2}\right) = |D_1|^{-1/2}p^{1/4}(2r-1)^{1/2}|W| + |D_1|^{1/2}\left(\frac{1}{4}p^{3/4}r^{3/2} + p^{1/2}\right)$$

Аналогично получается оценка

$$\left|\sum_{x\in W}\chi(x)\right| \leqslant |D_i|^{-1/2}p^{1/4}(2r-1)^{1/2}|W| + |D_i|^{1/2}\left(\frac{1}{4}p^{3/4}r^{3/2} + p^{1/2}\right)$$

Выберем i так, чтобы эта оценка была наилучшей. Рассмотрим функцию $H(x) = x^{-1/2}p^{1/4}(2r-1)^{1/2}|W| + x^{1/2}\left(\frac{1}{4}p^{3/4}r^{3/2} + p^{1/2}\right)$, $1 \leqslant x \leqslant |W|$. Имеем

$$H'(x) = \frac{\frac{1}{4}p^{3/4}r^{3/2} + p^{1/2}}{2x^{1/2}} - \frac{p^{1/4}(2r-1)^{1/2}|W|}{2x^{3/2}},$$

и $H'(x) = 0$ при $x = 4|W|p^{-1/2}\frac{(2r-1)^{1/2}}{r^{3/2}+4p^{-1/4}} \geqslant 2|W|p^{-1/2}r^{-1} \geqslant |W|^{1/2}$ при $|W| \geqslant 8p^{r/2}(2r-1)^r$. Таким образом, минимум функции $H(x)$ достигается при $x \geqslant |W|^{1/2} \geqslant |W|^{1/r}$. Мы можем выбрать i так, что $|D_i| \geqslant |W|^{1/r}$; так как $H'(x) < 0$ при $|W|^{1/r} \leqslant x \leqslant |W|^{1/2}$, то можно гарантировать оценку

$$\left|\sum_{x\in W}\chi(x)\right| \leqslant H(|W|^{1/r}) = |W|^{1-1/(2r)}p^{1/4}(2r-1)^{1/2} + |W|^{1/(2r)}\left(\frac{1}{4}p^{3/4}r^{3/2} + p^{1/2}\right).$$

Из неравенства (3.32) и последней оценки вытекает утверждение теоремы. □

3.6 Доказательство следствий 3.5 и 3.6.

Доказательство следствия 3.5. Из теоремы 3.4 следует, что

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

При $|W| \geqslant (2r-1)^r p^{r(1/2+\varepsilon)}$ имеем $|W|^{-1/(2r)} \leqslant (2r-1)^{-1/2} p^{-1/4} p^{-\varepsilon/2}$ и

$$|W \cap Q| = |W| \left(\frac{1}{2} + O\left(p^{-\varepsilon/2} + r^{2-r} p^{1-r/2} p^{-(2r-1)\varepsilon/2} \right) \right).$$

Так как $r \geqslant 2$, то отсюда вытекает утверждение следствия 3.5. $\square$

Доказательство следствия 3.6. Во множестве W есть квадраты, если правая часть неравенства (2.5) строго меньше, чем $|W|-1$. Это равносильно условию

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

Покажем, что последнее неравенство выполнено при $|W| \geqslant 8(2r-1)^r p^{r/2}$. Имеем $|W|^{1/(2r)} \geqslant \left(e^2 (2r-1)^r p^{r/2} \right)^{1/(2r)} \geqslant (1+1/r)(2r-1)^{1/2} p^{1/4}$ и

$$|W|^{1-1/r} \left(|W|^{1/(2r)} - (2r-1)^{1/2} p^{1/4} \right) \geqslant \frac{1}{r} (2r-1)^{1/2} p^{1/4} (2r-1)^{r-1} p^{(r-1)/2} =$$
$$\frac{1}{r} (2r-1)^{r-1/2} p^{(r-1)/2+1/4} \geqslant \frac{3}{4} p^{3/4} r^{3/2} > \frac{1}{4} p^{3/4} r^{3/2} + p^{1/2} + |W|^{-1/(2r)}.$$

Здесь предпоследнее неравенство очевидно при $r \geqslant 3$ и легко проверяется при $r = 2$; последнее неравенство следует из неравенства $\frac{1}{2} p^{3/4} r^{3/2} > p^{1/2} + (2r-1)^{-1/2} p^{-1/4}$, верного при всех $p \geqslant 3$, $r \geqslant 2$.

