МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

Хафез Аль-Ассад

Арифметические вопросы многочленов в полях алгебраических чисел

Специальность 1.1.5. — математическая логика, алгебра, теория чисел и дискретная математика.

ДИССЕРТАЦИЯ

на соискание ученой степени
кандидата физико-математических наук

Научный руководитель:
доктор физико-математических наук,
профессор
Владимир Николаевич Чубариков

Москва — 2024

Оглавление

Введение

Актуальность тем исследования и степень их разработанности

Диссертация посвящена аналитической и алгебраической теории чисел.

Первая тема, которую мы рассмотрим, — это представления двух рациональных целых чисел в виде сумм трех рациональных квадратов, имеющих общий квадрат. Представления целых рациональных чисел в виде многочленов всегда представляли интерес для математики. Многие известные теоремы и результаты, такие как теорема Лежандра о трех квадратах ([8], стр. 47), теоремы Лагранжа [29] и Якоби [30] о четырех квадратах, проблема Гильберта-Гамке ([1], стр. 297.) и многие другие, посвящены этому вопросу. В частности, теорема Лежандра о трех квадратах полностью решает задачу представления рационального целого числа в виде суммы трех рациональных квадратов. Для представления целого числа однородным многочленом второй степени локально-глобальный принцип Хассе ([8], стр. 41) сводит проблему к представимости по модулю всех степеней простых чисел и представимости в действительных числах. В 1980 году Д.Л. Коллио-Телен и Д. Корэ [13] обобщили принцип Хассе на два однородных многочлена при определенных условиях. Наше исследование направлено на обобщение вышеупомянутой теоремы Лежандра, и использует это обобщение.

Вторая тема, которую мы рассматриваем — это оценки тригонометрических сумм в полях алгебраических чисел. Тригонометрические суммы уже давно представляют интерес из-за их глубокой связи с модулярной арифметикой в кольце вычетов по модулю q. В частности, они возникают в методе круга Харди-Литтлвуда-Рамануджана в форме тригонометрических сумм И.М. Виноградова [6] для оценки числа решений диофантовых уравнений. В частности, рассматривается разрешимость данного уравнения, во-первых, в действительных числах, а во-вторых, по модулю любого рационального целого q. Последняя часть обычно бывает более глубокой

и трудной, и существенную роль в ней играют рациональные тригонометрические суммы; они эффективно отвечают за разрешимость по модулю q. В 1940 г. Хуа Ло-кен [17] нашел нетривиальную оценку тригонометрических сумм в поле рациональных чисел. Последующие работы Чэнь Джун-руна [21,22] и В.И. Нечаева [23] улучшали оценку. В 1984 г. Ци Мингао и Дин Пин [24] нашли константу в оценке Хуа Ло-кена. В 1949 г. Хуа Ло-кен [15] обобщил свою оценку на случай тригонометрических сумм в полях алгебраических чисел. Первая часть нашего исследования по этой теме направлена на усиление этой оценки. Вторая часть нашего исследования по этой теме направлена на обобщение метода деревьев Хуа Ло-кена [16,20] для построения решений полиномиальных сравнений по модулю рационального простого числа, используемого в решении проблемы сходимости особого ряда в проблеме Пруэ-Терри-Эскота ([1], стр. 26), на случай полей алгебраических чисел.

Третья тема, которую мы рассматриваем, — это представления характеров Дирихле. Характеры Дирихле, впервые введенные П.Л. Дирихле в 1837 г., играют центральную роль в мультипликативной теории чисел. Первоначально они использовались им для доказательства теоремы о простых числах в арифметических прогрессиях ([5], стр. 50). Многие важные вопросы аналитической теорией чисел были разработаны на основе характеров Дирихле, и теории L-функций Дирихле. В современной теории L-функций, большое значение имеют оценки сумм характеров. Формула А.Г. Постникова [26], доказанная им в 1955 г., выражает характеры Дирихле по модулю степени нечетного простого числа через экспоненты от многочленов с рациональными коэффициентами. Таким образом задача об оценке сумм таких характеров Дирихле сводится к методу тригонометрических сумм И.М. Виноградова [6]. Наше исследование по этой теме связано с обобщением формулы А.Г. Постникова на случай характера Дирихле по модулю степени 2 и применением как оригинальной, так и обобщенной формулы А.Г. Постникова для оценки сумм характеров в полях алгебраических чисел.

Цели и задачи диссертационной работы

Целью диссертации является исследование арифметических вопросов тригонометрических сумм в полях алгебраических чисел, в частности:

- Обобщить теорему Лежандра о трех квадратах на случай представления пар целых чисел суммами трех квадратов с общим квадратом.
- Усилить оценки Хуа Ло-кена для тригонометрических сумм в полях алгебраических чисел.

- Обобщить метод деревьев Хуа Ло-кена на поля алгебраических чисел и использовать его для оценки тригонометрических сумм в них.
- Обобщить формулу А.Г. Постникова на случай степеней числа 2 и использовать ее для оценки сумм характеров в полях алгебраических чисел.

Научная новизна

Результаты, полученные в диссертации, являются новыми. Среди них:

- Теорема Лежандра о трёх квадратах обобщается на пары целых рациональных чисел, с точностью до кратных целых рациональных квадратов.
- Метод деревьев Хуа Ло-кена обобщен на поля алгебраических чисел.
- Оценки Хуа Ло-кена в полях алгебраических чисел улучшены в случае степеней простых идеалов, а также для общих неразветвленных идеалов, когда число классов равно 1.
- Формула А.Г. Постникова для характеров обобщена на случай степени числа 2.

Теоретическая и практическая значимость

Работа имеет теоретический характер и может быть использована в различных задачах теории чисел.

Методология и методы исследования

В исследовании используются классические и современные понятия, методы и достижения алгебраической и аналитической теории чисел и алгебраической геометрии.

Положения, выносимые на защиту

На защиту представлены следующие результаты диссертации:

- Характеризуются, с точностью до кратных квадратов целых рациональных чисел, пары целых рациональных чисел, которые можно представить в виде суммы трех квадратов с общим квадратом.
- Усиление оценки Хуа Ло-кена для тригонометрических сумм в полях алгебраических чисел в ряде случаев.
- Обобщение метода деревьев Хуа Ло-кена на поля алгебраических чисел и получение соответствующих оценок тригонометрических сумм.
- Обобщение формулы А.Г. Постникова на случай степени числа 2.
- Применение формулы А.Г. Постникова для оценки некоторых сумм характеров в полях алгебраических чисел.

Степень достоверности и апробация результатов

Достоверность результатов диссертационного исследования гарантируется следующими фактами. Все результаты диссертации имеют законченный характер и снабжены строгими математическими доказательствами. Все результаты диссертации являются новыми, а результаты других авторов, упомянутые в диссертации, отмечены соответствующими ссылками. Результаты диссертации являются достоверными и прошли апробацию на научных семинарах и конференциях. Основные результаты диссертации опубликованы в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 1.1.5. — математическая логика, алгебра, теория чисел и дискретная математика.

В частности, результаты и положения диссертации неоднократно докладывались и обсуждались на научно-исследовательском семинаре на кафедре математических и компьютерных методов анализа механико-математического факультета МГУ и на международной конференции «Математика в созвездии наук» (МГУ, Москва, 1-2 апреля 2024 года).

Публикации

Материалы диссертации опубликованы в 4 печатных работах в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ, индексируемых в базе данных Scopus.

Личный вклад автора

Основные положения диссертации, выносимые на защиту, отражают персональный вклад автора в опубликованные работы. Основные результаты, представленные в диссертации, получены лично автором.

Структура и объем диссертации

Диссертация состоит из введения, трех независимых глав, разбитых на параграфы, заключения, списка литературы и списка публикаций автора. Общий объем работы составляет 98 страниц. Список литературы включает 34 наименования.

В **первой главе** обобщается теорема Лежандра о трех квадратах на представления двух целых чисел вместо одного. На основе обобщения Д.Л. Коллио-Телена и Д. Корэ [13] локально-глобального принципа Хассе, частично характеризуются пары целых чисел так, что каждое из них представимо в виде суммы трех квадратов так, что представления имеют общий квадрат. В частности, теорема сначала доказана для систем по модулю любой степени любого простого числа. Используя ее тривиальность в действительных числах, теорема затем доказана для систем в рациональных числах, откуда она следует для систем в целых числах с использованием теоремы Давенпорта-Касселса [8]. Основным результатом данной главы является теорема 1.2.

Во **второй главе** усилится оценка Хуа Ло-кена [15] в полях алгебраических чисел в случае степеней простых идеалов, а также для общих неразветвленных идеалов, когда число классов равно 1, опираясь на оригинальный метод, разработанный Хуа Ло-кеном.

Кроме того, автор продолжает работу В.Н. Чубарикова [2] в обобщении метода деревьев Хуа Ло-кена [16,20] на поля алгебраических чисел, и использует это обобщение для получения соответствующих оценок тригонометрических сумм.

В **третьей главе** обобщается формула А.Г. Постникова [26] на случай степеней числа 2. Автор применяет это обобщение наряду с оригинальной работой А.Г. Постникова для оценки некоторых сумм характеров в полях алгебраических чисел. Эта часть также содержит простое доказательство части недавнего результата М. Элиа, Д.С. Интерландо и Р. Розенбаума [27,28] касающегося мультипликативной структуры систем приведенных вычетов по модулю степени простого идеала.

В **заключении** перечислены основные результаты работы, и указаны возможные направления дальнейших исследований.

Глава 1

Обобщение теоремы Лежандра о трёх квадратах[1]

1.1 Постановка задачи

Основной результат данной главы, теорема 1.2, приведенная ниже. С помощью компьютерных вычислений, выполненных Али Дибом (dib_a@spbstu.ru, Высшая школа управления киберфизическими системами, Институт компьютерных наук и кибербезопасности,
Санкт-Петербургский политехнический университет Петра Великого (СПбПУ)), эта гипотеза о разрешимости системы диофантовых уравнений подтвердилась.

Проблема представления целого положительного числа в виде суммы трёх целых квадратов решается следующей теоремой Лежандра ([8], стр. 47).

Теорема 1.1. ***(Лежандр)*** *Пусть m — целое положительное число. Уравнение*

$$m = x^2 + y^2 + z^2$$

имеет решение в $x, y, z \in \mathbb{Z}$ если и только если m удовлетворяет условию

$$m \neq 4^a(8b + 7);\ a, b \in \mathbb{Z},\ a, b \geq 0.$$

Обобщим этот классический результат, рассматривая представления двух натуральных чи-

[1]При подготовке данной главы диссертации использовались следующие публикации автора, в которых, согласно «Положению о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова», отражены основные результаты, положения и выводы исследования: [31].

сел в виде сумм трех квадратов с общим квадратом, т.е. рассматриваем решения системы уравнений

$$\begin{cases} m = a^2 + b_1^2 + c_1^2, \\ m' = a^2 + b_2^2 + c_2^2 \end{cases} \tag{1.1}$$

в целых числах a, b_1, b_2, c_1, c_2.

Определение 1.1. *Целое число, представимое в виде суммы трёх квадратов, называем Лежандровым.*

Определение 1.2. *Две пары целых чисел (m_1, m_1') и (m_2, m_2') называем сравнимыми по модулю целого числа n, если справедливо либо*

$$m_1 \equiv m_2 \mod n, \ \ m_1' \equiv m_2' \mod n,$$

либо

$$m_1 \equiv m_2' \mod n, \ \ m_1' \equiv m_2 \mod n.$$

Основной результат данной главы - следующая теорема.

Теорема 1.2. *Пусть $m, m' \in \mathbb{Z}$ — пара Лежандровых положительных целых чисел.*

Система уравнений

$$\begin{cases} q^2 m = a^2 + b_1^2 + c_1^2, \\ q^2 m' = a^2 + b_2^2 + c_2^2 \end{cases} \tag{1.2}$$

имеет решение в положительных q, a, b_1, b_2, c_1, c_2 тогда и только тогда, когда пара (m, m') не сравнима с $(0, 3)$ или $(3, 4)$ по модулю 8 и не сравнима ни с одной из

$$(0, 3 \cdot 2^{k-3}),$$

$$(0, 3 \cdot 2^{k-2}),$$

$$(0, 7 \cdot 2^{k-3}),$$

$$(2^{k-3}, 3 \cdot 2^{k-2}),$$

$$(5 \cdot 2^{k-3}, 3 \cdot 2^{k-2})$$

по модулю 2^k*, для любого четного целого* $k \geq 4$.

Более того, существует решение системы (1.2) такое, что q *нечетно и взаимно просто с* a.

План доказательства следующий.

Рассматриваем систему (1.1) в рациональных числах a, b_1, b_2, c_1, c_2.

Сначала покажем, что для любой пары (m, m'), система (1.1) имеет ненулевое решение в кольце $\mathbb{Z}/p\mathbb{Z}$ для любого простого числа p.

Потом покажем, что для любой пары (m, m'), система (1.1) имеет ненулевое решение в кольце $\mathbb{Z}/p^k\mathbb{Z}$ для любого нечетного простого числа p и любого целого числа $k > 1$.

Затем покажем, что если $v_2(\text{НОД}(m, m')) \leq 1$, то система (1.1) имеет ненулевое решение в кольце $\mathbb{Z}/2^k\mathbb{Z}$ для любого целого числа $k > 1$ тогда и только тогда, тогда пара (m, m') удовлетворяет условиям теоремы 1.2.

Из этого получим условия нетривиальной разрешимости системы (1.1) в $p-$адических полях $\mathbb{Q}_p$ при $v_2(\text{НОД}(m, m')) \leq 1$, и, поскольку разрешимость в $\mathbb{R}$ очевидна, то используя форму локально-глобального принципа Хассе ([13], стр. 22, теорема 3.2), переходим к решениям системы (1.1) в $\mathbb{Q}$, при условии, что $v_2(\text{НОД}(m, m')) \leq 1$.

После этого, используем теорему Давенпорта-Касселса ([8], стр. 46) для перехода от решений системы (1.1) к решениям системы (1.2), при условии, что $v_2(\text{НОД}(m, m')) \leq 1$.

Наконец, воспользуемся леммой для перехода от решений системы (1.2) в случае, когда $v_2(\text{НОД}(m, m')) \leq 1$ к решениям системы (1.2) в общем случае.

1.2 Задача по модулю простого числа

Пусть p — некоторое простое число. Рассматриваем систему сравнений

$$\begin{cases} t^2 + x^2 + y^2 \equiv m \mod p, \\ t^2 + z^2 + w^2 \equiv m' \mod p, \end{cases} \tag{1.3}$$

в $t, x, y, z, w \in \mathbb{Z}/p\mathbb{Z}$.

Покажем, что (1.3) разрешимо для всех m, m'.

Разрешимость (1.3) в случае $p = 2$ тривиальна, а 0 нетривиально представляется как $0 \equiv 1 + 1 \mod 2$. Дальше предположим, что $p > 2$.

Лемма 1.1. *Если $m \not\equiv 0 \mod p$, то сравнение*

$$x^2 + y^2 \equiv m \mod p \tag{1.4}$$

разрешимо.

Доказательство. Если m — квадратичный вычет по модулю p, то можно взять $y = 0$. Предположим, что m — квадратичный невычет.

Пусть $Q_1 = \{q_i\}_{i=1}^{\frac{p-1}{2}}$ — множество квадратичных вычетов по модулю p.

Покажем, что множество $Q_2 = \{q_i + 1\}_{i=1}^{\frac{p-1}{2}}$ содержит хотя бы один квадратичный невычет.

Действительно, если Q_2 не содержит квадратичных невычетов, то $Q_2 = Q_1$, и можем рассматривать элементы Q_2 как перестановку элементов Q_1.

Рассмотрим цикл в перестановке, который содержит элемент q_1:

$$q_{i+1} \equiv q_i + 1 \mod p,\ 1 \le i \le k-1,\ q_1 \equiv q_k + 1 \mod p,$$

для некоторого $1 \le k \le \frac{p-1}{2}$.

Однако это дает, что

$$q_1 \equiv q_k + 1 \equiv q_{k-1} + 2 \equiv \cdots \equiv q_1 + k \mod p \implies k \equiv 0 \mod p,$$

что является противоречием.

Следовательно, множество Q_2 содержит некоторый квадратичный невычет r, скажем с

$$r = q + 1 = \tilde{r}^2 + 1, \tag{1.5}$$

для некоторого $\tilde{r}$.

Пусть g — первообразный корень по модулю p. Поскольку m и r — квадратичные невычеты, можем написать

$$m \equiv g^{2a+1},\ r \equiv g^{2b+1}, \tag{1.6}$$

для некоторых $0 \le a, b \le \frac{p-3}{2}$.

Из (1.5) и (1.6) видим, что (1.4) разрешимо

$$m \equiv rg^{2(a-b)} \equiv \tilde{r}^2 g^{2(a-b)} + g^{2(a-b)} \equiv x^2 + y^2.$$

□

Теперь докажем основной результат данного раздела.

Теорема 1.3. *Система (1.3) разрешима для всех m, m'.*

Доказательство. Если $m, m' \not\equiv 0 \mod p$, то берем $t = 0$, и теорема следует из леммы 1.1.

Если, скажем, $m' \equiv 0$, то берем $t \neq 0$ такой, что $t^2 \not\equiv m$, и теорема опять следует из леммы 1.1. □

1.3 Задача по модулю степени нечетного простого числа

Пусть p — нечетное простое число, а $k \geq 2$ — целое число. Рассматриваем систему сравнений

$$\begin{cases} t^2 + x^2 + y^2 \equiv m \mod p^k, \\ t^2 + z^2 + w^2 \equiv m' \mod p^k, \end{cases} \tag{1.7}$$

в $t, x, y, z, w \in \mathbb{Z}/p^k\mathbb{Z}$.

Покажем, что (1.7) разрешима для всех m, m'.

Теорема 1.4. *Система (1.7) разрешима для всех m, m'.*

Доказательство. Будем действовать индукцией по k. Случай $k = 1$ доказанно в теореме 1.3.

Предположим сначала, что $m, m' \not\equiv 0 \mod p$. Доказательство теоремы 1.3 показало, что в этом случае при $k = 1$ система (1.7) разрешима при $t = 0$, и по индукции предполагаем, что это верно по модулю p^{k-1}, так что

$$x^2 + y^2 \equiv m \mod p^{k-1} \implies x^2 + y^2 \equiv m + rp^{k-1} \mod p^k;\ 0 \leq r \leq p-1, \tag{1.8}$$

где, поскольку $m \not\equiv 0 \mod p$, то можем считать, что $x \not\equiv 0 \mod p$.