Следствие доказано. $\square$

Глава 4

Множества, разность которых не содержит квадратов

Главным результатом этой 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 неё 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.

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*

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

Кроме того, мы представляем короткое доказательство нижней оценки, полученной в работе [21] (если m есть произведение различных простых чисел вида $4k+1$, то найдётся множество $A \subset \mathbb{Z}_m$ такое, что $A-A$ не содержит квадратичных вычетов и $|A| \geqslant \prod_{p|m} \frac{\log_2 p}{2}$).

Пусть сначала m является простым числом $p \equiv 1 \pmod 4$. Рассмотрим полный граф $G=(V,E)$ с множеством вершин $V=\mathbb{Z}_p$ и разбиение $E = E_1 \bigsqcup E_2$, где

$$E_1 = \{(x,y) : x-y \text{ — квадратичный вычет по модулю } p\}$$

и $E_2 = E \setminus E_1$. Тогда если $|V| = p \geqslant \binom{2n-2}{n-1}$, то согласно теореме Рамсея о раскраске в два цвета (см., например, [51], Теорема 6.9) найдется подграф $G'=(V',E')$ нашего графа G такой, что $|V'|=n$ и $E' \subseteq E_j$ для некоторого $j \in \{1,2\}$. Таким образом, мы можем гарантировать наличие такого подграфа с по крайней мере $\frac{1}{2}\log_2 p$ вершинами. Если при этом $E \subseteq E_2$, то множество V' даёт нам нужный пример; если же $E \subseteq E_1$, то при любом квадратичном невычете $\xi \in \mathbb{Z}_p$ мы получаем нужный пример в виде $\xi V'$. Пусть теперь $m = \prod_{i=1}^k p_i$, где p_i — различные простые вида $4l+1$. Имея множества $A_i \subset \mathbb{Z}_{p_i}$, $i=1,\dots,k$, обладающие тем свойством, что $A_i - A_i$ не содержит ненулевых квадратичных вычетов, построим множество $A_1 \times \ldots \times A_k \subset \mathbb{Z}_m$. Легко видеть, что оно также обладает нужным свойством, причём $|A| \geqslant \prod_{p|m} \frac{\log_2 p}{2}$. Тем самым нужная оценка доказана.

Теорема 4.1 будет доказана в разделе 4.1. Следствие 4.2 непосредственно вытекает из теоремы; следствие 4.3 доказывается в разделе 4.2, следствие 4.4 доказывается в разделе 4.3. Под словом «невычет» везде далее понимается квадратичный невычет.

4.1 Доказательство теоремы 4.1

Не ограничивая общности, можно считать, что m нечетно. Проведём доказательство индукцией по n. В случае когда $n=1$, то есть когда $m=p$ — простое, докажем оценку $|A| \leqslant p^{1/2}$. Если $p \equiv 3 \pmod 4$, то легко видеть, что $|A| \leqslant 1$; пусть $p \equiv 1 \pmod 4$. Мы приводим изящное фольклорное доказательство. Предположим, что $|A| > p^{1/2}$ и зафиксируем квадратичный невычет $\xi \in \mathbb{Z}_p$. Рассмотрим отображение $\varphi\colon A^2 \to \mathbb{Z}_p$, $\varphi(a,b) = a + \xi b$. Согласно принципу Дирихле, найдутся две различные пары (a_1,b_1) и (a_2,b_2) такие, что $\varphi(a_1,b_1) = \varphi(a_2,b_2)$, что равносильно $\xi = (a_1-a_2)(b_2-b_1)^{-1}$. Но последнее означает, что одна из разностей a_1-a_2 и b_1-b_2 является квадратичным невычетом по модулю p. Тем самым утверждение доказано.

Предположим, что $n \geqslant 2$ и теорема верна для всех значений m, свободных от квадратов и имеющих менее n простых делителей. Пусть $p_1 < p_2 < \ldots < p_n$ — все простые делители числа m. Обозначим через χ_j квадратичный характер по модулю p_j. По предположению каждая разность a_1-a_2 различных элементов множества A является невычетом по крайней мере по

одному модулю p_i. Поэтому

$$|A| = \sum_{a_1,a_2\in A:\, a_1=a_2} 1 = \sum_{a_1=a_2\in A} \prod_{j=1}^{n}(1+\chi_j(a_1-a_2)) = \sum_{a_1,a_2\in A} \prod_{j=1}^{n}(1+\chi_j(a_1-a_2)) = |A|^2 + \sum_{D} \sum_{a_1,a_2\in A} \chi_D(a_1-a_2),$$

где D пробегает все непустые подмножества $[n] = \{1,\dots,n\}$ и $\chi_D(x) = \prod_{j\in D}\chi_j(x)$. Положим $\sigma = 1 - |A|^{-1}$. Перепишем последнее равенство в следующем виде:

$$|A|^2\sigma = -\sum_{D} \sum_{a_1,a_2\in A} \chi_D(a_1-a_2).$$

Применяя неравенство Коши-Буняковского, получим

$$|A|^2\sigma \leqslant \sum_{D} |A|^{1/2} S_D^{1/2},$$

где

$$S_D = \sum_{a\in A} \left| \sum_{b\in A} \chi_D(a-b) \right|^2 .$$

Таким образом,

$$|A|^{3/2}\sigma \leqslant \sum_{D} S_D^{1/2}. \tag{4.1}$$

Теперь оценим суммы S_D. Зафиксируем множество D. Обозначим для краткости $p_D = \prod_{j\in D} p_j$ и

$$H_D = (mp_D^{-1})^{1/2}(3n)^{1.5(n-|D|)}. \tag{4.2}$$

Далее, для каждого вычета x по модулю p_D положим

$$A_x = \{a \in A : a \equiv x \pmod{p_D}\}.$$

Можно считать, что элементы множества A_x суть вычеты по модулю mp_D^{-1}; при этом разность любых различных элементов A_x есть невычет по этому модулю. Согласно предположению индукции имеем

$$|A_x| \leqslant H_D\,.$$

Заметим, что все элементы A_x дают один и тот же вклад в сумму S_D, поскольку внутренняя сумма в определении S_D не зависит от выбора элемента

$a \in A_x$. Кроме того, $A = \bigsqcup\limits_{x \in \mathbb{Z}_{p_D}} A_x$. Поэтому мы имеем

$$S_D = \sum_{x \in \mathbb{Z}_{p_D}} \sum_{a \in A_x} \left| \sum_{b \in A} \chi_D(x-b) \right|^2 = \sum_{x \in \mathbb{Z}_{p_D}} |A_x| \left| \sum_{b \in A} \chi_D(x-b) \right|^2 \leqslant$$
$$H_D \sum_{b_1, b_2 \in A} \sum_{a \in \mathbb{Z}_{p_D}} \prod_{j \in D} \chi_j(a-b_1)\chi_j(a-b_2) =$$
$$H_D \sum_{b_1, b_2 \in A} \prod_{j \in D} \sum_{a_j \in \mathbb{Z}_{p_j}} \chi_j(a_j-b_1)\chi_j(a_j-b_2).$$

Вычислим внутреннюю сумму. Для краткости введём следующее определение: пару (b_1, b_2) будем называть *особой* по модулю p, если $b_1 \equiv b_2 \pmod p$. Если пара (b_1, b_2) является особой по модулю p_j, то

$$\sum_{a \in \mathbb{Z}_{p_j}} \chi_j(a-b_1)\chi_j(a-b_2) = p_j - 1.$$

В противном случае имеем

$$\sum_{a \in \mathbb{Z}_{p_j}} \chi_j(a-b_1)\chi_j(a-b_2) = \sum_{a \neq b_2} \chi_j\left(1 + \frac{b_2-b_1}{a-b_2}\right) = \sum_{a \neq 1} \chi_j(a) = -1.$$