Следовательно, пусть $\tilde{r}$ — единственное решение сравнения

$$2x\tilde{r} \equiv -r \mod p.$$

Тогда согласно (1.8) имеем

$$(x+\tilde{r}p^{k-1})^2+y^2\equiv x^2+y^2+2x\tilde{r}p^{k-1}\equiv m \mod p^k,$$

что завершает индукцию в этом случае и показывает, как и при доказательстве теоремы 1.3, что система (1.7) разрешима с $t=0$, если $m,m'\not\equiv 0 \mod p$.

Предположим теперь, что $m\not\equiv 0 \mod p, m'\equiv 0 \mod p$. Выбираем любой $t\not\equiv 0 \mod p$ такой, что $t^2\not\equiv m \mod p$, и рассматриваем эквивалентную систему сравнений

$$\begin{cases} x^2+y^2\equiv m-t^2 \mod p^k, \\ z^2+w^2\equiv m'-t^2 \mod p^k, \end{cases} \tag{1.9}$$

в x,y,z,w.

По определению t знаем, что

$$m'-t^2\not\equiv 0 \mod p,\ m-t^2\not\equiv 0 \mod p$$

и, таким образом, решение (1.9) сводится к предыдущему случаю.

Наконец, доказательство случая $m,m'\equiv 0 \mod p$ полностью аналогично доказательству предыдущего случая, надо только выбирать любое $t\not\equiv 0 \mod p$. □

1.4 Задача по модулю степени 2

Пусть $k\geq 1$ — целое число. Рассматриваем систему сравнений

$$\begin{cases} t^2+x^2+y^2\equiv m \mod 2^k, \\ t^2+z^2+w^2\equiv m' \mod 2^k, \end{cases} \tag{1.10}$$

в $t,x,y,z,w\in\mathbb{Z}/2^k\mathbb{Z}$.

В этом разделе предположим, что m,m' — Лежандровые целые числа, и что $v_2(\text{НОД}(m,m'))\leq 1$.

Случай $k=1$ тривиален (он был рассмотрен в начале раздела 2), и нетрудно видеть, что при $k=2$ система (1.10) разрешима для всех (m,m'), не сравнимых с $(0,3)$ по модулю 4.

В дальнейшем обозначаем через m_0 и m_1 соответствующие приведения m и m' по модулю 2^{k-1} и рассматриваем приведение (1.10) по модулю 2^{k-1}:

$$\begin{cases} t^2 + x^2 + y^2 \equiv m_0 \mod 2^{k-1}, \\ t^2 + z^2 + w^2 \equiv m_1 \mod 2^{k-1}, \end{cases} \tag{1.11}$$

Если (1.11) имеет решение, то можем записать (1.10) в виде

$$\begin{cases} t^2 + x^2 + y^2 \equiv m_0 + r2^{k-1} \mod 2^k, \\ t^2 + z^2 + w^2 \equiv m_1 + s2^{k-1} \mod 2^k, \end{cases} \tag{1.12}$$

где $r, s \in \{0, 1\}$.

Всего существует четыре возможных пары (r, s), и основная идея, лежащая в основе данного раздела, заключается в том, что решение (1.11) дает решение (1.12) ровно для одной пары (r, s), и мы будем использовать это решение (1.12) для перехода к остальным решениям (1.12) для трех остальных пар (r, s).

При необходимости, сделав замену переменных

$$m_0 \to m_0 + 2^{k-1}, \;\; m_1 \to m_1 + 2^{k-1},$$

можно считать, что данное решение всегда имеет $r = s = 0$.

Для любой компоненты решения (1.11) u с

$$v_2(u) < \frac{k-3}{2}, \tag{1.13}$$

замена переменных

$$u' = u + 2^{k-v_2(u)-2}$$

дает

$$u'^2 \equiv u^2 + 2^{k-1} \mod 2^k.$$

Кроме того, если

$$k \text{ нечетно}, \; v_2(u) > \frac{k-3}{2}, \tag{1.14}$$

тогда замена переменных

$$u' = u + 2^{\frac{k-1}{2}}$$

дает

$$u'^2 \equiv u^2 + 2^{k-1} \mod 2^k.$$

Определение 1.3. *Компоненты решения (1.11), удовлетворяющие (1.13) или (1.14), называем поднимаемыми.*

Определение 1.4. *Решение (1.12) называем применимым, если хотя бы одна из t, x, y и одна из t, z, w поднимаемы, а если t поднимаемый, то существует еще один поднимаемый компонент, кроме t.*

Определение 1.5. *Определим для поднимаемого вычета и функцию*

$$\psi(u) = \begin{cases} k - v_2(u) - 2, & \text{если } u \text{ удовлетворяет (1.13)}, \\ \frac{k-1}{2}, & \text{если } u \text{ удовлетворяет (1.14)}. \end{cases}$$

Предложение 1.1. *Если существует применимое решение (1.12) для $r = s = 0$, то существует решение (1.12) для любой пары $(r, s) \in J$.*

Доказательство. Пусть ϵ_0, ϵ_1 означают либо 0, либо 1.

Если $u_0, u_1 \in \{t, x, y, z, w\}$ — разные поднимаемые компоненты данного решения (1.12), то фиксируем остальные компоненты, и тогда замены переменных

$$u_0' = u_0 + \epsilon_0 2^{\psi(u_0)}, u_1' = u_1 + \epsilon_1 2^{\psi(u_1)}, \tag{1.15}$$

при всех возможных значениях $\epsilon_0, \epsilon_1 \in \{0, 1\}$, дают решения (1.12) для остальных пар $(r, s) \in J$. □

Лемма 1.2. *Если m, m' нечетны, то (1.10) разрешимо.*

Доказательство. Индуктивно покажем, что существует решение (1.10) с нечетными x и z и, следовательно, поднимаемыми.

При $k = 3$ это можно проверить вычислительно.

Предположим, что это справедливо для $k - 1$, так что (1.11), а значит, и (1.12), имеют решение с нечетными x и z.

Замена переменных в (1.15) при $u_0 = x, u_1 = z$ дает решения (1.12) для остальных пар $(r, s) \in J$, а u'_0, u'_1 остаются нечетными при всех значений ϵ_0, ϵ_1. □

Предложение 1.2. *Пусть $k \geq 3$. Нечетный вычет $u \in \mathbb{Z}/2^k\mathbb{Z}$ является квадратичным вычетом тогда и только тогда, когда $u \equiv 1 \mod 8$.*

Доказательство. Обратное утверждение очевидное из того факта, что 1 — единственный нечетный квадратичный вычет по модулю 8.

Для прямого утверждения, знаем, что u выражается однозначно как

$$u \equiv (-1)^{\frac{u-1}{2}} 5^{h(u)};\ 0 \leq h(u) < 2^{k-2}.$$

Следовательно, несложно увидеть, что u является квадратичным вычетом тогда и только тогда, когда $\frac{u-1}{2}$ и $h(u)$ четны, что дает ровно $2^{k-3} = \frac{2^k}{8}$ квадратичных вычетов, и с учетом обратной импликации отсюда следует, что любой $u \equiv 1 \mod 8$ является квадратичным вычетом. □

Предложение 1.3. *Если существует решение (1.12) при $r = s = 0$ с хотя бы одним из x, y, z, w нечётным, то существует решение (1.12) для любой пары $(r, s) \in J$.*

Доказательство. Без ограничения общности предположим, что x нечетно. Фиксируя s, это позволяет перейти к решению (1.12) при $r = 1$, применив замену переменных в (1.15) с $u_0 = z$, без u_1.

Следовательно, нам достаточно найти решения уравнения (1.12) для $s = 1$, поскольку можем перейти между решениям для $r = 0$ и $r = 1$, сохраняя при этом s фиксированным, как было только что показано.

Если одно из t, z, w поднимаемо, то имеем применимое решение, и предложение следует из предложения 1.1.

Предположим, что ни один из t, z, w не является поднимаемым. Рассматриваем два случая.

Случай 1. k четно:

Тогда $t^2, z^2, w^2 \in \{0, 2^{k-2}\}$ и, следовательно, $m_1 \in \{0, 2^{k-2}, 2^{k-1}, 3 \cdot 2^{k-2}\}$, что дает

$$m_1 + 2^{k-1} \in \{0, 2^{k-2}, 2^{k-1}, 3 \cdot 2^{k-2}\}.$$

Следовательно, всегда можем взять $t^2 = 0$ или $t^2 = 2^{k-2}$ в представлении $m_1 + 2^{k-1}$, и, таким образом, решение (1.12) для $s = 1$ всегда можно найти либо взяв $z' = z$, если $t^2 = 0$, либо

$$z'^2 \equiv z^2 - 2^{k-2} \mod 2^k$$

если $t^2 = 2^{k-2}$, что возможно по предложению 1.2, поскольку имеем $z^2 - 2^{k-2} \equiv z^2 \equiv 1 \mod 8$, так как $k \geq 5$ и z нечетно.

Случай 2. k нечетно:

Тогда $t^2 = z^2 = w^2 = 2^{k-3}$, и поэтому $m_1 = 3 \cdot 2^{k-3}$, что дает $m_1 + 2^{k-1} \equiv 7 \cdot 2^{k-1}$.

Поскольку k нечетно, видим, что $m_1 + 2^{k-1}$ не является Лежандровым, и поэтому $s = 1$ не может быть. □

Сформулируем и докажем основной результат данного раздела.

Теорема 1.5. *Пусть m, m' — Лежандровые целые числа, и что $v_2(НОД(m, m')) \leq 1$.*

Тогда система (1.10) разрешима если и только если (m, m') не сравнима с $(0, 3)$ или $(3, 4)$ по модулю 8, и не сравнима ни с одной из $(0, 6), (0, 14), (2, 12), (10, 12)$ по модулю 16.

Доказательство. При $k = 3, 4$ это можно проверить непосредственным вычислением.

Предположим, что $k \geq 5$.

Докажем теорему по индукции. Предположим, что (1.10) разрешимо для $k-1$, так что нам дано решение (1.14), которое, не ограничивая общности, можно считать с $r = s = 0$.

Если данное решение поднимаемое, то теорема следует из предложения 1.1.

Предположим, что данное решение не является поднимаемым. Если один из x, y, z, w был нечетным, то теорема следует из предложения 1.3.

Если все x, y, z, w четные, а t нечетно, то m и m' оба нечетны, и теорема следует из леммы 1.2.

Если бы все t, x, y, z, w были четными, то имели бы $v_2(\text{НОД}(m, m')) \geq 2$, что противоречит условиям теоремы. □

1.5 Доказательство основного результата

Доказательство теоремы 1.2 займет весь данный раздел.

Сначала докажем третье утверждение теоремы 1.2. Допустим, что нам дано решение системы (1.2) такое, что q четно. Тогда $q^2 \equiv 0 \mod 4$, а рассмотрение (1.2) по модулю 4 показывает, что a, b_1, b_2, c_1, c_2 обязательно четны, поэтому мы можем разделить все члены обоих уравнений

в (1.2) на 4. Повторяя этот процесс, мы приходим к тому, что при наличии решения системы (1.2), можно предположить нечетность числа q. Это доказывает третье утверждение теоремы 1.2.

Рассмотрим систему двух диагональных квадратичных форм с целыми коэффициентами

$$\begin{cases} mu^2 - t^2 - x^2 - y^2 = 0, \\ m'u^2 - t^2 - z^2 - w^2 = 0. \end{cases} \tag{1.16}$$

Если m и m' оба рациональные квадраты, то (1.16) имеет нетривиальное решение

$$u = 1, x = \sqrt{m}, z = \sqrt{m'}, t = y = w = 0,$$

и поэтому в дальнейшем мы предполагаем, что хотя бы один из m и m' не является рациональным квадратом.

В разделах 2,3,4 мы рассматривали разрешимость системы (1.16) в кольцах $\mathbb{Z}/p^k\mathbb{Z}$ для всех простых p и целых чисел $k \geq 1$, при условии, что $v_2(\text{НОД}(m, m')) \leq 1$.

При переходе к $p-$адическим полям $\mathbb{Q}_p$ воспользуемся следующей простой леммой ([8], стр. 14, предложение 6).

Лемма 1.3. *Пусть $f_i \in \mathbb{Z}_p[X_1, \ldots, X_h]$ — однородные многочлены с целыми $p-$адическими коэффициентами, и пусть $f_{i,k} \in (\mathbb{Z}/p^k\mathbb{Z})[X_1, \ldots, X_h]$ обозначают их вычеты по модулю p^k. Тогда f_i имеют общий нетривиальный нуль в $(\mathbb{Q}_p)^h$ тогда и только тогда, когда $f_{i,k}$ имеют общий примитивный нуль в $(\mathbb{Z}/p^k\mathbb{Z})^h$ для всех $k > 1$.*

Чтобы убедиться, что лемма 1.3 применима к нашему случаю, рассмотрим систему (1.16) по модулю p^k.

Если p — нечетное простое число, то теорема 1.4 показала, что система (1.16) имеет нетривиальное решение в $\mathbb{Z}/p^k\mathbb{Z}$ для всех пар (m, m'), и существует такое решение содержащее примитивный элемент из $\mathbb{Z}/p^k\mathbb{Z}$.

Если $p = 2$, то из предположения, что $v_2(\text{НОД}(m, m')) \leq 1$, следует, что хотя бы одно из m и m' не сравнимо с 0 по модулю 2^k при $k > 1$, а теорема 1.5 показывает, что (1.16) разрешимо в $\mathbb{Z}/2^k\mathbb{Z}$ для всех таких пар (m, m'), не сравнимых с исключениями из теоремы 1.2 (или, что то же самое, исключениями из самой теоремы 1.5). Такие пары (m, m') обладают тем свойством, что хотя бы одно из m и m' предполагается ненулевым в $\mathbb{Z}/2^k\mathbb{Z}$, мы всегда можем взять $u = 1$ при решении (1.16) в $\mathbb{Z}/2^k\mathbb{Z}$, и это, очевидно, дает примитивное решение.

Таким образом, мы показали, что для пар, не сравнимых с исключениями из теоремы 1.2, система (1.16) имеет нетривиальные решения во всех $p-$адических полях $\mathbb{Q}_p$, при условии, что $v_2(\text{НОД}(m, m')) \leq 1$.

Система (1.16), очевидно, нетривиально разрешима в $\mathbb{R}$.

Теперь нам нужен механизм перехода от решений во всех пополнениях $\mathbb{Q}$, а именно, $p-$адических полях $\mathbb{Q}_p$ и $\mathbb{R}$, к решениям в самом $\mathbb{Q}$.

Для этого воспользуемся следующим результатом Д.Л. Коллио-Телена, Д. Корэ и Д.Д. Сансука ([13], стр. 22, теорема 3.2).

Теорема 1.6. *Пусть $\mathbb{K}$ — числовое поле и ϕ, ϕ_1, ϕ_2 — невырожденные бинарные квадратичные формы с коэффициентами из $\mathbb{K}$.*

Рассмотрим трехмерное $\mathbb{K}-$многообразие V в проективном пространстве $\mathbb{P}^5_{\mathbb{K}}$, заданное пересечением двух квадратных уравнений

$$\phi(u_1, v_1) = \phi_1(x, y),\ \phi(u_2, v_2) = \phi_2(x, y).$$

Предположим, что ϕ_1 или ϕ_2 анизотропны. Тогда если V имеет $\mathbb{K}_p$-ую точку для каждого пополнения $\mathbb{K}_p$ поля $\mathbb{K}$, то V имеет $\mathbb{K}$-ую точку.

Взяв $\mathbb{K} = \mathbb{Q}$ и

$$\phi(u, v) = u^2 + v^2,\ \phi_1(x, y) = mx^2 - y^2,\ \phi_2(x, y) = m'x^2 - y^2,$$

мы видим, поскольку в начале данного раздела предполагалось, что хотя бы один из m и m' не является рациональным квадратом, то один из ϕ_1 и ϕ_2 анизотропен.

Следовательно, теорема 1.6 применима, и мы видим, что (1.16) имеет нетривиальное рациональное решение, при $v_2(\text{НОД}(m, m')) \leq 1$.

Если $u = 0$ в рациональном решении (1.16) в $\mathbb{Q}$, то $t = x = y = z = w = 0$, что является тривиальным решением, и поэтому существует решение системы (1.16) в $\mathbb{Q}$ с $u \neq 0$. Взяв такое решение и умножив (1.16) на u^{-2}, получим

$$m = \frac{a^2}{q^2} + \frac{a_1^2}{q_1^2} + \frac{a_2^2}{q_2^2},\ \ m' = \frac{a^2}{q^2} + \frac{a_3^2}{q_3^2} + \frac{a_4^2}{q_4^2},$$

где $a, q, a_i, q_i \in \mathbb{Z}$, при этом можно предположить, что $\text{НОД}(a, q) = 1$, и это все можно записать как

$$q^2m - a^2 = \frac{q^2a_1^2}{q_1^2} + \frac{q^2a_2^2}{q_2^2},\ \ q^2m' - a^2 = \frac{q^2a_3^2}{q_3^2} + \frac{q^2a_4^2}{q_4^2}.$$

Следовательно, целые числа $q^2m - a^2$ и $q^2m' - a^2$ представляются в виде суммы двух рациональных квадратов.

Чтобы показать, что $q^2m - a^2$ и $q^2m' - a^2$ представляются в виде суммы двух целых квадратов, нам нужно одно следствие теоремы Давенпорта-Касселса ([8], стр. 46), которую мы сейчас сформулируем.

Теорема 1.7. ***(Давенпорт-Касселс)*** *Пусть f — положительно определенная квадратичная форма от h переменных с целыми коэффициентами.*

Предположим, что для любого $(y_1, \ldots, y_h) \in \mathbb{Q}^h$ существует $(x_1, \ldots, x_h) \in \mathbb{Z}^h$ такое, что

$$f(\vec{x} - \vec{y}) < 1.$$

Тогда любое целое число, представимое формой f в $\mathbb{Q}$, также представимое формой f в $\mathbb{Z}$.

Лемма 1.4. *Если целое число представляется в виде суммы двух рациональных квадратов, то оно представляется в виде суммы двух целых квадратов.*

Лемма непосредственно следует из применения теоремы Давенпорта-Касселса с

$$f(\vec{v}) = v_1^2 + v_2^2,\ \ x_i = ||y_i||,$$

где $||y_i||$ обозначает ближайшее целое число к y_i.