Обозначим через $B_{D'}$ вклад от пар (b_1, b_2), особых в точности по модулям p_j, $j \in D'$, в сумму

$$\sum_{b_1, b_2 \in A} \prod_{j \in D} \sum_{a_j \in \mathbb{Z}_{p_j}} \chi_j(a_j-b_1)\chi_j(a_j-b_2)$$

(при этом мы не исключаем возможности $D' = \varnothing$, что соответствует вкладу от неособых пар). Тогда

$$S_D \leqslant H_D \sum_{D' \subseteq D} B_{D'}. \tag{4.3}$$

Оценивая число неособых пар тривиально, получим

$$B_\varnothing \leqslant |A|^2. \tag{4.4}$$

Теперь оценим $B_{D'}$ для непустого множества D'. Вклад от каждой пары (b_1, b_2), особой в точности по модулям p_j, $j \in D'$, не больше, чем $p_{D'} = \prod_{j \in D'} p_j$. Количество таких пар не превосходит числа решений сравнения $x \equiv y \pmod{p_{D'}}$, $x, y \in A$, которое, пользуясь предположением индукции, можно оценить сверху величиной $|A| H_{D'}$. Таким образом,

$$B_{D'} \leqslant |A| H_{D'} p_{D'} \tag{4.5}$$

Подставляя полученные оценки (4.4) и (4.5) в неравенство (4.3), мы видим, что для всех D имеет место неравенство

$$S_D \leqslant |A|^2 H_D + |A| H_D \sum_{\varnothing \neq D' \subseteq D} H_{D'} p_{D'}.$$

Отсюда имеем

$$S_D^{1/2} \leqslant |A| H_D^{1/2} + |A|^{1/2} H_D^{1/2} \sum_{D' \subseteq D} H_{D'}^{1/2} p_{D'}^{1/2}.$$

Подставляя это неравенство в (4.1), получаем

$$|A|\sigma \leqslant |A|^{1/2} T_1 + T_2, \tag{4.6}$$

где

$$T_1 = \sum_{d=1}^{n} \sum_{|D|=d} H_D^{1/2},$$

$$T_2 = \sum_{D \subseteq [n]} H_D^{1/2} \sum_{D' \subseteq D} H_{D'}^{1/2} p_{D'}^{1/2}.$$

Остаётся оценить суммы T_1 и T_2. Оценим вначале T_1. Пользуясь выпуклостью функции $u^{-1/4}$ и тем, что $p_1 \geqslant 3$, видим, что

$$\sum_{j=1}^{n} p_j^{-1/4} \leqslant \sum_{j=1}^{n} (2j+1)^{-1/4} \leqslant 0.5 \sum_{j=1}^{n} \int_{2j}^{2j+2} u^{-1/4} du =$$

$$\frac{2}{3}((2n+2)^{3/4} - 2^{3/4}) < \frac{2}{3}(2n)^{3/4} < 1.13 n^{3/4}. \tag{4.7}$$

Вспоминая определение (4.2) величины H_D, находим

$$T_1 \leqslant m^{1/4} \sum_{d=1}^{n} (3n)^{0.75(n-d)} \frac{1}{d!} \left(\sum_{j=1}^{n} p_j^{-1/4} \right)^d \leqslant m^{1/4} \sum_{d=1}^{n} \frac{1.13^d}{d!} (3n)^{0.75(n-d)} n^{0.75d}$$

$$= m^{1/4} (3n)^{0.75n} \sum_{d=1}^{n} 3^{-0.75d} \frac{1.13^d}{d!} \leqslant 0.65 m^{1/4} (3n)^{0.75n}.$$

Теперь оценим сумму T_2. Перепишем её в следующем виде:

$$T_2 = m^{1/2} \sum_{D\subseteq[n]} (3n)^{0.75(n-|D|)} p_D^{-1/4} \sum_{\varnothing\neq D'\subseteq D} (3n)^{0.75(n-|D'|)} p_{D'}^{1/4} =$$
$$m^{1/2}(3n)^{1.5n} \sum_{D\subseteq[n]} (3n)^{-0.75|D|} \sum_{\varnothing\neq D'\subseteq D} (3n)^{-0.75|D'|} (p_{D'}/p_D)^{1/4}$$

$$m^{1/2}(3n)^{1.5n} \sum_{D\subseteq[n]} (3n)^{-0.75|D|} \sum_{D'\subset D} (3n)^{-0.75(|D|-|D'|)} p_{D'}^{-1/4} =$$
$$m^{1/2}(3n)^{1.5n} \sum_{D'\subset[n]} p_{D'}^{-1/4} \sum_{D\supset D'} (3n)^{-1.5(|D|-|D'|/2)}.$$

Оценим внутреннюю сумму. Имеем

$$\sum_{D\supset D'} (3n)^{-1.5(|D|-|D'|/2)} \leqslant \sum_{r=|D'|+1}^{n} n^{r-|D'|} (3n)^{-1.5(r-|D'|/2)} =$$
$$(3n)^{0.75|D'|} n^{-|D'|} \sum_{r=|D'|+1}^{n} 3^{-1.5r} n^{-r/2} \leqslant$$
$$(3n)^{0.75|D'|} n^{-|D'|} 3^{-1.5(|D'|+1)} n^{-(|D'|+1)/2} (1-3^{-1.5}n^{-1/2})^{-1} \leqslant 0.16(3n)^{-0.75|D'|}.$$

Поэтому, используя оценку (4.7), найдём

$$T_2 \leqslant 0.16 m^{1/2}(3n)^{1.5n} \sum_{l=0}^{n-1} (3n)^{-0.75l} \sum_{|D'|=l} p_{D'}^{-1/4} \leqslant$$
$$0.16 m^{1/2}(3n)^{1.5n} \sum_{l=0}^{n-1} 3^{-0.75l} \frac{1.13^l}{l!} \leqslant 0.27(3n)^{1.5n}.$$

Подставляя полученные оценки сумм T_1 и T_2 в (4.6), получим

$$L := |A|^{1/2} \left(|A|^{1/2}\sigma - 0.65 m^{1/4}(3n)^{0.75n} \right) \leqslant 0.27 m^{1/2}(3n)^{1.5n} =: R.$$

Предположим теперь, что

$$|A| > m^{1/2}(3n)^{1.5n}.$$

Но $n \geqslant 2$, и следовательно, $m \geqslant 15$, $|A| \geqslant 6^3\sqrt{15} > 100$ и $\sigma = 1-|A|^{-1} \geqslant 0.99$. Поэтому

$$L > (0.99 - 0.65) m^{1/2}(3n)^{1.5n} > R,$$

противоречие. Тем самым теорема 4.1 доказана. $\square$

4.2 Доказательство следствия 4.3

Для доказательства получим другую оценку на $|A|$, которая убывает по n, а после выясним, когда она будет точнее оценки из теоремы.

Мы будем использовать подход, предложенный М. Матолчи и И. Ружи [42]. Нам понадобится следующий результат Н. Алона.

Лемма 4.5 ([12], Теорема 1.2)**.** *Пусть $(V_1, E_1), \dots, (V_k, E_k)$ — ориентированные графы с максимальными степенями выхода $d_1, \dots, d_k$ соответственно. Предположим, что S — подмножество $V_1 \times \dots \times V_k$ с тем свойством, что для каждой упорядоченной пары $(u_1, \dots, u_k)$ и $(v_1, \dots, v_k)$ элементов S справедливо $(u_i, v_i) \in E_i$ для некоторого i. Тогда*

$$|S| \leqslant \prod_{i=1}^{k} (d_i + 1).$$

Отметим, что в работе [12] рассматривается лишь случай $(V_1, E_1) = \dots = (V_k, E_k)$, однако доказательство немедленно распространяется на случай различных ориентированных графов. Для полноты мы приводим это доказательство.

Доказательство. Можно считать, что V_i —непересекающиеся множества целых чисел. Поставим в соответствие каждому элементу $u = (u_1, \dots, u_k)$ множества S многочлен $P_u \in \mathbb{Q}[x_1, \dots, x_k]$, определяемый равенством

$$P_u(x_1, \dots, x_k) = \prod_{i=1}^{k} \prod_{j \in N(u_i)} (x_i - j),$$

где $N(u_i) = \{v \in V_i : (u_i, v) \in E_i\}$ — множество всех тех вершин i-го графа, в которые есть ребра из вершины u_i.