Таким образом, применяя лемму мы видим, что $q^2m - a^2$ и $q^2m' - a^2$ оба представляются как сумма двух целых квадратов, что дает (1.2):

$$q^2m - a^2 = b_1^2 + c_1^2,\ \ q^2m' - a^2 = b_2^2 + c_2^2.$$

Это доказывает первое утверждение теоремы 1.2, при условии, что $v_2(\text{НОД}(m, m')) \leq 1$, и, более того, поскольку $\text{НОД}(a, q) = 1$, это также доказывает второе утверждение теоремы 1.2, при условии, что $v_2(\text{НОД}(m, m')) \leq 1$.

Тем самым завершается доказательство теоремы 1.2 при условии, что $v_2(\text{НОД}(m, m')) \leq 1$.

Для доказательства первого утверждения теоремы 1.2 в общем случае, воспользуемся следующей леммой.

Лемма 1.5. *Пусть $m, m' \in \mathbb{Z}$ такие, что $4|НОД(m, m')$. Тогда (1.2) разрешимо для (m, m') тогда и только тогда, когда оно разрешимо для $(\frac{m}{4}, \frac{m'}{4})$.*

Доказательство. Предположим, что дано решение (1.2) для (m, m'). Тогда рассмотрение обоих уравнений (1.2) по модулю 4 показывает, что a, b_1, b_2, c_1, c_2 четные, и поэтому можем разделить все члены обоих уравнений в (1.2) на 4, и получим

$$q^2\Big(\frac{m}{4}\Big) = \Big(\frac{a}{2}\Big)^2 + \Big(\frac{b_1}{2}\Big)^2 + \Big(\frac{c_1}{2}\Big)^2,$$
$$q^2\Big(\frac{m'}{4}\Big) = \Big(\frac{a}{2}\Big)^2 + \Big(\frac{b_2}{2}\Big)^2 + \Big(\frac{c_2}{2}\Big)^2,$$

что является решением (1.2) для $(\frac{m}{4}, \frac{m'}{4})$.

Наоборот, если дано решение (1.2) для $(\frac{m}{4}, \frac{m'}{4})$, то умножение всех слагаемых на 4 дает

$$q^2 m = (2a)^2 + (2b_1)^2 + (2c_1)^2,$$
$$q^2 m' = (2a)^2 + (2b_2)^2 + (2c_2)^2,$$

что является решением уравнения (1.2) для (m, m'). □

Из утверждения теоремы 1.2 легко видеть, что исключения для любого четного $k \geq 6$ являются образцами исключений $k - 2$ при умножении на 4. При $k = 4$ все исключения из теоремы 1.2 входят в теорему 1.5. Следовательно, лемма 1.5 показывает, что доказательство первого утверждения теоремы 1.2 при условии, что $v_2(\text{НОД}(m, m')) \leq 1$, эквивалентно общему случаю.

Для второго утверждения теоремы 1.2, по лемме 1.5 можно предположить, что дано решение (1.2) для $(\frac{m}{4}, \frac{m'}{4})$ с $\text{НОД}(a, q) = 1$, и по третьему утверждению теоремы 1.2, доказанному в общем случае в начале данного раздела, можно считать, что q нечетно. Доказательство леммы 1.5 показало, что соответствующее решение (1.2) для (m, m') есть $(q, 2a, 2b_1, 2b_2, 2c_1, 2c_2)$, и очевидно, что $\text{НОД}(q, 2a) = \text{НОД}(q, a) = 1$.

Таким образом, завершено доказательство теоремы 1.2 в общем случае.

Глава 2

Об оценках Хуа Ло-кена тригонометрических сумм в полях алгебраических чисел[2]

2.1 Постановка задачи

Рациональные тригонометрические суммы многочленов представляют собой суммы вида

$$S(f,q) = \sum_{x \mod q} e^{2\pi i \frac{f(x)}{q}},$$

где $q \geq 1$ — рациональное целое число, и

$$f(x) = \alpha_m x^m + \cdots + \alpha_1 x$$

многочлен с целыми коэффициентами, такой что $(\alpha_m, \ldots, \alpha_1, q) = 1$.

Эти суммы давно представляют интерес из-за их глубокой связи с модулярной арифметикой в кольце вычетов по модулю q.

В частности, они возникают в методе круга Харди-Литтлвуда-Рамануджана в форме тригонометрических сумм Виноградова для оценки числа решений диофантовых уравнений. Рас-

[2]При подготовке данной главы диссертации использовались следующие публикации автора, в которых, согласно «Положению о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова», отражены основные результаты, положения и выводы исследования: [32].

сматривается разрешимость данного уравнения в действительных числах и в соответствующих сравнениях по модулю любого рационального целого q. Последняя часть обычно бывает более глубокой и трудной, и существенную роль в ней играют рациональные тригонометрические суммы; они эффективно отвечают за разрешимость по модулю q.

В 1940 г. Хуа Ло-кен [17] нашел оценку

$$S(f,q) = O_{m,\epsilon}\big(q^{1-\frac{1}{m}+\epsilon}\big),$$

где $\epsilon > 0$ произвольное. Последующие работы Чэнь Джун-руна [21],[22] и В. И. Нечаева [23] убрали ϵ из оценки. В 1984 г. Ци Мингао и Дин Пин [24] получили оценку

$$|S(f,q)| \le e^{2m} q^{1-\frac{1}{m}}.$$

В 1949 г. Хуа Ло-кен [15] обобщил этот результат на случай поля алгебраических чисел степени d, получив оценку

$$S(f,Q) = \sum_{x \mod Q} e^{2\pi i T(f(x))} = O_{m,\epsilon,d}\big(N(Q)^{1-\frac{1}{m}+\epsilon}\big),$$

где T и N обозначают след и норму соответственно, Q — целый идеал, а идеал $A(f) = (\alpha_m, \ldots, \alpha_1)$ удовлетворяет $A(f) = \frac{B\delta^{-1}}{Q}$, где δ — дифферента, а B — целый идеал с $(B,Q) = 1$.

В данной главе мы получим более сильный результат в случае $Q = P^n$, где P — простой идеал, в виде

$$|S(f,P^n)| \le C_d(m) N(P)^{n(1-\frac{1}{m})},$$

где $C_d(m)$ — константа, зависящая только от d и m.

Кроме того, мы будем использовать наш усиленный результат, чтобы убрать ϵ и вычислить константу в символе O, когда данное числовое поле имеет число классов, равное 1 (т.е. кольцо целых является кольцом главных идеалов), а идеал $A(f)$ удовлетворяет условию $A(f) = \frac{B}{Q}$, для некоторых целых идеалов B и Q, где Q такой, что $(Q,\delta) = 1$.

В частности, для таких идеалов мы получаем

$$|S(f,Q)| \le e^{\frac{5}{2}d^2(2d+1)} e^{3.442md} N(Q)^{1-\frac{1}{m}}.$$

В другом направлении Хуа Ло-кен в [16] (см. также [20]) использовал метод деревьев для

построения решений полиномиальных сравнений по модулю рационального простого числа, что позволило ему решить проблему сходимости особого ряда в проблеме Пруэ-Терри-Эскота. Для этого он рассмотрел элемент x по модулю p^n, где p — рациональное простое число, в виде

$$x = x_1 + x_2 p + \cdots + x_s p^s,$$

где $0 \leq x_j < p$ для $1 \leq j \leq s$, и использовал это представление для построения решений полиномиальных сравнений по модулю p^n.

Это позволило ему получить новую оценку вида

$$|S(f, p^n)| \leq m p^{n-h},$$

где h — положительное целое число, зависящее от делимости коэффициентов f на p.

В данной главе мы обобщим этот метод на кольцо целых поля алгебраических чисел и впоследствии получим аналогичную оценку

$$|S(f, P^n)| \leq (m-1) N(P)^{n-h}.$$

Наконец, мы объединим наши оценки, чтобы получить новую оценку в теореме 2.6.

Данная глава расширяет работу В.Н. Чубарикова в [2], опираясь преимущественно на идеи Хуа Ло-кена в [15], Г.И. Архипова, А.А. Карацубы и В.Н. Чубарикова в [1], и Ван Юаня в [18].

2.2 Полиномиальные сравнения по модулю простого идеала

В этом разделе мы приводим результаты о числе решений полиномиальных сравнений по модулю простого идеала, аналогичные подобным результатам в случае сравнений по рациональному простому модулю.

Лемма 2.1. *([18], стр. 15). Пусть $A = (\alpha_m, \ldots, \alpha_0)$ — целый идеал $\mathbb{K}$, и пусть P — простой идеал такой, что $P \nmid A$.*

Тогда число решений сравнения

$$f(x) = \alpha_m x^m + \cdots + \alpha_1 x + \alpha_0 \equiv 0 \mod P,$$

учитывая их кратность, не превосходит m.

Доказательство. В этом доказательстве под корнем многочлена понимается корень данного многочлена по модулю P.

Докажем лемму индукцией по m.

Базовый случай $m = 1$ выполняется из-за условия $P \nmid A$ и поскольку P — простой идеал. Предположим, что лемма справедлива для $m - 1$.

Предположим, что f имеет h несравнимых корней $r_1, \ldots, r_h$, так что

$$r_{j_1} \not\equiv r_{j_2} \mod P, \forall j_1 \neq j_2.$$

Предположим, что r_j имеет кратность λ_j, и что $\sum_{j=1}^{h} \lambda_j > m$.

Без ограничения общности будем считать, что корень r_1 имеет минимальную кратность $\lambda_1 \geq 1$. Рассмотрим многочлен

$$f(x) - f(r_1) = \alpha_m(x^m - r_1^m) + \cdots + \alpha_1(x - r_1) = (x - r_1)g(x),$$

где g – многочлен степени $m - 1$ со старшим коэффициентом α_m.

Поскольку для всех $2 \leq j \leq h$ имеем

$$f(r_j) \equiv f(r_1) \equiv 0 \mod P,\ r_j \not\equiv r_1 \mod P,$$

тогда, поскольку P простой идеал, отсюда следует, что

$$g(r_j) \equiv 0 \mod P.$$

Сначала мы покажем, что r_1 является корнем g с кратностью $\lambda_1 - 1$, причем некорень считается имеющим кратность 0.

Действительно, из определения g имеем

$$f^{(k)}(x) = (x - r_1)g^{(k)}(x) + (k - 1)g^{(k-1)}(x).$$

Если $\lambda_1 = 1$, то r_1 не является корнем f' и, следовательно, не является корнем g. В противном случае мы увидим, что для всех $k \leq \lambda_1$, r_1 является корнем $f^{(k)}$ и, следовательно, является корнем $g^{(k-1)}$. Для $k = \lambda_1 + 1$ мы знаем, что r_1 не является корнем $f^{(\lambda_1+1)}$ и поэтому не может быть корнем $g^{(\lambda_1)}$.

Таким образом, мы показали, что r_1 является корнем g кратности $\lambda_1 - 1$. Аналогичное

рассуждение показывает, что r_j является корнем g кратности λ_j для $2 \leq j \leq h$.

Отсюда следует, что корни $r_1, \ldots, r_h$ группы g имеют общую кратность

$$\Big(\sum_{j=1}^{h} \lambda_j\Big) - 1 > m - 1,$$

но поскольку $\deg(g) = m - 1$, то это противоречит предположению индукции. □

В качестве простого, но полезного следствия из предыдущей леммы получаем следующее предложение.

Предложение 2.1. *([18], стр. 15). Пусть $A = (\alpha_m, \ldots, \alpha_1)$ — дробный идеал такой, что $A\delta = \frac{R}{P^n}$, где R — целый идеал, P — простой идеал такой, что $(R, P) = 1$ и $n \geq 1$ — рациональное целое число. Пусть*

$$f(x) = \alpha_m x^m + \cdots + \alpha_1 x.$$

Тогда число решений сравнения

$$f(x) \equiv 0 \mod P^{-n+1},$$

учитывая их кратность, не превосходит m.

Лемма 2.2. *([18], стр. 15). Пусть P — простой идеал, а f — многочлен с целыми коэффициентами. Пусть a — корень кратности λ сравнения $f(x) \equiv 0 \mod P$.*

Пусть $\pi \in R$ — целое, которое делится на P, но не делится на P^2, и пусть v — наибольшее рациональное целое число такое, что

$$P^u | f(\pi x + a) - f(a).$$

Пусть

$$g(x) = \pi^{-u}\big(f(\pi x + a) - f(a)\big).$$

Тогда $u \leq \lambda$, и число решений сравнения

$$g(x) \equiv 0 \mod P,$$

учитывая их кратность, не превосходит λ.

Доказательство. Сначала мы покажем, что, поскольку a является корнем кратности λ сравнения $f(x) \equiv 0 \mod P$, то мы можем записать f как

$$f(x) = (x-a)^{\lambda} h(x) + \pi_1 r(x), \tag{2.1}$$

для некоторого $\pi_1 \in P$, такого, что $P \nmid h(a)$ и $\deg(r) < \lambda$.

Действительно, по формуле Тейлора имеем

$$f(x) = \sum_{j=0}^{m} \frac{f^{(j)}(a)}{j!}(x-a)^j = (x-a)^{\lambda} h(x) + r_1(x), \tag{2.2}$$

где

$$h(x) = \sum_{j=\lambda}^{m} \frac{f^{(j)}(a)}{j!}(x-a)^{j-\lambda},\ r_1(x) = \sum_{j=0}^{\lambda-1} \frac{f^{(j)}(a)}{j!}(x-a)^j,\ \deg(r_1) < \lambda.$$

Легко видеть, что $P \nmid h(a)$, поскольку

$$h(a) = \frac{f^{(\lambda)}(a)}{\lambda!} \not\equiv 0 \mod P.$$

Более того, поскольку a имеет кратность λ, мы знаем, что существует h_1 такой, что

$$f(x) \equiv (x-a)^{\lambda} h_1(x) \mod P. \tag{2.3}$$

Сравнивая (2.2) и (2.3) по модулю P, получаем

$$(x-a)^{\lambda} h(x) + r_1(x) \equiv (x-a)^{\lambda} h_1(x) \mod P,$$

что, поскольку $\deg(r_1) < \lambda$, означает, что $r_1(x) \equiv 0 \mod P$, и поэтому r_1 можно записать как $r_1 = \pi_1 \cdot r$ для $\pi_1 \in P$, где $\deg(r) < \lambda$, что и это доказывает (2.1).

Следовательно, имеем

$$\pi^{-u}\big(f(\pi x + a) - f(a)\big) = \pi^{-u}\Big((\pi x)^{\lambda} h(\pi x + a) + \pi_1\big(r(\pi x + a) - r(a)\big)\Big) =$$
$$= \pi^{\lambda - u} x^{\lambda} h(\pi x + a) + (\pi_1 \pi^{-u})\big(r(\pi x + a) - r(a)\big).$$

Отсюда ясно, что $v \leq \lambda$, что и доказывает первое утверждение леммы. Более того, это

показывает, что $\deg(h) \leq \lambda$, и поэтому второе утверждение леммы следует из применения леммы 2.1 к h. □

2.3 Свойства ортогональности и мультипликативности тригонометрических сумм

В этом разделе мы приводим результаты, касающиеся свойств ортогональности и мультипликативности тригонометрических сумм, аналогичные подобным результатам в рациональном случае. Последнее позволит нам ограничить наше внимание тригонометрическими суммами над идеалами, равными степени простого идеала.

Лемма 2.3. *([18], стр. 16). Пусть Q — целый идеал, а $\alpha \in R$ — целое число. Пусть η пробегает полную систему вычетов $(Q\delta)^{-1}$ по модулю δ^{-1}. Тогда*

$$\sum_{\eta} E(\alpha\eta) = \sum_{\eta} e^{2\pi i T(\alpha\eta)} = \begin{cases} N(Q) & \text{если } Q|\alpha, \\ 0 & \text{если } Q \nmid \alpha. \end{cases}$$

Доказательство. Если $Q|\alpha$, то $\alpha\eta \in \delta^{-1}$, что дает $E(\alpha\eta) = 1$, и тогда

$$\sum_{\eta} E(\eta\alpha) = N(Q).$$

Предположим, что $Q \nmid \alpha$. Сначала мы покажем, что существует некоторый $\eta \in (Q\delta)^{-1}$, скажем η_0, такой, что $\eta\alpha \notin \delta^{-1}$.

Если $\eta\alpha \in \delta^{-1}$ для всех $\eta \in (Q\delta)^{-1}$, то $\delta^{-1}|\alpha(Q\delta)^{-1}$, и поэтому $Q|\alpha$, что является противоречием.

По определению δ^{-1} существует целое число γ такое, что $E(\gamma\eta_0\alpha) \neq 1$. Поскольку $\gamma\eta_0 \in (Q\delta)^{-1}$, имеем

$$\sum_{\eta} E(\eta\alpha) = \sum_{\eta} E(\gamma\eta_0\alpha + \eta\alpha) = E(\gamma\eta_0\alpha) \sum_{\eta} E(\eta\alpha),$$

которые, поскольку $E(\gamma\eta_0\alpha) \neq 1$, дает

$$\sum_{\eta} E(\eta\alpha) = 0.$$

□

Лемма 2.4. *([18], стр. 16). Пусть* $A = (\alpha_m, \dots, \alpha_1), Q, Q_1, Q_2, B$ *— целые идеалы такие, что*

$$Q = Q_1 Q_2,\ (Q_1, Q_2) = 1,\ A = \frac{B\delta^{-1}}{Q},\ (B, Q) = 1,$$

и пусть

$$f(x) = \alpha_m x^m + \cdots + \alpha_1 x.$$

Тогда существуют многочлены

$$f_j(x) = \alpha_{m,j} x^m + \cdots + \alpha_{1,j} x,$$

для $j = 1, 2$*, с идеалами* $A_j = (\alpha_{j,m}, \cdots, \alpha_{j,1})$*, такими, что существуют целые идеалы* B_1, B_2 *с*

$$A_1 = \frac{B_1\delta^{-1}}{Q_1}, A_2 = \frac{B_2\delta^{-1}}{Q_2}, (B_1, Q_1) = (B_2, Q_2) = 1,$$

и так, что

$$S(f, Q) = S(f_1, Q_1) S(f_2, Q_2).$$

Доказательство. Поскольку $(Q_1, Q_2) = 1$, то существуют целые числа k_1, k_2 такие, что

$$(k_1, Q) = Q_1, (k_2, Q) = Q_2.$$

Полагая $k = \lambda_1 k_1 + \lambda_2 k_2$, мы видим по китайской теореме об остатках, что при пробегании λ_1, λ_2 по полным системам вычетов по модулю Q_1, Q_2 соответственно, k пробегает полную систему вычетов по модулю Q.

Следовательно, имеем

$$S(f, Q) = \sum_{k \bmod Q} E(f(k)) = \sum_{\lambda_1 \bmod Q_1} \sum_{\lambda_2 \bmod Q_2} E(f(\lambda_1 k_1 + \lambda_2 k_2)) =$$

$$= \sum_{\lambda_1 \bmod Q_1} E(f(\lambda_1 k_1)) \sum_{\lambda_2 \bmod Q_2} E(f(\lambda_2 k_2)) = S(f_1, Q_1) S(f_2, Q_2),$$

где $f_j(k) = f(k k_j)$. Утверждение об идеалах B_1 и B_2 очевидно. □

2.4 Метод деревьев Хуа Ло-кена для тригонометрических сумм по идеалам, равным степени простого идеала

В этом разделе мы представляем обобщение метода деревьев Хуа Ло-кена, на основе [2], и получаем соответствующую оценку тригонометрических сумм по идеалам, равным степени простого идеала. Мы также представим результаты по тригонометрическим суммам, которые будут использоваться в последующих разделах.

Благодаря теореме о единственности разложения идеалов в полях алгебраических чисел, лемма 2.4 позволяет нам ограничить наши рассмотрения идеалами, равными степени простого идеала, поскольку любой целый идеал может быть однозначно выражен как произведение таких идеалов.

Таким образом, в остальной части главы, пусть $A(f) = (\alpha_m, \ldots, \alpha_1)$ — дробный идеал такой, что

$$A = \frac{B\delta^{-1}}{P^n};\ (B, P) = 1 \tag{2.4}$$

где B — целый идеал, P — простой идеал, и $n \geq 1$ — рациональное целое число.

Более того, π всегда обозначает элемент R такой, что $\pi \in P, \pi \notin P^2$ (см., например, [4], стр. 441).

Пусть

$$f(x) = \alpha_m x^m + \cdots + \alpha_1 x.$$

Будем рассматривать полные тригонометрические суммы

$$S(f, P^n) = \sum_{x \bmod P^n} E(f(x)).$$

Пусть t — наибольшее рациональное целое число такое, что $P^t | A(f')A(f)^{-1}$. Поскольку $A(f)|A(f')$, имеем $t \geq 0$.

Очевидно, что каждый $x \mod P^n$ однозначно выражается как $x = y + \pi^{n-t-1}z$ для $y \mod P^{n-t-1}, z \mod P^{t+1}$, и поэтому имеем

$$S(f, P^n) = \sum_{y \bmod P^{n-t-1}} \sum_{z \bmod P^{t+1}} E(f(y + \pi^{n-t-1}z)) = \sum_{v \bmod P} S_v, \tag{2.5}$$

где

$$S_v = \sum_{\substack{y \bmod P^{n-t-1} \\ y \equiv v \mod P}} \sum_{z \bmod P^{t+1}} e^{2\pi i T(f(y+\pi^{n-t-1}z))}.$$

Лемма 2.5. *([2], стр. 9). Если $l \geq 2(t+1)$, и v не является решением сравнения $\pi^{n-t} f'(v) \equiv 0 \mod P$, то*

$$S_v = 0.$$

Доказательство. Используя формулу Тейлора, получаем

$$f(y + \pi^{n-t-1}z) = \sum_{j=0}^{m} \frac{f^{(j)}(y)}{j!} (\pi^{n-t-1}z)^s \equiv f(y) + \pi^{n-t-1} z f'(y) \mod P^{n-t},$$

что, поскольку $n \geq 2(t+1)$, дает

$$S_v = \sum_{\substack{y \bmod P^{n-t-1} \\ y \equiv v \mod P}} \sum_{z \bmod P^{t+1}} e^{2\pi i T(f(y)+\pi^{n-t-1} z f'(y))} =$$

$$= \sum_{\substack{y \bmod P^{n-t-1} \\ y \equiv v \mod P}} e^{2\pi i T(f(y))} \sum_{z \bmod P^{t+1}} e^{2\pi i T(\pi^{n-t} f'(v) \pi^{-1} z)}.$$

Применение леммы 2.3 к внутренней сумме дает

$$\sum_{z \bmod P^{t+1}} e^{2\pi i T(\pi^{n-t} f'(v)\pi^{-1} z)} = 0 \implies S_v = 0.$$

□

Для каждого решения v сравнения $\pi^{n-t} f'(v) \equiv 0 \mod P$ положим

$$\tilde{f}_1(y) = f(y+v) - f(v) = \sum_{j=1}^{m} \tilde{\alpha}_{j,1} y^j.$$

Тогда имеем тождества

$$\tilde{\alpha}_{j,1} = \sum_{l=0}^{m-j} \alpha_{j+l} \binom{j+l}{j} v^l;\ 1 \leq j \leq m. \tag{2.6}$$

Определим теперь

$$f_1(y) = \tilde{f}_1(\pi y) = \sum_{j=1}^{m} \pi^j \tilde{\alpha}_{j,1} y^j = \sum_{j=1}^{m} \alpha_{j,1} y^j, \tag{2.7}$$

и определим индекс $u = u(v)$ как наибольшее рациональное целое число такое, что $P^u | A(f_1)A(f)^{-1}$.

Из (2.4) и (2.6) ясно, что $A(f)|A(f_1)$, и поэтому $u \geq 0$. Более того, из (2.7) и определения u следует, что

$$A(f_1) = \frac{B_1 \delta^{-1}}{P^{n-u}};\ (B_1, P) = 1$$

для какого-то целого идеала B_1.

Лемма 2.6. *([2], стр. 9). Если $l \geq 2(t+1)$, тогда*

$$S(f, P^n) = \sum_{v}{}' N(P^{u-1}) E(f(v)) S(f_1, P^{n-u}),$$

где штрих означает, что суммирование ведется по решениям сравнения $\pi^{n-t} f'(v) \equiv 0 \mod P$ в полной системе вычетов по модулю P.

Доказательство. Если v является решением сравнения $\pi^{n-t} f'(v) \equiv 0 \mod P$, тогда

$$S_v = \sum_{\substack{y \bmod P^{n-t-1} \\ y \equiv v \bmod P}} \sum_{z \bmod P^{t+1}} E(f(y + \pi^{n-t-1} z)) =$$

$$= \sum_{\substack{y \bmod P^{n-t-1} \\ y \equiv v \bmod P}} E(f(y)) \sum_{z \bmod P^{t+1}} E(f(y + \pi^{n-t-1} z) - f(y)) =$$

$$= \sum_{\substack{y \bmod P^{n-t-1} \\ y \equiv v \bmod P}} E(f(y)) \sum_{z \bmod P^{t+1}} E(\pi^{n-t-1} f'(y) z) =$$

$$= N(P^{t+1}) \sum_{\substack{y \bmod P^{n-t-1} \\ y \equiv v \bmod P}} E(f(y)) = N(P^{t+1}) E(f(v)) \sum_{y \bmod P^{n-t-2}} E(f(\pi y + v) - f(v)) =$$

$$= N(P^{t+1}) E(f(v)) \sum_{y \bmod P^{n-t-2}} E(f_1(y)) = N(P^{u-1}) E(f(v)) S(f_1, P^{n-u}).$$

Если v не является решением сравнения $\pi^{n-t}f'(v) \equiv 0 \mod P$, то лемма 2.5 дает $S_v = 0$, и тогда утверждение леммы следует от (2.5). $\square$

Определим w как наибольшее рациональное целое число такое, что $P^w | k$ для некоторого $1 \le k \le m$. В лемме 2.10 мы покажем, что

$$w = (e+1)\left\lfloor \frac{\ln m}{\ln q} \right\rfloor .$$

Следующая конструкция является обобщением метода Хуа Ло-кена.

Полагая $f_0 = f$ и $u_1(v_0) = u(v)$, мы индуктивно определяем функции f_k и индексы $u_k = u_k(v_{k-1})$ аналогично построению f_1 и $u(v)$ перед леммой 2.6.

Предположим, что для $k \ge 1$

$$f_{k-1}(y) = \alpha_{m,k-1}y^m + \cdots + \alpha_{1,k-1}y;\ A(f_{k-1}) = \frac{B_{k-1}\delta^{-1}}{P^{n-u_1-\cdots-u_{k-1}}} \tag{2.8}$$

уже определена, где B_{k-1} — целый идеал такой, что $(B_{k-1}, P) = 1$, и пусть t_{k-1} — наибольшее рациональное целое число такое, что $P^{t_{k-1}} | A(f'_{k-1})A(f_{k-1})^{-1}$.

Поскольку $A(f_{k-1}) | A(f'_{k-1})$, имеем $t_{k-1} \ge 0$.

Для каждого решения v_{k-1} сравнения

$$\pi^{n-u_1-\cdots-u_{k-1}-t_{k-1}} f'_{k-1}(x) \equiv 0 \mod P,$$

положим

$$\tilde{f}_k(y) = f_{k-1}(y + v_{k-1}) - f_{k-1}(v_{k-1}) = \sum_{j=1}^{m} \tilde{\alpha}_{j,k} y^j.$$

Тогда имеем тождества

$$\tilde{\alpha}_{j,k} = \sum_{l=0}^{m-j} \alpha_{j+l,k-1} \binom{j+l}{j} v_{k-1}^l. \tag{2.9}$$

Определим теперь

$$f_k(y) = \tilde{f}_k(\pi y) = \sum_{j=1}^{m} \pi^j \tilde{\alpha}_{j,k} y^j = \sum_{j=1}^{m} \alpha_{j,k} y^j, \tag{2.10}$$

и определим индекс $u_k = u_k(v_{k-1})$ как наибольшее рациональное целое число такое, что $P^{u_k} | A(f_k)A(f_{k-1})^{-1}$.

Из (2.8) и (2.9) следует, что $A(f_{k-1})|A(f_k)$, и поэтому $u_k \geq 0$. Более того, из определения u_k следует, что

$$A(f_k) = \frac{B_k \delta^{-1}}{P^{n-u_1-\cdots-u_k}}. \tag{2.11}$$

Для удобства положим

$$U_k = \sum_{j=1}^{k} u_k,\ l_k = l - U_k,\ l_0 = l.$$

Повторяем эту конструкцию до шага с номером h, который определяется условиями

$$l - U_{h-1} \geq 2(w+1),\ l - U_h < 2(w+1).$$

Предложение 2.2. *Для $1 \leq k \leq h-1$, имеем неравенство*

$$t_k \leq w.$$

Доказательство. По построению мы знаем, что

$$A(f_k) = \frac{B_k \delta^{-1}}{P^{n_k}},$$

для некоторого целого идеала B_k с $(B_k, P) = 1$, и поэтому $V_P(A(f_k)) = -l_k - e$.

По определению w мы видим, что

$$V_P(A(f_k')) \leq w + V_P(A(f_k)) = w - l_k - e \implies w \geq l_k + V_P(A(f_k')) = t_k.$$

□

Теорема 2.1. *Если $h > 0$, то*

$$S(f, P^n) = \sum_{v_0,\ldots,v_{h-1}}{}' N(P^{U_h - h}) E(f_0(v_0) + \cdots + f_{h-1}(v_{h-1})) S(f_h, P^{n-U_h}).$$

где штрих означает, что суммирование ведется по решениям сравнений $\pi^{n_k - t_k} f_k'(v_k) \equiv 0 \mod P$, для $0 \leq k \leq h-1$, в полной системе вычетов по модулю P.

Доказательство. Докажем утверждение теоремы повторным применением леммы 2.6.

Поскольку $h > 0$, имеем $l \geq 2(w+1)$, и поэтому для $1 \leq k \leq h-1$ имеем $w \geq t_k$ по предложению 2.2, что по определение h показывает, что $l_k \geq 2(t_k+1)$.

Следовательно, индуктивно, для $1 \leq k \leq h-1$ предположим, что имеем

$$S(f, P^n) = \sum_{v_0,\ldots,v_{k-1}}{}' N(P^{U_k-k})E(f_0(v_0)+\cdots+f_{k-1}(v_{k-1}))S(f_k, P^{n-U_k}).$$

Поскольку $l_k \geq 2(t_k+1)$, то можем применить лемму 2.6 и получить

$$S(f_k, P^{n-U_k}) = \sum_{v_k}{}' N(P^{u_{k+1}-1})E(f_k(v_k))S(f_{k+1}, P^{n-U_{k+1}}).$$

□

Лемма 2.7. *Количество наборов индексов* $\{u_1, \ldots, u_h\}$ *не превосходит* $m-1$.

Доказательство. Пусть $\{v_{0,j_0}\}_{j_0=1}^{J_0}$ — множество несравнимых решений сравнения $\pi^{n-t}f_0'(x) \equiv 0 \mod P$, где v_{0,j_0} имеет кратность λ_{0,j_0}. По предложению 2.1 мы знаем, что

$$\sum_{j_0=1}^{J_0} \lambda_{0,j_0} \leq m-1.$$

Теперь для каждого v_{0,j_0} пусть, $\{v_{1,j_0,j_1}\}_{j_1=1}^{J_1(j_0)}$ — множество несравнимых решений сравнения $\pi^{n_1-t_1}f_1'(x) \equiv 0 \mod P$, где v_{1,j_0,j_1} имеет кратность λ_{1,j_0,j_1}.

Индуктивно предположим, что

$$\sum_{j_0=1}^{J_0} \cdots \sum_{j_{k-1}=1}^{J_{k-1}(j_0,\ldots,j_{k-2})} \lambda_{k-1,j_0,\ldots,j_{k-1}} \leq m-1. \tag{2.12}$$

По лемме 2.2 мы знаем, что

$$\sum_{j_k=1}^{J_k(j_0,\ldots,j_{k-1})} \lambda_{k,j_0,\ldots,j_k} \leq \lambda_{k-1,j_0,\ldots,j_{k-1}}. \tag{2.13}$$

Следовательно, по (2.12) и (2.13) имеем

$$\sum_{j_0=1}^{J_0} \cdots \sum_{j_k=1}^{J_k(j_0,\ldots,j_{k-1})} \lambda_{k,j_0,\ldots,j_k} \leq \sum_{j_0=1}^{J_0} \cdots \sum_{j_{k-1}=1}^{J_{k-1}(j_0,\ldots,j_{k-2})} \lambda_{k-1,j_0,\ldots,j_{k-1}} \leq m-1.$$

По индукции мы видим, что

$$\sum_{j_0=1}^{J_0}\sum_{j_1=1}^{J_1(j_0)}\cdots\sum_{j_{h-1}=1}^{J_{h-1}(j_0,\ldots,j_{h-2})}\lambda_{h-1,j_0,\ldots,j_{h-1}}\leq m-1,$$

а поскольку $\lambda_{h-1,j_0,\ldots,j_{h-1}}\geq 1$, количество множеств $\{v_{0,j_0},\ldots,v_{h-1,j_0,\ldots,j_{h-1}}\}=\{v_0,\ldots,v_{h-1}\}$ не превосходит $m-1$, что эквивалентно утверждению леммы, по определению u_k. □

Предложение 2.3. *Имеем*

$$\{j;V_P(\pi^{n_{k-1}+e}\tilde{\alpha}_{j,k})=0\}\neq\emptyset,\ \ \{j;V_P(\pi^{n_k+e}\alpha_{j,k})=0\}\neq\emptyset.$$

Доказательство. Имеем

$$\alpha_{j,k}\in A(f_k)\implies A(f_k)|\alpha_{j,k}\implies V_P(\alpha_{j,k})\geq V_P(A(f_k))=-l_k-e. \tag{2.14}$$

Поскольку $V_P(A(f_{k-1}))=-l_{k-1}-e$, то не может быть, что $V_P(\alpha_{j,k-1})>-l_{k-1}-e$ для всех $1\leq j\leq m$.

Поэтому, по (2.14) (для $k-1$), можем положить $s'=\max\{j;V_P(\alpha_{j,k-1})=-l_{k-1}-e\}$, и тогда (2.9) дает

$$V_P(\tilde{\alpha}_{s',k})=V_P(\alpha_{s',k-1})=-l_{k-1}-e\implies V_P(\pi^{n_{k-1}+e}\tilde{\alpha}_{s',k})=0,$$

что показывает, что первое множество в утверждении теоремы непусто.

Аналогично, поскольку $V_P(A(f_k))=-l_k-e$, то не может быть, что $V_P(\alpha_{j,k})>-l_k-e$ для всех $1\leq j\leq m$.

Применяя (2.14), видим, что мы можем положить $r'=\max\{j;V_P(\alpha_{j,k})=-l_k-e\}$, и тогда

$$V_P(\pi^{n_k+e}\alpha_{r,k})=0,$$

что показывает, что второе множество в утверждении теоремы непусто. □

Лемма 2.8. *Имеем цепочку неравенств*

$$m\geq u_1\geq\cdots\geq u_h\geq 2.$$

Доказательство. Сначала мы докажем, что $m \geq u_k \geq u_{k+1}$ для $1 \leq k \leq h-1$.