Так как $u_i \notin N(u_i)$, то мы видим, что $P_u(u_1, \dots, u_k) \neq 0$ для каждого $u = (u_1, \dots, u_k) \in S$. С другой стороны, по предположению имеем $P_u(v) = 0$ при всех $v \in S$, $v \neq u$. Отсюда вытекает, что многочлены $\{P_u : u \in S\}$ линейно независимы (так как если $\sum_{u \in S} c_u P_u(x_1, \dots, x_k) = 0$, то, подставляя $(x_1 \dots, x_k) = (u_1, \dots, u_k)$, получаем $c_u = 0$). Но каждый P_u есть многочлен не выше d_i по переменной x_i; в силу линейной независимости количество этих многочленов не превосходит размерности пространства многочленов от k переменных с этими ограничениями, которая равна $\prod_{i=1}^{k}(d_i + 1)$. Лемма доказана. $\square$

Теперь предположим, что множество $A \subset \mathbb{Z}_m$ таково, что $A - A$ не содержит ненулевых квадратичных вычетов. Рассмотрим ориентированные графы $(\mathbb{Z}_p, E_p)$, $p|m$, где $(x, y) \in E_p$ тогда и только тогда, когда $x - y$ является невычетом по модулю p. Тогда для любых различных $a, b \in A$ найдется $p|m$ такое, что $(a - b) \pmod p \in E_p$. Применяя лемму, получаем, что

$|A| \leqslant \prod_{i=1}^{n}(p_i+1)/2 = m2^{-n}\prod_{i=1}^{n}(1+1/p_i) \leqslant m2^{-cn}$ для некоторого $c>0$. Поэтому из теоремы следует, что

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

откуда вытекает следствие 4.2. $\square$

4.3 Доказательство следствия 4.4

Для натурального $n = p_1^{\alpha_1}\dots p_k^{\alpha_k}$ через $P(n)$ обозначим его мощную часть: $P(n) = \prod_{i:\alpha_i\geqslant 2} p_i^{\alpha_i}$.

Нам понадобится следующее известное утверждение о том, что большинство натуральных чисел имеют малую мощную часть.

Лемма 4.6. *Имеет место оценка*

$$\#\{n \leqslant X : P(n) \geqslant y\} \ll Xy^{-1/2},$$

причём подразумевая постоянная абсолютна.

Доказательство. Заметим, что любое натуральное число, не меньшее двух, представимо в виде $2\alpha+3\beta$, где α,β — целые неотрицательные. Поэтому при простом p и натуральном $k\geqslant 2$ имеем $p^k = p^{2\alpha}p^{3\beta}$ для некоторых целых неотрицательных α,β. Отсюда следует, что мощная часть любого числа $r\in\mathbb{N}$ представима в виде $P(r)=a^2b^3$, где $a,b\in\mathbb{N}$. Поэтому имеем

$$\#\{n\leqslant X : P(n)\geqslant y\} \leqslant \sum_{a^2b^3\geqslant y}\frac{X}{a^2b^3} = X\sum_{a\geqslant 1}a^{-2}\sum_{b\geqslant (ya^{-2})^{1/3}}b^{-3} \ll$$
$$X\left(\sum_{a\leqslant y^{1/2}}a^{-2}(ya^{-2})^{-2/3} + \sum_{a>y^{1/2}}a^{-2}\right) \ll Xy^{-1/2}.$$

Лемма доказана. $\square$

Заметим, что оценка леммы 4.6 точна по порядку: при $y=X/2$ левая часть неравенства оценивается снизу количеством точных квадратов в промежутке $(X/2, X)$, которое по порядку равно $X^{1/2}$.

Далее, сформулируем утверждение о том, что большинство чисел от 1 до X имеют примерно $\log\log X$ простых делителей.