По предложению 2.3, пусть

$$s = \max\{j; V_P(\pi^{n_{k-1}+e}\tilde{\alpha}_{j,k}) = 0\},$$

тогда ясно, что $m \geq s$, и по (2.10) имеем

$$\pi^s(\pi^{n_{k-1}+e}\tilde{\alpha}_{s,k}) = \pi^{n_{k-1}+e}\alpha_{s,k}. \tag{2.15}$$

По определению s, (2.14) и (2.15) имеем

$$s = V_P\big(\pi^s(\pi^{n_{k-1}+e}\tilde{\alpha}_{s,k})\big) = V_P(\pi^{n_{k-1}+e}\alpha_{s,k}) = l_{k-1} + e + V_P(\alpha_{s,k}) =$$

$$= l_{k-1} + e - l_k - e = u_k,$$

что дает

$$m \geq s \geq u_k. \tag{2.16}$$

Теперь, снова по предложению 2.3, пусть

$$r = \max\{j; V_P(\pi^{n_k+e}\alpha_{j,k}) = 0\},$$

и тогда (2.10) дает

$$\pi^r(\pi^{n_k+e}\tilde{\alpha}_{r,k}) = \pi^{n_k+e}\alpha_{r,k}. \tag{2.17}$$

Кроме того, согласно (2.9) имеем

$$\tilde{\alpha}_{j,k} \in A(f_{k-1}) \implies A(f_{k-1})|\tilde{\alpha}_{j,k} \implies V_P(\tilde{\alpha}_{j,k}) \geq V_P(A(f_{k-1})) = -l_{k-1} - e. \tag{2.18}$$

По определению r и (2.17), применяя (2.18) с $j = r$ дает

$$0 = V_P(\pi^{n_k+e}\alpha_{r,k}) = V_P(\pi^{n_k+e+r}\tilde{\alpha}_{r,k}) = l_k + e + r + V_P(\tilde{\alpha}_{r,k}) \geq$$

$$\geq l_k + e + r - l_{k-1} - e = r - u_k \implies u_k \geq r. \tag{2.19}$$

По (2.9) имеем тождество

$$\tilde{\alpha}_{r,k+1} = \sum_{l=0}^{m-j} \alpha_{r+l,k} \binom{r+l}{r} v_k^l,$$

итак, по определению r (в частности, его максимальность) очевидно, что $V_P(\pi^{n_k+e}\tilde{\alpha}_{r,k+1}) = 0$, что согласно (2.17) дает

$$r = V_P\big(\pi^r(\pi^{n_k+e}\tilde{\alpha}_{r,k+1})\big) = V_P(\pi^{n_k+e}\alpha_{r,k+1}) = l_k + e + V_P(\alpha_{r,k+1}) \geq$$

$$\geq l_k + e - l_{k+1} - e = u_{k+1} \implies r \geq u_{k-1}. \tag{2.20}$$

В силу (2.16), (2.19) и (2.20) имеем цепочку неравенств

$$m \geq s \geq u_k \geq r \geq u_{k+1}. \tag{2.21}$$

Теперь мы покажем, что $u_k \geq 2$.
Мы знаем из (2.10) и (2.11), что

$$u_k = r' + V_P(\tilde{\alpha}_{r',k}) + l_{k-1} + e,$$

где

$$r' + V_P(\tilde{\alpha}_{r',k}) = \min\{j + V_P(\tilde{\alpha}_{j,k}); 1 \leq j \leq m\}.$$

Из (2.9) и (2.14) (при $k-1$) сразу видно, что

$$V_P(\tilde{\alpha}_{j,k}) \geq V_P(A(f_{k-1})) = -l_{k-1} - e,$$

так что если $r' \geq 2$, то будем иметь

$$u_k = r' + V_P(\tilde{\alpha}_{r',k}) + l_{k-1} + e \geq r' \geq 2. \tag{2.22}$$

Если $r' = 1$, тогда знаем, что

$$\tilde{\alpha}_{1,k} = f'_{k-1}(v_{k-1}) \implies V_P(\tilde{\alpha}_{1,k}) \geq 1 - l_{k-1},$$

что дает

$$u_k = 1 + V_P(\tilde{\alpha}_{1,k}) + l_{k-1} + e \geq 2 + e \geq 2. \tag{2.23}$$

Заметим, что (2.22) и (2.23) показывают, что $u_k \geq 2$, что вместе с (2.21) завершает доказательство леммы. □

Теорема 2.2. *Справедлива оценка*

$$|S(f, P^n)| \leq (m-1)N(P^{n-h}).$$

Доказательство. Если $l < 2(w+1)$, то $h = 0$ и утверждение теоремы тривиально. Предположим, что $l \geq 2(w+1)$, и тогда $h > 0$.

Применяя теорему 2.1, видим, что

$$S(f, P^n) = \sum_{v_0,\ldots,v_{h-1}}{}' N(P^{U_h - h}) E(f_0(v_0) + \cdots + f_{h-1}(v_{h-1})) S(f_h, P^{n-U_h}).$$

По лемме 2.7 мы знаем, что количество наборов $\{u_1, \ldots, u_k\}$ не превосходит $m-1$, что вместе с тривиальными оценками $|S(f_h, P^{n-U_h})| \leq N(P^{n-U_h})$ и $|E(x)| = 1$ дает

$$|S(f, P^n)| \leq (m-1)N(P^{U_h-h})N(P^{n-U_h}) = (m-1)N(P^{n-h}).$$

□

2.5 Уточненная оценка Хуа Ло-кена в случае степени простого идеала

В этом разделе мы представляем более сильную форму оценки Хуа Ло-кена [15] в случае идеала, равного степени простого идеала, основываясь на [1], глава 2 (оригинальная работа в [21]). Начнем с представления некоторых вспомогательных результатов.

Предложение 2.4. *([1], стр. 56). Пусть $N > 1$ — вещественное число, а $k, r, \lambda_1, \ldots, \lambda_r$ — рациональные целые числа такие, что $1 \leq r \leq k$ и $\lambda_1, \ldots, \lambda_r > 0$. Тогда*

$$\max_{\lambda_1 + \cdots + \lambda_r = k} \sum_{j=1}^{r} N^{\lambda_j} \leq \max(kN, N^k).$$

Доказательство. Для $\lambda' \geq \lambda \geq 1$, поскольку $N > 1$, имеем

$$(N^{\lambda'} - N)(N^{\lambda-1} - 1) > 0 \implies N^{\lambda'+\lambda-1} + N \geq N^{\lambda'} + N^{\lambda}.$$

Следовательно, имеем

$$\sum_{j=1}^{r} N^{\lambda_j} \leq N^{\lambda_1+\lambda_2-1} + \sum_{j=3}^{r} N^{\lambda_j} + N,$$

и повторное применение этого рассуждения дает

$$\sum_{j=1}^{r} N^{\lambda_j} \leq N^{\lambda_1+\cdots+\lambda_r-r+1} + (r-1)N,$$

что дает оценку

$$\max_{\lambda_1+\cdots+\lambda_r=k} \sum_{j=1}^{r} N^{\lambda_j} \leq N^{k-r+1} + (r-1)N = h(r).$$

Так как $N > 1$, то $h''(r) = N^{k-r+1}(\ln N)^2 > 0$, и поэтому в отрезке $[1, k]$ у нас есть

$$\max_{\lambda_1+\cdots+\lambda_r=k} \sum_{j=1}^{r} N^{\lambda_j} \leq \max\left(h(2.1), h(k)\right) = \max\left(kN, N^k\right).$$

□

Лемма 2.9. *Если $q > m$, то $t = 0$.*

Доказательство. Предположим, $(\alpha_j) = \frac{B_j}{P^{s_j}}$, где B_j — дробный идеал такой, что $V_P(B_j) = 0$. Тогда у нас есть

$$A(f) = \sum_{j=1}^{m} \frac{B_j}{P^{s_j}}. \tag{2.24}$$

По дистрибутивному свойству сложения идеалов мы можем сгруппировать равные степени P в (2.24), что дает

$$A(f) = \sum_{j=1}^{m'} \frac{\tilde{B}_j}{P^{r_j}};\ \tilde{B}_j = \sum_{k;V_P(\alpha_k)=-r_j} B_k,$$

где рациональные целые числа $r_1 > \cdots > r_{m'}$ — разные элементы набора индексов $\{s_j\}_{j=1}^m$. Покажем, что $V_P(\tilde{B}_j) = 0$.

Если $V_P(\tilde{B}_j) = V \neq 0$, то для каждого $1 \leq k \leq m$ пишем $B_k = \frac{C_k}{D_k}$, где C_k, D_k — целые идеалы с $(C_k, D_k) = 1$. Теперь, поскольку $V_P(B_k) = 0$, имеем $V_P(D_k) = 0$. Определим целый идеал

$$\tilde{D}_k = \prod_{k';V_P(\alpha_{k'})D_{k'}=-r_j,k'\neq k} \implies V_P(\tilde{D}_k) = 0.$$

Ясно, что

$$\tilde{B}_j \prod_{k;V_P(\alpha_k)=-r_j} D_k = \sum_{k;V_P(\alpha_k)=-r_j} C_k\tilde{D}_k,$$

и поэтому

$$V_P(\tilde{B}_j) = V \implies V_P(\tilde{B}_j \prod_{k;V_P(\alpha_k)=-r_j} D_k) = V \implies$$

$$\implies V_P(\sum_{k;V_P(\alpha_k)=-r_j} C_k\tilde{D}_k) = V \implies V > 0$$

поскольку $\sum_{k;V_P(\alpha_k)=-r_j} C_k\tilde{D}_k$ — целый идеал.

Кроме того, имеем

$$V_P(\sum_{k;V_P(\alpha_k)=-r_j} C_k\tilde{D}_k) = V \implies \sum_{k;V_P(\alpha_k)=-r_j} C_k\tilde{D}_k \subseteq P^V \implies$$

$$\implies C_k\tilde{D}_k \subseteq P^V \implies V_P(C_k\tilde{D}_k) \geq V,$$

что является противоречием тому, что $V_P(C_k) = V_P(\tilde{D}_k) = 0$.

Следовательно, имеем $V_P(\tilde{B}_j) = 0$ и тогда

$$V_P(A(f)) = -r_1. \tag{2.25}$$

Мы знаем, что

$$A(f') = \sum_{j=1}^m \frac{jB_j}{P^{s_j}},$$

и аналогично (2.24) запишем

$$A(f) = \sum_{j=1}^{m'} \frac{\tilde{B}_j}{P^{r_j}};\ \tilde{B}_j = \sum_{k;V_P(\alpha_k)=-r_j} kB_k.$$

Так как $q > m$ и q — рациональное простое число в $\mathbb{Z}$, то $(k, q) = 1$ для всех $1 \leq k \leq m$, откуда следует, что $(k, P) = 1$, и поэтому $(kB_k, P) = 1$.

Аналогично видим, что $V_P(\tilde{B}_j) = 0$ и, следовательно, что

$$V_P(A(f')) = -r_1. \tag{2.26}$$

Таким образом, согласно (2.25) и (2.26), по определению t имеем

$$V_P(A(f)) = V_P(A(f')) \implies t = 0.$$

□

Лемма 2.10. *Справедливо тождество*

$$w = (e+1)\left\lfloor \frac{\ln m}{\ln q} \right\rfloor.$$

Доказательство. Мы знаем (см., например, [4], стр. 427), что

$$P \cap \mathbb{Z} = (q),$$

и что

$$q = P^{e+1}Q;\ (Q, P) = 1 \implies q \in P^{e+1}, q \notin P^{e+2},$$

для некоторого целого идеала Q, и тогда $V_P(q) = e + 1$.

Рассмотрим рациональное целое число k с $1 \leq k \leq m$. Запишем $k = q^{r(k)}k'$, где $(k', q) = 1$, и тогда имеем

$$V_P(k) = V_P(q^{r(k)}) + V_P(k') = V_P(q^{r(k)}) = r(k)V_P(q) = r(k)(e+1). \tag{2.27}$$

Легко видеть, что

$$\max\{r(k); 1 \le k \le m\} = \left\lfloor \frac{\ln m}{\ln q} \right\rfloor,$$

откуда, вместе с (2.27), непосредственно следует утверждение леммы. □

Теорема 2.3. *Пусть $N(P) = q^r$, где $r \ge 1$ рациональное целое число. Справедлива общая оценка*

$$|S(f, P^n)| \le C_d(m) N(P)^{n(1-\frac{1}{m})},$$

где

$$C_d(m) = \begin{cases} m^d \quad \textit{если } q > m, N(P) \ge (m-1)^{\frac{m}{m-2}}, \\ \frac{m-1}{m} m^{\frac{3}{m}} \quad \textit{если } q > m, N(P) \le (m-1)^{\frac{m}{m-2}}, \\ m^{\frac{d(2d+1)}{m}} \quad \textit{если } q \le m, N(P) \ge (m-1)^{\frac{m}{m-2}}, \\ (m-1) m^{\frac{d(2d+1)}{m}} \quad \textit{если } q \le m, N(P) \le (m-1)^{\frac{m}{m-2}}. \end{cases}$$

Более того, справедлива конкретная оценка

$$|S(f, P^n)| \le C_d(m, P) N(P)^{n(1-\frac{1}{m})},$$

где

$$C_d(m, P) = \begin{cases} m^d \quad \textit{если } q > m, N(P) \ge (m-1)^{\frac{m}{m-2}}, \\ \frac{m-1}{m} m^{\frac{3}{m}} \quad \textit{если } q > m, N(P) \le (m-1)^{\frac{m}{m-2}}, \\ m^{\frac{r(2e+3)}{m}} \quad \textit{если } q \le m, N(P) \ge (m-1)^{\frac{m}{m-2}}, \\ (m-1) m^{\frac{r(2e+3)}{m}} \quad \textit{если } q \le m, N(P) \le (m-1)^{\frac{m}{m-2}}. \end{cases}$$

Доказательство. Сначала мы докажем конкретную оценку, а затем из нее выведем общую оценку.

Для удобства положим $N = N(P)$. Мы рассматриваем несколько случаев. Во всех случаях доказательство будет проводиться индукцией по l.

Случай 1. $q > m$:

По лемме 2.10 имеем $t = 0$. Если $l < 2(t+1)$, то $l = 1$, и лемма следует из оценки Морделла ([18], стр. 17, а оригинальная работа в [25]).

$$|S(f, P)| \le m^d N^{1-\frac{1}{m}}. \tag{2.28}$$

Предположим, что $l \geq 2$. Пусть $v_1, \ldots, v_r$ — несравнимые решения сравнения $\pi^l f'(v) \equiv 0 \mod P$ такие, что v_j имеет кратность λ_j, и пусть $\sum_{j=1}^{r} \lambda_j = n$. Далее, обозначим через $\sigma_j = u(v_j)$ индексы в конструкции после леммы 2.5.

Используя разложение в ряд Тейлора

$$g_j(y) = f(\pi y + v_j) - f(v_j) = \sum_{k=1}^{m} \frac{\pi^k y^k}{k!} f^{(k)}(v_j),$$

лемму 2.2 и (2.11), видим, что

$$V_P\left(\frac{\pi^{\lambda_j+1}}{(\lambda_j+1)!}\pi^{n+e} f^{(\lambda_j+1)}(v_j)\right) \leq \lambda_j + 1 \implies \sigma_j \leq \lambda_j + 1. \tag{2.29}$$

По лемме 2.1 мы знаем, что

$$n \leq m - 1. \tag{2.30}$$

Применение неравенства треугольника к (2.5) дает

$$|S(f, P^n)| \leq \sum_{j=1}^{r} |S_{v_j}|. \tag{2.31}$$

Если $l > \sigma_j$, то в доказательстве леммы 2.6 было показано, что

$$|S_{v_j}| = N^{\sigma_j - 1} |S(g_j, P^{n-\sigma_j})|. \tag{2.32}$$

Случай 1а. $N \geq (m-1)^{\frac{m}{m-2}}$:

По (2.28) и предположению индукции в (2.32), имеем

$$|S_{v_j}| \leq m^d N^{\sigma_j - 1} N^{(l-\sigma_j)(1-\frac{1}{m})}, \tag{2.33}$$

причем эта оценка верна и в том случае, если $\sigma_j \geq l$, так как в этом случае она следует из тривиальной оценки $|S_{v_j}| \leq N^{l-1}$.

Следовательно, по (2.31) и (2.33), получаем

$$|S(f, P^n)| \leq m^d \sum_{j=1}^{r} N^{\sigma_j - 1} N^{(l-\sigma_j)(1-\frac{1}{m})} =$$

$$= m^d N^{l(1-\frac{1}{m})} \sum_{j=1}^{r} N^{-1+\frac{\sigma_j}{m}}. \tag{2.34}$$

Поскольку по (2.29) и лемме 2.1 имеем $\sigma_j \le \lambda_j + 1 \le m$, то предложение 2.9 дает

$$\sum_{j=1}^{r} N^{-1+\frac{\sigma_j}{m}} \le N^{-1+\frac{1}{m}} \sum_{j=1}^{r} N^{\frac{\lambda_j}{m}} \le N^{-1+\frac{1}{m}} \max\left((m-1)N^{\frac{1}{m}}, N^{1-\frac{1}{m}}\right). \tag{2.35}$$

Легко видеть, что

$$N \ge (m-1)^{\frac{m}{m-2}} \implies \max\left((m-1)N^{\frac{1}{m}}, N^{1-\frac{1}{m}}\right) = N^{1-\frac{1}{m}}. \tag{2.36}$$

Подстановка (2.35) и (2.36) в (2.34) дает

$$\sum_{j=1}^{r} N^{-1+\frac{\sigma_j}{m}} \le 1 \implies |S(f, P^n)| \le m^d N^{l(1-\frac{1}{m})},$$

что и доказывает утверждение теоремы в данном случае.

Случай 1б. $N \le (m-1)^{\frac{m}{m-2}}$:

Сначала докажем оценку

$$|S(f, P^n)| \le n N^{-1+\frac{3}{m}} N^{l(1-\frac{1}{m})}. \tag{2.37}$$

По определению сразу видно, что $r \le n$, поэтому базовый случай $l = 2$ следует из тривиальной оценки

$$|S(f, P^2)| \le \sum_{j=1}^{r} |S_{v_j}| \le rN \le nN^{1+\frac{1}{m}}.$$

Предполагая, что (2.37) справедлива для всех $2 \le l \le L$, мы докажем, что она справедлива для $l = L + 1$.

По определению σ_j и поскольку в силу (2.29) имеем $\sigma_j \le \lambda_j + 1$, мы видим, что

$$g_j(y) \equiv \sum_{k=1}^{\lambda_j+1} \frac{\pi^k y^k}{k!} f^{(k)}(v_j) \mod P,$$

и значит, по лемме 2.1 число решений сравнения $\pi^{n-\sigma_j} g_j'(y) \equiv 0 \mod P$ не превосходит λ_j.

Если $\sigma_j < L$, то предположение индукции дает

$$|S_{v_j}| = N^{\sigma_j - 1}|S(g_j, P^{n+1-\sigma_j})| \le \lambda_j N^{\sigma_j - 2 + \frac{3}{m} + (L+1-\sigma_j)(1-\frac{1}{m})} \le$$

$$\lambda_j N^{-2+\frac{\lambda_j+1}{m}+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})}. \tag{2.38}$$

Если $\sigma_j \ge L$, используем тривиальную оценку $|S_{v_j}| \le N^L$.

Сначала предположим, что $L > \sigma_j$ для всех $1 \le j \le r$. Тогда, поскольку $\lambda_j \le m-1$ по лемме 2.1, подстановка (2.38) в (2.31) дает

$$|S(f, P^{n+1})| \le \sum_{j=1}^{r} |S_{v_j}| \le N^{-2+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})} \sum_{j=1}^{r} \lambda_j N^{\frac{\lambda_j+1}{m}} \le$$

$$\le N^{-1+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})} \sum_{j=1}^{r} \lambda_j = nN^{-1+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})},$$

что завершает доказательство (2.37) если $L > \sigma_j$ для всех $1 \le j \le r$.