Лемма 4.7. *[[53], упражнение 04]*

1. При $X\geqslant 3$ и $u\leqslant 1$ имеем

$$|\{m\leqslant X : \omega(m)\leqslant u\log\log X\}| \ll X(\log X)^{-u\log u+u-1}.$$

2. При $X\geqslant 3$ и $u\geqslant 1$ имеем

$$|\{m\leqslant X : \omega(m)\geqslant u\log\log X\}| \ll X(\log X)^{-u\log u+u-1}.$$

Теперь мы готовы доказать следствие 4.4. Пусть M — множество тех натуральных $m \geqslant 2$, для которых выполнены условия

(i) $\omega(m) \leqslant 2\log\log m$;

(ii) $P(m) \leqslant \log m$.

Покажем, что множество $\overline{M} = \mathbb{N} \setminus M$ имеет нулевую плотность. Зафиксируем большое число $X > 0$. Тогда если $m \in \overline{M}$ и $X/2 < m \leqslant X$, то либо $P(m) > \log(X/2)$, либо $\omega(m) > 2\log\log(X/2) > 1.9\log\log X$. Согласно леммам 4.6 и 4.7 имеем

$$|\overline{M} \cap (X/2, X]\}| \ll X(\log X)^{-1/2} + X(\log X)^{-c} \ll X(\log X)^{-c},$$

где $c > 0$ — некоторая абсолютная постоянная. Отсюда вытекает, что $|\overline{M} \cap [1, X]| \ll X(\log X)^{-c}$, то есть множество $\overline{M}$ имеет нулевую плотность, и, следовательно, множество M имеет плотность 1.

Пусть теперь $m \in M$; обозначим $m_1 = m/P(m)$ и $n = \omega(m)$, $n_1 = \omega(m_1)$. Предположим, что множество $A \subset \mathbb{Z}_m$ таково, что $A - A$ не содержит ненулевых квадратичных вычетов по модулю m. Зафиксируем произвольный вычет x по модулю $P(m)$ и положим

$$A_x = \{a \in A : a \equiv x \pmod{P(m)}.$$

Пусть A'_x — естественная проекция множества A_x по модулю m_1. Тогда множество $A_x - A_x$ не содержит ненулевых квадратичных вычетов по модулю m_1; используя теорему 4.1 и условие (i), получим

$$|A_x| = |A'_x| \leqslant m_1^{1/2}(3n_1)^{1.5n_1} \leqslant m_1^{1/2}(3n)^{1.5n} = m_1^{1/2}m^{o(1)}, \quad m \in M,\ m \to \infty.$$

Отсюда и из условия (ii)

$$|A| = \sum_{x \in \mathbb{Z}_{P(m)}} |A_x| \leqslant P(m)m_1^{1/2}m^{o(1)} \leqslant m^{1/2+o(1)}, \quad m \in M,\ m \to \infty.$$

Тем самым следствие доказано. $\square$

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.

Литература

[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] Виноградов И. М., Новая оценка функции $\zeta(1+it)$, Изв. АН СССР. Сер. Матем., 22:2, 1958, с.161-164.

[4] Виноградов И. М., Метод тригонометрических сумм в теории чисел, Тр.МИАН СССР, Т.23, Изд-во АН СССР, М.-Л., 1947, 3-109.

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

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

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

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

[9] 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.

[10] 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.

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

[12] Alon N., On the capacity of Digraphs, Europ. J. Combinatorics, 19, 1-5, 1998.

[13] Balog A., Pelikan J., Pintz J., Szemerédi E., Difference sets without kth powers Acta Math. Hungar., 65, 2, 165-187, 1994

[14] Banaszczyk W., "Inequalities for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$ ", Discrete Comput. Geom. 13 (2), 217-231 (1995).

[15] Banks W. D., Conflitti A., Shparlinski I. E., Character sums over integers with restricted g-ary digits // Illinois J. Math. 2002. Vol. 46, №3. P. 819-836.

[16] Banks W. D., Shparlinski I. E. Arithmetic properties of numbers with restricted digits. Acta Arith. 2004. Vol. 112. P. 313-332.

[17] Betke U., Henk M., Wills J. M., "Successive-minima-types inequalities", Discrete Comput. Geom., 9:2 (1993), 165-175.