Предположим теперь, не ограничивая общности, что

$$\sigma_1 \ge \cdots \ge \sigma_{r_1} \ge L > \sigma_{r_1+1} \ge \cdots \ge \sigma_r.$$

Положим $\sum_{j=1}^{r_1} \lambda_j = n_1$ и $\sum_{j=r_1+1}^{r} \lambda_j = n_2$, а тогда $n_1 + n_2 = n$.

Для $1 \le j \le r_1$ по (2.29) имеем

$$\lambda_j + 1 \ge \sigma_j \ge L \implies n_1 + r_1 \ge r_1 L \implies \frac{n_1}{r_1} + 1 \ge L,$$

что дает

$$L = (L+1)(1-\frac{1}{m}) - 1 + \frac{2}{m} + \frac{L-1}{m} \le (L+1)(1-\frac{1}{m}) - 1 + \frac{2}{m} + \frac{n_1}{r_1 m}.$$

Положим $h_1(y) = yN^{\frac{n_1}{ym}}$. Тогда имеем

$$h_1'(y) = N^{\frac{n_1}{ym}}\Big(1 - \frac{n_1 \ln(N)}{ym}\Big) \implies h_1''(y) = N^{\frac{n_1}{ym}} \frac{n_1^2\big(\ln(N)\big)^2}{y^3 m^2},$$

и поэтому $h_1''(y) \ge 0$, что дает

$$r_1 N^{\frac{n_1}{r_1 m}} \le \max\left(N^{\frac{n_1}{m}}, n_1 N^{\frac{1}{m}}\right) \tag{2.39}$$

Теперь мы покажем, что $n_1 N^{\frac{1}{m}} \ge N^{\frac{n_1}{m}}$.

Положим $h_2(y) = yN^{\frac{1}{m}} - N^{\frac{y}{m}}$. Тогда имеем

$$h_2'(y) = N^{\frac{1}{m}} - \frac{1}{m}\ln(N)N^{\frac{y}{m}} \implies h_2''(y) = \frac{-1}{m^2}\big(\ln(N)\big)^2 N^{\frac{y}{m}},$$

и поэтому $h_2''(y) \le 0, h_2(2,1) = 0$.

Более того, поскольку $(m-1)^{\frac{m}{m-2}} \ge N > m$, то $h_2'(2,1) \ge 0$ и $h_2(m-1) \ge 0$.

Следовательно, имеем $h_2(y) \ge 0$ для $1 \le y \le m-1$, и поскольку по (2.30) и определению n_1 имеем $n_1 \le n \le m-1$, то это дает

$$n_1 N^{\frac{1}{m}} \ge N^{\frac{n_1}{m}}. \tag{2.40}$$

Поэтому, подставив (2.40) в (2.39), учитывая (2.31), (2.38) и тривиальную оценку $|S_{v_j}| \le N^L$, получим

$$|S(f,P^{n+1})| \le \sum_{j=1}^{r_1}|S_{v_j}| + \sum_{j=r_1+1}^{r}|S_{v_j}| \le r_1 N^L + N^{-2+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})} \sum_{j=r_1+1}^{r} \lambda_j N^{\frac{\lambda_j+1}{m}} \le$$

$$\le N^{-1+\frac{2}{m}} N^{(L+1)(1-\frac{1}{m})}\Big(r_1 N^{\frac{n_1}{r_1 m}} + \sum_{j=r_1+1}^{r} \lambda_j N^{\frac{\lambda_j+1}{m}-1+\frac{1}{m}}\Big) \le$$

$$\le N^{-1+\frac{2}{m}} N^{(L+1)(1-\frac{1}{m})}\big(n_1 N^{\frac{1}{m}} + n_2 N^{\frac{1}{m}}\big) \le n N^{-1+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})},$$

что завершает доказательство (2.37) если $\sigma_1 \ge \cdots \ge \sigma_{r_1} \ge L > \sigma_{r_1+1} \ge \cdots \ge \sigma_r$.

Так как $q > m$, то $N \ge m$, а так как $-1 + \frac{3}{m} \le 0$, учитывая (2.30), то в силу (2.37) имеем

$$|S(f,P^n)| \le n N^{-1+\frac{3}{m}} N^{l(1-\frac{1}{m})} \le \frac{m-1}{m} m^{\frac{3}{m}} N^{l(1-\frac{1}{m})},$$

что и доказывает утверждение теоремы в данном случае.

Случай 2. $q \le m$:

Предположим сначала, что $l < 2(t+1)$. В этом случае воспользуемся тривиальной оценкой

$$|S(f,P^n)| \le N^l = N^{\frac{l}{m}} N^{l(1-\frac{1}{m})} \le N^{\frac{2t+1}{m}} N^{l(1-\frac{1}{m})},$$

что в силу предложения 2.2, леммы 2.10 и того факта, что $q \le m$, дает

$$|S(f,P^n)| \le N^{\frac{2(e+1)\ln(m)}{m\ln(q)}+\frac{\ln(m)}{m\ln(q)}} N^{l(1-\frac{1}{m})} =$$

$$= m^{\frac{2(e+1)\ln(N)}{m\ln(q)}+\frac{\ln(N)}{m\ln(q)}} N^{l(1-\frac{1}{m})} = m^{\frac{r(2e+3)}{m}} N^{l(1-\frac{1}{m})}. \tag{2.41}$$

Для $l \ge 2(t+1)$ утверждение теоремы доказывается индукцией по l.

Случай 2а. $N \ge (m-1)^{\frac{m}{m-2}}$:

Этот случай аналогичен случаю 1а. По предположению индукции (2.41) получаем

$$|S_{v_j}| = m^{\frac{r(2e+3)}{m}} N^{\sigma_j-1}|S(g_j,P^{n-\sigma_j})| \le N^{\sigma_j-1}N^{(l-\sigma_j)(1-\frac{1}{m})}, \tag{2.42}$$

причем эта оценка верна и в том случае, если $\sigma_j \ge l$, так как в этом случае она следует из тривиальной оценки $|S_{v_j}| \le N^{l-1}$.

Подстановка (2.42) в (2.31) дает

$$|S(f,P^n)| \le m^{\frac{r(2e+3)}{m}} \sum_{j=1}^{r} N^{\sigma_j-1}N^{(l-\sigma_j)(1-\frac{1}{m})} =$$

$$= m^{\frac{r(2e+3)}{m}} N^{l(1-\frac{1}{m})} \sum_{j=1}^{r} N^{-1+\frac{\sigma_j}{m}}. \tag{2.43}$$

Поскольку $\sigma_j \le \lambda_j + 1 \le m$ в силу (2.29) и леммы 2.1, то предложение 2.9 дает

$$\sum_{j=1}^{r} N^{-1+\frac{\sigma_j}{m}} \le N^{-1+\frac{1}{m}} \sum_{j=1}^{r} N^{\frac{\lambda_j}{m}} \le N^{-1+\frac{1}{m}} \max\left((m-1)N^{\frac{1}{m}}, N^{1-\frac{1}{m}}\right). \tag{2.44}$$

Мы знаем, что

$$N \ge (m-1)^{\frac{m}{m-2}} \implies \max\left((m-1)N^{\frac{1}{m}}, N^{1-\frac{1}{m}}\right) = N^{1-\frac{1}{m}}, \tag{2.45}$$

и поэтому подстановка (2.44) и (2.45) в (2.43) дает

$$\sum_{j=1}^{r} N^{-1+\frac{\sigma_j}{m}} \le 1 \implies |S(f,P^n)| \le m^{\frac{r(2e+3)}{m}} N^{l(1-\frac{1}{m})},$$

что и доказывает утверждение теоремы в данном случае.

Случай 2б. $N \le (m-1)^{\frac{m}{m-2}}$:

По предположению индукции (2.41), если $l > \sigma_j$, получим

$$|S_{v_j}| = N^{\sigma_j - 1}|S(g_j, P^{n-\sigma_j})| \le m^{\frac{r(2e+3)}{m}} \lambda_j N^{\sigma_j - 1} N^{(l-\sigma_j)(1-\frac{1}{m})}, \tag{2.46}$$

и эта оценка справедлива и в том случае, если $\sigma_j \ge l$, так как в этом случае она следует из тривиальной оценки $|S_{v_j}| \le N^{l-1}$.

Следовательно, поскольку $\sigma_j \le \lambda_j + 1 \le m$ в силу (2.29) и леммы 2.1, то подстановка (2.46) в (2.31) дает

$$|S(f, P^n)| \le m^{\frac{r(2e+3)}{m}} N^{l(1-\frac{1}{m})} N^{-1} \sum_{j=1}^{r} \lambda_j N^{\frac{\lambda_j + 1}{m}} \le nm^{\frac{r(2e+3)}{m}} N^{l(1-\frac{1}{m})},$$

что, поскольку $n \le m - 1$ по (2.30), дает

$$|S(f, P^n)| \le (m-1)m^{\frac{r(2e+3)}{m}} N^{l(1-\frac{1}{m})},$$

что и доказывает утверждение теоремы в данном случае.

Этим завершается доказательство конкретной оценки во всех случаях.

Общая оценка непосредственно следует из неравенств $r \le d$ и $e \le d - 1$, которые легко следуют из применения теоремы о единственности разложения идеалов в полях алгебраических чисел к (q):

$$(q) = \prod_{j=1}^{s'} \tilde{P}_j^{e_j - 1} \implies q^d = \prod_{j=1}^{s'} N(\tilde{P}_j^{e_j+1}) = q^{\sum_{j=1}^{s'} r_j(e_j+1)} \implies d = \sum_{j=1}^{s'} r_j(e_j + 1),$$

где $e_j + 1$ — индекс ветвления простого идеала $\tilde{P}_j$. □

2.6 Уточненная оценка Хуа Ло-кена для определенного класса многочленов, когда число классов равно 1

В этом разделе мы получим более сильную форму теоремы 2.3 в частном случае, когда $\mathbb{K}$ имеет число классов равно 1, а идеал A имеет вид

$$A = \frac{B}{P^n};\ (B, P) = 1,$$

для некоторого целого идеала B, что позволит получить более сильную форму оценки Хуа

Ло-кена в [15] для идеалов Q, удовлетворяющих условию $(Q, \delta) = 1$.

Начнем со вспомогательной леммы, которая будет играть роль, аналогичную лемме 2.3.

Лемма 2.11. *Пусть P — простой идеал такой, что $P \nmid \delta$, а $\alpha \in R$ — целое число. Пусть η пробегает полную систему вычетов P^{-n} по модулю R.*

Тогда

$$\sum_{\eta} E(\alpha\eta) = \sum_{\eta} e^{2\pi i T(\alpha\eta)} = \begin{cases} N(P^n) & \text{если } P^n|\alpha, \\ 0 & \text{если } P^n \nmid \alpha. \end{cases}$$

Доказательство. Если $P^n|\alpha$, то $\alpha\eta \in R$, что дает $E(\alpha\eta) = 1$, и тогда

$$\sum_{\eta} E(\eta\alpha) = N(P^n).$$

Мы покажем, что существует $\eta \in P^{-n}$, скажем η_0, такая, что $\eta\alpha \notin \delta^{-1}$.

Если $\eta\alpha \in \delta^{-1}$ для всех $\eta \in P^{-n}$, то $\delta^{-1}|\alpha P^{-n}$, и тогда $P^n|\alpha\delta^{-1}$.

Поскольку P — простой идеал и $P^n \nmid \alpha$, то $P|\delta^{-1}$, что является противоречием.

По определению δ^{-1} существует целое число γ такое, что $E(\gamma\eta_0\alpha) \neq 1$. Поскольку $\gamma\eta_0 \in P^{-n}$, имеем

$$\sum_{\eta} E(\eta\alpha) = \sum_{\eta} E(\gamma\eta_0\alpha + \eta\alpha) = E(\gamma\eta_0\alpha) \sum_{\eta} E(\eta\alpha) \implies \sum_{\eta} E(\eta\alpha) = 0,$$

поскольку $E(\gamma\eta_0\alpha) \neq 1$. □

Теорема 2.4. *Пусть $N(P) = q^r$, где $r \geq 1$ — целое рациональное число. Тогда мы имеем общую оценку*

$$|S(f, P^n)| \leq C_d(m) N(P)^{n(1-\frac{1}{m})},$$

где

$$C_d(m) = \begin{cases} 1 \quad \textit{если } q > m, N(P) \geq (m-1)^{\frac{2m}{m-2}}, \\ (m-1)^{\frac{2}{m}} \textit{если } q > m, (m-1)^{\frac{2m}{m-2}} > N(P) \geq (m-1)^{\frac{m}{m-2}}, \\ \frac{m-1}{m} m^{\frac{3}{m}} \quad \textit{если } q > m, N(P) < (m-1)^{\frac{m}{m-2}}, \\ m^{\frac{d(2d+1)}{m}} \quad \textit{если } q \leq m, N(P) \geq (m-1)^{\frac{m}{m-2}}, \\ (m-1)m^{\frac{d(2d+1)}{m}} \quad \textit{если } q \leq m, N(P) < (m-1)^{\frac{m}{m-2}}. \end{cases}$$

Доказательство. Доказательство полностью аналогично доказательству теоремы 2.3, за исключением случая 1a, где вместо использования оценки Морделла ([18], стр. 17) теперь используем оценку Вейля для экспоненциальных сумм над конечными полями [19].

Действительно, поскольку P простой идеал, то R/P — конечное поле. Более того, поскольку число классов $\mathbb{K}$ равно 1, знаем, что P — главный идеал, скажем, с $P = (\pi)$. Допустим сначала, что $n = 1$.

Поскольку $A = \frac{B}{P}$, то каждое α_j можно выразить как

$$\alpha_j = \frac{b_j}{\pi},$$

и имеем

$$e^{2\pi i T(\frac{b_j + r\pi}{\pi} x^j)} = e^{2\pi i T(\frac{b_j}{\pi} x^j)}$$

для любого $r \in R$, откуда следует, что $\chi(y) = e^{2\pi i T(\frac{y}{\pi})}$ — аддитивный характер конечного поля R/P.

Следовательно, сумма действительно является экспоненциальной суммой по конечному полю, и оценка Вейля [19] в этом случае дает

$$|S(f,P)| \leq (m-1)N^{\frac{1}{2}} \Longleftrightarrow |S(f,P)| \leq \min\left(N^{\frac{1}{m}}, (m-1)N^{\frac{-1}{2}+\frac{1}{m}}\right) N^{1-\frac{1}{m}},$$

где эквивалентность следует из тривиальной оценки $|S(f,P)| \leq N$.

Как и в случае 1a теоремы 2.3, получаем

$$|S(f,P^n)| \leq \max\left(1, \min\left(N^{\frac{1}{m}}, (m-1)N^{\frac{-1}{2}+\frac{1}{m}}\right)\right) N^{l(1-\frac{1}{m})}. \tag{2.47}$$

Если $N \leq (m-1)^2$, то

$$\min\left(N^{\frac{1}{m}}, (m-1)N^{\frac{-1}{2}+\frac{1}{m}}\right) = N^{\frac{1}{m}}\ 1 \leq N^{\frac{1}{m}} \leq (m-1)^{\frac{2}{m}}, \tag{2.48}$$

и поэтому подстановка (2.48) в (2.47) дает

$$|S(f, P^n)| \leq (m-1)^{\frac{2}{m}} N^{l(1-\frac{1}{m})}.$$

Если $N \geq (m-1)^2$ и $N \leq (m-1)^{\frac{2m}{m-2}}$, то

$$\min\left(N^{\frac{1}{m}}, (m-1)N^{\frac{-1}{2}+\frac{1}{m}}\right) = (m-1)N^{\frac{-1}{2}+\frac{1}{m}},\ 1 \leq (m-1)N^{\frac{-1}{2}+\frac{1}{m}} \leq (m-1)^{\frac{2}{m}}, \tag{2.49}$$

и поэтому в этом случае также подстановка (2.49) в (2.47) дает

$$|S(f, P^n)| \leq (m-1)^{\frac{2}{m}} N^{l(1-\frac{1}{m})}.$$

Наконец, если $N \geq (m-1)^{\frac{2m}{m-2}}$, то $N \geq (m-1)^2$, и поэтому

$$\min\left(N^{\frac{1}{m}}, (m-1)N^{\frac{-1}{2}+\frac{1}{m}}\right) = (m-1)N^{\frac{-1}{2}+\frac{1}{m}} \leq 1, \tag{2.50}$$

и подстановка (2.50) в (2.47) дает

$$|S(f, P^n)| \leq N^{l(1-\frac{1}{m})}.$$

□

Предложение 2.5. *Пусть $\tilde{q}$ — рациональное простое число. Тогда число простых идеалов $\tilde{P}_j$ в R, у которых $N(\tilde{P}_j) = \tilde{q}^{c_j}$ для некоторого $c_j \geq 1$, не превосходит d.*

Доказательство. По теореме о единственности разложения идеалов в полях алгебраических чисел, имеем

$$(\tilde{q}) = \prod_{j=1}^{s'} \tilde{P}_j^{e_j+1} \implies q'^d = \prod_{j=1}^{s'} N(\tilde{P}_j^{e_j+1}) \implies d = \sum_{j=1}^{s'} c_j(e_j+1) \geq s'$$

где e_j — индекс ветвления простого идеала $\tilde{P}_j$. □

Теперь сформулируем и докажем следующую усиленную форму теоремы Хуа Ло-кена, в нашем частном случае.

Теорема 2.5. *Пусть Q — целый идеал с $(Q,\delta)=1$. Тогда справедлива оценка*

$$|S(f,Q)| \le e^{\frac{5}{2}d^2(2d+1)} e^{3.442md} N(Q)^{1-\frac{1}{m}}.$$

Доказательство. По теореме о единственности разложения идеалов в полях алгебраических чисел мы знаем, что Q однозначно выражается как

$$Q = \prod_{j=1}^{s} P_j^{r_j},\ r_j \ge 0, \tag{2.51}$$

где P_j — различные простые идеалы, а $r_j \in \mathbb{Z}$.

Следовательно, по (2.51) и лемме 2.4 имеем

$$S(f,Q) = \prod_{j=1}^{s} S(f_j, P_j^{r_j}),$$

для некоторых многочленов f_j степени m (а не многочленов из построения деревьев Хуа Локена в разделе 2.5, хоть обозначения совпадают), и поэтому, поскольку $(P_j,\delta)=1$ для $1 \le j \le s$, то по теореме 2.4 это дает

$$|S(f,Q)| \le \prod_{j=1}^{s} C_{d,j}(m) N(P_j^{r_j})^{1-\frac{1}{m}} = N(Q)^{1-\frac{1}{m}} \prod_{j=1}^{s} C_{d,j}(m), \tag{2.52}$$

где $C_{d,j}(m)$ — константа из теоремы 2.4, соответствующая P_j.