[18] Blackburn S. R., Konyagin S. V, Shparlinski I. E., Counting additive decompositions of quadratic residues in finite fields 52.2 Functiones et Approximatio 2015 223-227

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

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

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

[22] Col S. Propriétés multiplicatives d'entiers soumis à des contraintes digitales. Thèse de doctorat de mathématiques de l'Université Henri Poincaré-Nancy. 2006. Vol.1.

[23] Col S. Diviseurs des nombres ellipséphiques. Periodica Mathematica Hungarica. 2009. Vol. 58, №1. P. 1-23.

[24] Coquet J. On the uniform distribution modulo one of some subsequences of polynomial sequences. J. Number Theory. 1978. Vol. 10, №3. P. 291-296.

[25] Coquet J. On the uniform distribution modulo one of some subsequences of polynomial sequences. J. Number Theory. 1980. Vol. 12, №2. P. 244-250.

[26] Coquet J. Graphes connexes, représentation de entiers et équirépartition. J. Number Theory. 1983. Vol. 16, №3. P. 363-375.

[27] 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).

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

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

[30] Dartyge C., Mauduit C. Nombres presque premiers dont l'écriture en base r ne comporte pas certain chiffres. Journal of Number Theory. 2000. Vol. 81. P. 270-291.

[31] Dartyge C., Mauduit C. Ensembles de densité nulle contenant des entiers possédant au plus deux facteurs premiers. Journal of Number Theory. 2001. Vol. 91. P. 230-255.

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

[33] 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.

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

[35] Drmota M., Mauduit C. Weyl sums over integers with affine digits restriction. Journal of Number Theory. 2010. Vol. 30. P. 2404-2427.

[36] Erdős P., Mauduit C., Sárközy A. On the arithmetic properties of integers with missing digits I: Distribution in residue classes. Journal of Number Theory. 1998. Vol. 70, №2. P. 99-120.

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

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

[39] Johnsen J., On the distribution of powers in finite fields, 251, J. Reine Angew. Math., 1971, 10–19

[40] Katz N., "An estimate for character sums", JAMS Vol. 2, No 2 1989, 197-200.

[41] Konyagin S. V., Mauduit C., Sárközy A. On the number of prime factors of integers characterized by digits properties. Period. Math. Hung. 2000. Vol. 40. P. 37-52.

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

[43] 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.

[44] 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

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

[46] Schmidt W. M., "Equations over Finite Fields: An Elementary Approach", Lecture Notes in Math. (Springer-Verlag, Berlin, 1976), Vol. 536.

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

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

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

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

[51] Tao T., Vu V., "Additive Combinatorics", Cambridge Stud. Adv. Math., Vol. 105.

[52] Temlyakov V.N., Multivariate Approximation, Cambridge University Press, 2018.

[53] Tenenbaum G., Introduction to analytic and probabilistic number theory, Cambridge studies in advanced mathematics, 46 Cambridge Univ. Press, 1995.

[54] van der Corput J.G., "Vershärfung der Abschätzung beim Teilerproblem", Math. Ann., 87:1-2 (1922), s. 39-65, Satz 2.

[55] Wan D., Generators and irreducible polynomials over finite fields, 66, Math. Comp., 1997, 1195 - 1212.

[56] Winterhof A., Characters sums, primitive elements, and powers in finite fields. Journal of Number Theory. 2001. Vol. 91. P. 153-161.

[57] Weil H., "Über die Gleichverteilung von Zahlen mod Eins", Math. Ann., 77 (1916), s. 313-352.

[58] Weil H., "Zur Abschätzung von $\zeta(1+it)$, Math. Z., 10 (1921), s.88-101.

Работы автора по теме диссертации:

Статьи в научных журналах Web of Science, Scopus

[59] М. Р. Габдуллин, "О подмножествах Zm, разность которых не содержит квадратов", Матем. сб., 209:11 (2018), 60–68; M. R. Gabdullin, "Sets in Zm whose difference sets avoid squares", Sb. Math., 209:11 (2018), 1603–1610

[60] 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

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

[62] 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:

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

[64] Габдуллин М.Р., "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.