Для любого натурального числа $x \in \mathbb{Z}$, обозначаем через $\pi(x)$ обычную рациональную функцию распределения простых чисел в $\mathbb{Z}$,

$$\pi(x) = |\{k \in \mathbb{Z}; k \le x, k \text{ является простым в } \mathbb{Z}\}|,$$

и обозначаем через $\tilde{\pi}(x)$ функцию распределения простых идеалов в R,

$$\tilde{\pi}(x) = |\{P \subseteq R; N(P) \le x, P \text{ является простым идеалом в } R\}|.$$

Мы знаем, что $N(P) = q^r$, где q — простое число в $\mathbb{Z}$, и поэтому предложение 2.5 дает

$$N(P) \le x \implies q \le x \implies \tilde{\pi}(x) \le d\pi(x). \tag{2.53}$$

Положим $A = (m-1)^{\frac{2m}{m-2}}$ и $B = (m-1)^{\frac{m}{m-2}}$.

Теперь оценим $\prod_{j=1}^{s} C_{d,j}(m)$. Из формулировки теоремы 2.4 непосредственно следует, что

$$\prod_{j=1}^{s} C_{d,j}(m) \le \big((m-1)^{\frac{2}{m}}\big)^{\tilde{\pi}(A)-\tilde{\pi}(B)} \Big(\frac{m-1}{m} m^{\frac{3}{m}}\Big)^{\tilde{\pi}(B)} \big(m^{\frac{d(2d+1)}{m}}\big)^{d\pi(m)} \big((m-1)m^{\frac{d(2d+1)}{m}}\big)^{d\pi(m)}, \quad (2.54)$$

где степень $d\pi(m)$ в предыдущей оценке следует из предложения 2.5.

Поэтому, по (2.53) и (2.54) имеем

$$\prod_{j=1}^{s} C_{d,j}(m) \le e^{F(m)}, \quad (2.55)$$

где

$$F(m) = \ln(m)\bigg(\Big(\frac{3}{m}-1\Big)d\pi(B) + d\pi(m)\Big(\frac{2d(2d+1)}{m}\Big)\bigg) + \\ + \ln(m-1)\bigg(\frac{2d}{m}\pi(A) + \Big(1-\frac{2}{m}\Big)d\pi(B) + d\pi(m)\bigg). \quad (2.56)$$

Имеем $\frac{3}{m} - 1 \le 0$, и используя известную оценку $\pi(x) \le \frac{5x}{4\ln(x)}$ при $x \ge 3$ (см., например, [1], стр. 61) в (2.56) получим

$$F(m) \le \frac{5}{2}d^2(2d+1) + \ln(m-1)\bigg(\frac{5dA}{2m\ln(A)} + \frac{5dB(m-2)}{4m\ln(B)} + \frac{5dm}{4\ln(m)}\bigg). \quad (2.57)$$

Вычисляем

$$\frac{5dA\ln(m-1)}{2m\ln(A)} = md\bigg(\frac{5(m-2)(m-1)^{\frac{2m}{m-2}}}{4m^3}\bigg) \le 0.792md, \quad (2.58)$$

где последнее неравенство следует из элементарного математического анализа.

Аналогичным образом получим

$$\frac{5dB(m-2)\ln(m-1)}{4m\ln(B)} = md\bigg(\frac{5(m-2)^2(m-1)^{\frac{m}{m-2}}}{4m^3}\bigg) \le 1.4md, \quad (2.59)$$

и

$$\frac{5dm\ln(m-1)}{4\ln(m)} \le 1.25dm. \quad (2.60)$$

Поэтому подстановка (2.58), (2.59) и (2.60) в (2.57) дает

$$F(m) \leq \frac{5}{2}d^2(2d+1) + 3.442md,$$

что вместе с (2.52) и (2.55) завершает доказательство. □

2.7 Новая оценка и некоторые выводы

Заметим, что константу $e^{\frac{5}{2}d^2(2d+1)}e^{3.442md}$ в теореме 2.5 можно существенно улучшить, используя более точные оценки $\pi(x)$ и $\tilde{\pi}(x)$, а также числа простых идеалов, удовлетворяющих каждому из случаев теоремы 2.4.

Заметим также, что для доказательства аналога теоремы 2.5 в общем случае нам не обязательно нужна столь сильная оценка, как у Вейля. Действительно, если бы мы имели какую-либо оценку вида

$$|S(f,P)| \leq C' N^{1-\frac{1}{m}-\epsilon};\ \epsilon > 0,$$

для некоторой постоянной C', то аналогично доказательству теоремы 2.4, в тех же терминах получаем, что

$$N^{\epsilon} \geq C' \implies C_d(m) = 1.$$

Наконец, отметим, что объединение теоремы 2.1 и теоремы 2.3 дает следующую новую оценку.

Теорема 2.6. *Справедлива оценка*

$$|S(f,P^n)| \leq C_d(m)(m-1)N(P)^{n(1-\frac{1}{m})+\frac{U_h}{m}-h}.$$

Легко видеть, что теорема 2.6 дает более точную оценку, чем теорема 2.2, поскольку $l \geq U_h$, и также лучшую оценку, чем теорема 2.3, поскольку по лемме 2.8 $mh \geq U_h$.

Глава 3

Формула А.Г. Постникова и оценки некоторых сумм характеров в полях алгебраических чисел[3]

3.1 Постановка задачи

Характеры Дирихле, впервые введенные П.Л. Дирихле в 1837 г., играют центральную роль в мультипликативной теории чисел. Первоначально они использовались им для доказательства теоремы о простых числах в арифметических прогрессиях. Многие важные вопросы аналитической теорией чисел были разработаны на основе характеров Дирихле и теории L-функций Дирихле.

В современной теории L-функций большое значение имеют оценки сумм характеров.

Известная формула А.Г. Постникова [26], доказанная им в 1955 г., выражает характеры Дирихле по модулю степени простого числа через экспоненты от многочленов с рациональными коэффициентами. Таким образом, задача об оценке сумм таких характеров Дирихле сводится к методу тригонометрических сумм И.М. Виноградова. Подобные суммы оценивались Н.М. Коробовым, А.А. Карацубой, Н.Г. Чудаковым, С.М. Розиным, В.Н. Чубариковым и др.

Отличие общего случая от случая степени простого числа два обусловлено различием в строении групп $\mathbb{Z}/p^n\mathbb{Z}$ и $\mathbb{Z}/2^n\mathbb{Z}$ при $n \geq 3$, где p — нечетное простое число.

[3]При подготовке данной главы диссертации использовались следующие публикации автора, в которых, согласно «Положению о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова», отражены основные результаты, положения и выводы исследования: [33,34].

Из-за своей важности и общности характеры Дирихле были обобщены на поля алгебраических чисел. Подобная теория была разработана для теории L-функций в этих полях.

Данная глава состоит из трех частей. Первая часть обобщает формулу А.Г. Постникова на случай модуля, равного степени простого числа два, и выводятся некоторые полезные оценки, касающиеся сумм характеров по модулю степени простого числа два.

Вторая часть представляет собой набор структурных результатов, касающихся колец вычетов по модулю идеала, равного степени простого идеала в кольце целых поля алгебраических чисел. Подобная формулировка и доказательство этих результатов содержатся, в гораздо более общем формате, в работах М. Элиа, Д.С. Интерландо и Р. Розенбаума [27] (для неразветвленных простых идеалов) и в [28] (для разветвленных простых идеалов). Нами найдено простое доказательство для неразветвленного случая. Оно тесно связано с дальнейшим выводом аналога формулы А.Г. Постникова.

Третья часть объединяет первую часть, работу А.Г. Постникова и вторую часть, для того, чтобы получить оценки сумм мультипликативных характеров в полях алгебраических чисел.

3.2 Формула А.Г. Постникова для характеров по модулю степени простого числа 2

В данном разделе мы обобщаем формулу А.Г. Постникова [26] на случай модуля, равного степени простого числа два.

Пусть $n \geq 3$ — натуральное, и $d = \left\lfloor \frac{n-1}{2} \right\rfloor$. Положим $\varepsilon(n) = 1$, если n четное, и $\varepsilon(n) = 0$, если n нечетное.

Если d представляется в виде $d = \alpha 2^{\tilde{f}} - \mu(\tilde{f})$, где $\tilde{f}, \mu(\tilde{f}) \in \mathbb{Z}, 0 \leq \mu(\tilde{f}) \leq \frac{\tilde{f}+\varepsilon(n)}{2}$ и α нечетное, тогда положим f, равным максимальному значению среди таких $\tilde{f}$, т.е.

$$f = \max\{\tilde{f}; d = \alpha 2^{\tilde{f}} - \mu(\tilde{f});\ \tilde{f}, \mu(\tilde{f}) \in \mathbb{Z}, 0 \leq \mu(\tilde{f}) \leq \frac{\tilde{f}+\varepsilon(n)}{2}, \alpha \text{ нечетное}\}.$$

Определим

$$\mu = \begin{cases} \mu(f) \text{ если } d = \alpha 2^{\tilde{f}} - \mu(\tilde{f}), \\ 0 \text{ в противном случае.} \end{cases}$$

Для любого натурального m положим $V_2(m)$ равным наибольшей степени числа два, деля-

щей m.

Лемма 3.1. *Имеет место неравенство*

$$V_2\left(\frac{4^{d+\mu+t}}{d+\mu+t}\right) \geq n,$$

для любого целого $t \geq 1$.

Доказательство. Предположим сначала, что n нечетно и $\mu = \mu(f)$. Тогда неравенство в утверждении леммы эквивалентно

$$2(d+\mu+t) \geq V_2(d+\mu+t) + n \Longleftrightarrow 2(\mu+t) \geq V_2(d+\mu+t) + 1. \tag{3.1}$$

Если $V_2(d+\mu+t) = 0$, то (1), очевидно, выполнено.

Предположим, что (3.1) не выполнено, тогда $V_2(d+\mu+t) > 0$, и, следовательно, имеем

$$d+\mu+t = \beta 2^h; h, \beta \in \mathbb{Z},\ h \geq 1, \beta \text{ нечетное}.$$

Подставив это в (3.1), мы получим

$$h+1 > \beta 2^{h+1} - 2d \Longleftrightarrow d > \beta 2^h - \frac{h+1}{2}.$$

Поскольку $\beta 2^h > d$, отсюда следует, что

$$d = \beta 2^h - \Big(\frac{h+1}{2} - j\Big);\ 1 \leq j < \frac{h+1}{2},$$

откуда в силу максимальности f следует, что $f \geq h$.

Если $f > h$, то ясно, что $V_2(t) = h$, поэтому (3.1) выполнено, так как

$$2\mu + 2t \geq 2t \geq V_2(t) + 1 = h + 1.$$

Следовательно, имеем $h = f$, и тогда $t = (\beta - \alpha)2^f$, и, ввиду предположения, что (3.1) не выполнено, имеем

$$f + 1 > 2\mu + (\beta - \alpha)2^{f+1},$$

но легко видеть, что

$$2^{f+1} \geq f+1 \implies \beta = \alpha \implies t = 0,$$

что противоречит условию леммы.

Теперь рассмотрим случай, когда n нечетно и $\mu = 0 \neq \mu(f)$. В этом случае действуем, как и в предыдущем случае, в предположении, что $\mu = 0$, и получим

$$d = \beta 2^h - \Big(\frac{h+1}{2} - j\Big);\ 1 \leq j < \frac{h+1}{2},$$

что противоречит тому, что $d \neq \alpha 2^{\tilde{f}} + \mu(\tilde{f})$.

Наконец, предположим, что n четно. В этом случае мы имеем $\mu = \mu(f)$, так как если бы d было четным, то ясно, что $d = \alpha 2^{\tilde{f}}$, и если d было бы нечетным, то также ясно, что $d = \alpha 2^{\tilde{f}} - 1$, и

$$\frac{f + \varepsilon(n)}{2} = \frac{f+1}{2} \geq 1.$$

Дальнейшее доказательство этого случая полностью аналогично доказательству случая, когда n нечетно и $\mu = \mu(f)$. □

Теорема 3.1. *Существует многочлен $f(u) = a_{d+\mu}u^{d+\mu} + \cdots + a_2u^2 + u$ степени $d+\mu$ с целыми коэффициентами такой, что для любой образующей g подгруппы $(\mathbb{Z}/2^n\mathbb{Z})^{\times}_{1,1}$ при любом целом u справедливо сравнение*

$$ind_g(1+4u) \equiv \Lambda f(u) \mod 2^{n-2}. \tag{3.2}$$

Пусть $k = 4^{\tau}k'$, где $\tau, k' \in \mathbb{Z}$, u $(k',4) \leq 2$.

Тогда

$$a_k = \begin{cases} (-1)^{k+1}4^{k-1-\tau}x_k, & \text{если } (k',4) = 1, \\ (-1)^{k+1}\frac{4^{k-1-\tau}}{2}x_k, & \text{если } (k',4) = 2 \end{cases} \tag{3.3}$$

(очевидно, a_k можно брать с точностью до кратных 2^{n-2}), где x_k есть решение сравнения

$$\begin{cases} k'x_k \equiv 1 \mod 2^{n-2}, & \text{если } (k',4) = 1, \\ \frac{k'}{2}x_k \equiv 1 \mod 2^{n-2}, & \text{если } (k',4) = 2, \end{cases}$$

а Λ — решение сравнения

$$ind_g(5) \equiv \Lambda f(1) \mod 2^{n-2},$$

причем сравнение разрешимо и Λ *нечетное.*

Доказательство. Поскольку подгруппа $(\mathbb{Z}/2^n\mathbb{Z})^\times_{1,1}$ является циклической порядка 2^{n-2} и порождается 5 (см., например, [10], стр. 218), то ясно, что $\mathrm{ind}_g(5)$ является нечётным числом.

Для любого 2-адического целого числа u, сходится ряд

$$\sum_{k=1}^{\infty}(-1)^{k+1}\frac{(4u)^k}{k} = \ln(1+4u).$$

Кроме того, для любых двух таких целых чисел u_1 и u_2 имеем

$$\ln\big((1+4u_1)(1+4u_2)\big) = \ln(1+4u_1) + \ln(1+4u_2).$$

По лемме 3.1, если мы определим

$$\overline{F}(1+4u) = \sum_{k=1}^{d}(-1)^{k+1}\frac{(4u)^k}{k},$$

то имеет место тождество

$$\overline{F}((1+4u_1)(1+4u_2)) \equiv \overline{F}(1+4u_1) + \overline{F}(1+4u_2) \mod 2^n.$$

Следовательно, определим

$$\hat{F}(1+4u) = \frac{\overline{F}(1+4u)}{4} = \sum_{k=1}^{d}(-1)^{k+1}\frac{4^{k-1}u^k}{k},$$

и получим

$$\hat{F}((1+4u_1)(1+4u_2)) \equiv \hat{F}(1+4u_1) + \hat{F}(1+4u_2) \mod 2^{n-2}. \tag{3.4}$$

Мы можем заменить каждый коэффициент $\hat{F}$ по модулю 2^{n-2} целым числом, и сделаем это следующим образом.

Пусть a_k определено как в (3.3).

Если $(k', 4) = 1$, то

$$a_k = (-1)^{k+1}4^{k-1-\tau}x_k \equiv (-1)^{k+1}\frac{4^{k-1-\tau}}{k'} \equiv (-1)^{k+1}\frac{4^{k-1}}{k} \mod 2^{n-2}.$$

Если $(k', 4) = 2$, то

$$a_k = (-1)^{k+1}\frac{4^{k-1-\tau}}{2}x_k \equiv (-1)^{k+1}\frac{4^{k-1-\tau}}{k'} \equiv (-1)^{k+1}\frac{4^{k-1}}{k} \mod 2^{n-2},$$

и a_k — целое число, поскольку $k - 1 - \tau \geq 1$. Очевидно, что $a_1 = 1$.
Определим

$$f(u) = F(1 + 4u) = u + a_2u^2 + \cdots + a_{n-2}u^{n-2},$$

где ясно, что для всех u имеем

$$F(1 + 4u) \equiv \hat{F}(1 + 4u) \mod 2^{n-2}. \tag{3.5}$$

Из определения легко проверить, что коэффициенты $a_2, \ldots, a_{n-2}$ четны, и поэтому

$$F(5) \equiv 1 \mod 2 \implies F(5) \not\equiv 0 \mod 2.$$

Отсюда следует разрешимость сравнения

$$\mathrm{ind}_g(5) \equiv \Lambda F(5) \mod 2^{n-2},$$

решение которого обозначим через Λ.
Поскольку $F(5) \not\equiv 0 \mod 2$ и $\mathrm{ind}_g(5) \not\equiv 0 \mod 2$, то Λ нечетное.
Для $s = 1, 2, \ldots, 2^{n-2}$, имеем

$$\mathrm{ind}_g(5)s \equiv \Lambda sF(5) \mod 2^{n-2}.$$

Это, учитывая мультипликативные свойства обеих сторон по (3.4) и (3.5), означает, что

$$\mathrm{ind}_g(5^s) \equiv \Lambda F(5^s) \mod 2^{n-2}. \tag{3.6}$$

Поскольку 5 является порождающим подгруппы $(\mathbb{Z}/2^n\mathbb{Z})^\times_{1,1}$, то элементы 5^s для $s = 1, 2, \ldots, 2^{n-2}$ пробегают всю подгруппу $(\mathbb{Z}/2^n\mathbb{Z})^\times_{1,1}$, и, следовательно, (3.2) следует из (3.6):

$$\mathrm{ind}_g(1+4u) \equiv \Lambda F(1+4u) \equiv \Lambda f(u) \mod 2^{n-2}.$$

□

3.3 Оценки некоторых сумм характеров по модулю степени простого числа 2

В данном разделе мы действуем, как в [26], используя оценку И.М. Виноградова для получения оценок сумм характеров по модулю 2^n степени, не меньше 2^{n-2}.

Для полноты изложения приведем здесь оценку И.М. Виноградова ([6], стр. 389).

Теорема 3.2. ***(И.М. Виноградов).***

Пусть $m, L \in \mathbb{Z}$ с $m, L > 0$ и $f(u)$ — многочлен степени $D+1$ с вещественными коэффициентами такой, что некоторый коэффициент $b_{d'}$ удовлетворяет

$$b_{d'} = \frac{a}{q} + \frac{\theta}{q^2};\ (a,q) = 1, |\theta| < 1.$$

Полагая

$$\tau = \begin{cases} \frac{\ln q}{\ln L} \ \textit{если}\ 1 < q \le L, \\ 1 \ \textit{если}\ L < q \le L^{d'-1}, \\ d' - \frac{\ln q}{\ln L} \ \textit{если}\ L^{d'-1} < q < L^{d'}, \end{cases} \qquad \tilde{l} = \ln\Big(\frac{12(d+\mu-1)(d+\mu)}{\tau}\Big),\ \ \rho = \frac{1}{3D^2\tilde{l}},$$

то имеет место оценка

$$\Big|\sum_{u=1}^{L} e^{2\pi i m f(u)}\Big| < (8D)^{D\tilde{l}/2} m^{2\rho} L^{1-\tau\rho}.$$

Теорема 3.3. *Пусть χ — любой характер по модулю 2^n, степень которого не меньше 2^{n-2}.*

Тогда имеет место оценка

$$\Big|\sum_{u=1}^{L} \chi(u)\Big| < 1 + 2\big(8(d+\mu-1)\big)^{\frac{(d+\mu-1)}{2}\tilde{l}}\Big(\frac{L+1}{4}\Big)^{1-\frac{\tau}{3(d+\mu-1)^2\tilde{l}}}.$$

Доказательство. Известно ([10], стр. 218), что

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{n-2}\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/2^n\mathbb{Z})^\times_{1,1}.$$

В частности, знаем, что любой элемент $u \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ можно однозначно представить как

$$u \equiv (-1)^{\frac{u-1}{2}} g^{\mathrm{ind}_g((-1)^{\frac{u-1}{2}}u)}, \tag{3.7}$$

где g — любой образующий подгруппы $(\mathbb{Z}/2^n\mathbb{Z})^\times_{1,1}$ и $\mathrm{ind}_g(\cdot)$ – соответствующая функция индекса, так что $0 \le \mathrm{ind}_g\big((-1)^{\frac{u-1}{2}}u\big) < 2^{n-2}$ (см., например, [10], стр. 218).

Более того, мы знаем, что

$$\chi(u) = \chi_1(u)\chi_2(u),$$

где χ_1 — характер группы $\mathbb{Z}/2\mathbb{Z}$, а χ_2 — характер группы $\mathbb{Z}/2^{n-2}\mathbb{Z}$ (см., например, [10], стр. 219).

В частности, из (3.7) видим, что

$$\chi_2(u) = e^{2\pi i m \frac{\mathrm{ind}_g((-1)^{\frac{u-1}{2}}u)}{2^{n-2}}}, \tag{3.8}$$

где $m \in \mathbb{Z}$ — нечетное целое число, так как степень χ не меньше 2^{n-2}.

Поэтому, полагая $L' = \left\lfloor \frac{L-1}{2} \right\rfloor$, запишем

$$\sum_{u=1}^{L} \chi(u) = \sum_{u=1}^{L} \chi_1(u)\chi_2(u) = \sum_{u=0}^{L'} \chi_1(1+2u)\chi_2(1+2u) =$$

$$= 1 + \sum_{u=1}^{L_1} \chi_2(1+4u) \pm \sum_{u=1}^{L_2} \chi_2(-1+4u),$$

где знак равен $+1$, если χ_1 — главный характер, и -1 в противном случае, и $L_1 = \left\lfloor \frac{L'}{2} \right\rfloor, L_2 = \left\lfloor \frac{L'+1}{2} \right\rfloor$.

По (3.8) и теореме 3.1 имеем

$$\sum_{u=1}^{L_1} \chi_2(1+4u) = \sum_{u=1}^{L_1} e^{2\pi i m \frac{\mathrm{ind}_g(1+4u)}{2^{n-2}}} = \sum_{u=1}^{L_1} e^{2\pi i m \frac{\Lambda f(u)}{2^{n-2}}}.$$

Рассмотрим многочлен

$$F(u) = \frac{m\Lambda}{2^{n-2}} f(u) = \sum_{j=1}^{d+\mu} b_j u^j.$$

Если n нечетно и d нечетно, то берем $d' = d$, и тогда видим, что

$$V_2(b_d) = 2(d-1) - V_2(d) - n + 2 = -1,$$

так что

$$b_d = \frac{r}{2};\ r \in \mathbb{Z}, r \text{ нечетное}.$$

Если n нечетно и d четно, то берем $d' = d - 1$, и тогда видим, что

$$V_2(b_{d-1}) = 2(d-2) - V_2(d-1) - n + 2 = -3,$$

так что

$$b_{d-1} = \frac{r}{8};\ r \in \mathbb{Z}, r \text{ нечетное}.$$

Если n четно и d нечетно, то берем $d' = d$, и тогда видим, что

$$V_2(b_d) = 2(d-1) - V_2(d) - n + 2 = -2,$$

так что

$$b_d = \frac{r}{4};\ r \in \mathbb{Z}, r \text{ нечетное}.$$

Если n четно и d четно, то берем $d' = d - 1$, и тогда видим, что

$$V_2(b_{d-1}) = 2(d-2) - V_2(d-1) - n + 2 = -4,$$

так что

$$b_{d-1} = \frac{r}{16};\ r \in \mathbb{Z}, r \text{ нечетное}.$$

Во всех случаях мы применяем теорему 3.2 (оценка И.М. Виноградова) к $b_{d'}$, чтобы получить

$$\Big|\sum_{u=1}^{L_1}\chi_2(1+4u)\Big| = \Big|\sum_{u=1}^{L_1}e^{2\pi iF(u)}\Big| < \big(8(d+\mu-1)\big)^{\frac{(d+\mu-1)}{2}\tilde{l}}L_1^{1-\frac{\tau}{3(d+\mu-1)^2\tilde{l}}}. \tag{3.9}$$

Теперь по (3.8) знаем, что

$$\chi_2(-1+4u) = e^{2\pi im\frac{\mathrm{ind}g(1-4u)}{2^{n-2}}} = e^{2\pi im\frac{\mathrm{ind}g(1+4(2^{n-2}-u))}{2^{n-2}}},$$

так что по теореме 3.1 получим

$$\chi_2(-1+4u) = e^{2\pi im\frac{\Lambda f(2^{n-2}-u)}{2^{n-2}}} = e^{2\pi im\frac{\Lambda f(-u)}{2^{n-2}}},$$

где второе равенство следует из того, что f имеет целые коэффициенты.
Поэтому аналогично имеем

$$\Big|\sum_{u=1}^{L_2}\chi_2(-1+4u)\Big| < \big(8(d+\mu-1)\big)^{\frac{(d+\mu-1)}{2}\tilde{l}}L_2^{1-\frac{\tau}{3(d+\mu-1)^2\tilde{l}}}. \tag{3.10}$$

Используя две оценки в (3.9) и (3.10) и очевидные неравенства $L_1, L_2 \le \frac{L+1}{4}$, находим

$$\Big|\sum_{u=1}^{L}\chi(u)\Big| < 1 + 2\big(8(d+\mu-1)\big)^{\frac{(d+\mu-1)}{2}\tilde{l}}\Big(\frac{L+1}{4}\Big)^{1-\frac{\tau}{3(d+\mu-1)^2\tilde{l}}}.$$

□

Предложение 3.1. *Максимальное значение суммы*

$$\sum_{u=1}^{L}\chi(u)$$

достигается для некоторого $L \le 2^{n-1}$.

Доказательство. Поскольку χ периодичен с периодом 2^n, мы знаем, что

$$\sum_{u=1}^{2^n}\chi(u) = 0,$$

и поэтому максимальное значение суммы достигается для некоторого $L \le 2^n$.
Для любого нечетного u, поскольку $n \ge 3$, то в силу (3.8) имеем

$$\chi(u+2^{n-1}) = \chi_1(u+2^{n-1})\chi_2(u+2^{n-1}) = \chi_1(u)e^{2\pi i m\frac{\mathrm{ind}_g((-1)^{\frac{u-1}{2}}(u+2^{n-1}))}{2^{n-2}}}, \tag{3.11}$$

где последнее неравенство следует из того, что $\chi_1(u)$ зависит только от значения u по модулю 4.

Кроме того, у нас есть

$$\mathrm{ind}_g(1+2^{n-1}) = 2^{n-3},$$

что, поскольку u нечетно, дает

$$\mathrm{ind}_g((-1)^{\frac{u-1}{2}}(u+2^{n-1})) = \mathrm{ind}_g((-1)^{\frac{u-1}{2}}u(1+2^{n-1})) = \mathrm{ind}_g((-1)^{\frac{u-1}{2}}u) + 2^{n-3},$$

и, поскольку $n \geq 3$, подстановка в (3.11) дает

$$\chi(u+2^{n-1}) = -\chi_1(u)e^{2\pi i m\frac{\mathrm{ind}_g((-1)^{\frac{u-1}{2}}u)}{2^{n-2}}} = -\chi(u).$$

Поэтому максимальное значение суммы достигается для некоторого $L \leq 2^{n-1}$. □

Непосредственным следствием теоремы 3 является следующий результат.

Следствие 3.1. *Существуют вещественные константы c_1, c_2 такие, что для любого $U \in \mathbb{Z}$ выполняется неравенство*

$$\Big|\sum_{u=U+1}^{U+L}\chi(u)\Big| \leq e^{c_1 d(\ln d)^2}2^{\frac{2c_2}{d^3\ln d}}L^{1-\frac{c_2}{d^3\ln d}}.$$

Доказательство. По определению τ видим, что $\tau \leq 1$. Более того, по предложению 3.1 имеем, что можно взять $L \leq 2^{n-1}$. Откуда следует, что $\tau \geq \frac{1}{n-1}$.

Кроме того, многочлен $F(u)$ в доказательстве теоремы 3.3, к которому применяется оценка И.М. Виноградова, имеет рациональные коэффициенты, а, следовательно, и многочлен $F(u-U)$ имеет рациональные коэффициенты. Поэтому оценка И.М. Виноградова применима к $F(u-U)$ (хотя и с другим значением параметра τ).

Повторяя рассуждения теоремы 3.3 и используя приведенные выше неравенства для τ, находим, что следствие теперь выводится простыми вычислениями. □

3.4 Мультипликативная структура приведенных систем вычетов по модулю степени простого идеала, не делящего дифференту

В этом разделе описана мультипликативная структура приведенных систем вычетов по модулю идеала, равного степени простого идеала, не делящего дифференту. Как было сказано во введении, результаты этого раздела представляют собой частный случай теоремы 4 в [27].

Лемма 3.2. *Пусть P — простой идеал, и $N(P) = q^r$, где q — простое число, и пусть $n \geq 1$ — целое число. Тогда число элементов $(R/P^n)^\times$ равно*

$$|(R/P^n)^\times| = \Phi(P^n) = q^{r(n-1)}(q^r - 1),$$

и

$$(R/P^n)^\times \cong (R/P^n)_1^\times \oplus (R/P)^\times.$$

Более того, имеем

$$|(R/P^n)_1^\times| = q^{r(n-1)}.$$

Доказательство. Пусть $(R/P)^\times = \{a_1, \ldots, a_{q^r-1}\}$. Для первого утверждения леммы действуем индукцией по n. Если $n = 1$, то R/P — поле, и

$$|R/P| = N(P) = q^r \implies \Phi(P) = |(R/P)^\times| = q^r - 1. \tag{3.12}$$

Для любого элемента $u \in (R/P^n)^\times$ видим, что

$$u + a_i P^{n-1} \equiv u \mod P^{n-1},\ u + a_i P^{n-1} \not\equiv u \mod P^n;\ 1 \leq i \leq q^r - 1.$$

И наоборот, если $u \neq v \in (R/P^n)^\times$ и

$$u \equiv v \mod P^{n-1},$$

то

$$v \equiv u + a_i P^{n-1} \mod P^n$$

для некоторого a_i.

Следовательно, каждому элементу u из $(R/P^{n-1})^\times$ соответствует ровно q^r элементов из $(R/P^n)^\times$ (именно сам u и $\{u + a_i P^{n-1}\}_{i=1}^{q^r-1}$).

Это дает тождество

$$\Phi(P^n) = q^r \Phi(P^{n-1}),$$

что вместе с (3.12) доказывает первое утверждение леммы.

Для второго утверждения пусть $u \in (R/P^n)^\times$ такое, что $u \equiv a_i \mod P$. Тогда

$$u a_i^{-1} \equiv 1 \mod P \implies u a_i^{-1} \in (R/P^n)_1^\times,$$

и поэтому существует $u' \in (R/P^n)_1^\times$ такой, что $u \equiv u' a_i \mod P^n$.

Предположим, что имеем два таких представления u, так что $u' a_i \equiv u'' a_j \mod P^n$. Поскольку $u', u'' \in (R/P^n)_1^\times$, то, очевидно, имеем $i = j$, что, в свою очередь, означает, что $u' \equiv u''$ mod P^n. Это доказывает единственность представления, а значит, и разложение в прямую сумму, что и есть второе утверждение леммы.

Окончательное утверждение леммы следует из (3.12) подсчетом размерностей при разложении в прямую сумму. □

Лемма 3.3. *Пусть P — простой идеал, и $N(P) = q^r$, где q — простое число такое, что $q \nmid \Delta$. Тогда*

$$q \in P,\ q \notin P^2,\ P \cap \mathbb{Z} = (q).$$

Доказательство. Фактор-кольцо R/P — поле, поскольку R — область Дедекинда (см., например, [4], стр. 437). Поскольку $|R/P| = q^r$, мы видим, что это конечное поле, и поэтому $R/P \cong \mathbb{F}_{q^r}$. Следовательно, q есть нулевой элемент ($q \equiv 0$) в R/P, и так

$$q \equiv 0 \mod P \implies q \in P.$$

Поскольку $q \nmid \Delta$, q является неразветвленным элементом, и поэтому q разлагается в произведение

$$q = P\prod_{j=1}^{J} P_j,$$

для некоторых различных простых идеалов $P_j \neq P$. Отсюда видим, что $q \notin P^2$.
Известно, что $P \cap \mathbb{Z}$ — простой идеал в $\mathbb{Z}$ (см., например, [4], стр. 427) так что

$$P \cap \mathbb{Z} = (q'),$$

для некоторого простого числа $q' \in \mathbb{Z}$.
Поскольку $q \in P \cap \mathbb{Z}$, имеем, что

$$\exists m \in \mathbb{Z};\ q = q'm \implies q' = q$$

так как q и q' — простые. □

Предложение 3.2. *Пусть q — простое число и $h \geq 1$ — целое число. Пусть $1 \leq n < q$ и $1 \leq j \leq nq^h$ — целые числа. Тогда*

$$V_q\left(\binom{nq^h}{j}\right) = h - V_q(j).$$

Доказательство. Поскольку $n < q$, то $j \leq nq^h < q^{h+1}$, и поэтому для $1 \leq l \leq j$ имеем

$$V_q(nq^h - l) = V_q(l).$$

Более того, имеем

$$\binom{nq^h}{j} = \frac{1}{j!}\prod_{l=0}^{j-1}(nq^h - l) \implies V_q\left(\binom{nq^h}{j}\right) = h + \sum_{l=1}^{j-1} V_q(l) - \sum_{l=1}^{j} V_q(l) = h - V_q(j).$$

□

Теорема 3.4. *Пусть P — простой идеал, и $N(P) = q^r$, где q — нечетное простое число, такое, что $q \nmid \Delta$, и пусть $n \geq 1$ — целое число.*

Тогда имеем разложение в прямую сумму

$$(R/P^n)_1^\times \cong \bigoplus_{j=1}^{r} \mathbb{Z}/q^{n-1}\mathbb{Z},$$

где группы справа — аддитивные.

Доказательство. Сначала покажем, что любой элемент $u \in (R/P^n)_1^\times$ однозначно выражается как

$$u \equiv 1 + q\pi \mod P^n,\ \pi \in R/P^{n-1}.$$

Имеем, что

$$1 + q\pi' \equiv 1 + q\pi'' \mod P^n \implies \pi' \equiv \pi'' \mod P^{n-1},$$

поскольку $q \in P$ по лемме 3.3, а значит, элементы $1 + q\pi$ не сравнимы между собой по модулю P^{n-1}, что и доказывает единственность разложения.

Кроме того, по лемме 3.2 имеем

$$|(R/P^n)_1^\times| = q^{r(n-1)} = |R/P^{n-1}|,$$

и поэтому элементы $1 + q\pi$ охватывают $(R/P^n)_1^\times$, что доказывает существование разложения.

Теперь покажем, что любой элемент $u \in (R/P^n)_1^\times$ такой, что $u \not\equiv 1 \mod P^2$, имеет порядок $\mathrm{ord}(u) = q^{n-1}$.

Из представления $u \equiv 1 + q\pi \mod P^n$, находим

$$u \not\equiv 1 \mod P^2 \iff \pi \not\equiv 0 \mod P. \tag{3.13}$$

По лемме 3.2 имеем $\mathrm{ord}(u) = q^h$ для некоторого $h \geq 0$.

Теперь вычислим

$$(1 + q\pi)^{q^{n-2}} = 1 + \sum_{j=1}^{q^{n-2}} \binom{q^{n-2}}{j} q^j \pi^j. \tag{3.14}$$

Для слагаемых с $j \geq 2$ в (3.14), применение предложения 3.2 дает

$$V_q\left(\binom{q^{n-2}}{j}\right) = n-2-V_q(j) \implies V_q\left(\binom{q^h}{j}q^j\right) = n-2-V_q(j)+j.$$

Поскольку q нечетно, $q \geq 3$, и поэтому

$$j - V_q(j) \geq 2 \implies V_q\left(\binom{q^h}{j}q^j\right) \geq n \implies \binom{q^h}{j}q^j \in P^n. \tag{3.15}$$

Из (3.14) и (3.15) получим, что

$$(1+q\pi)^{q^{n-2}} \equiv 1 + q^{n-1}\pi \mod P^n.$$

Так как $q \nmid \Delta$ и $\pi \not\equiv 0 \mod P$, то имеем

$$q^{n-1}\pi \not\equiv 0 \mod P^n \implies (1+q\pi)^{q^{n-2}} \not\equiv 1 \mod P^n \implies \operatorname{ord}(u) > q^{n-2}. \tag{3.16}$$

Аналогичное рассуждение показывает, что

$$(1+q\pi)^{q^{n-1}} \equiv 1 \mod P^n,$$

откуда согласно (3.16) следует, что $\operatorname{ord}(u) = q^{n-1}$.

Более того, аналогично, если $u \equiv 1 \mod P^2$, то $\operatorname{ord}(u) < q^{n-1}$.

Таким образом, мы показали, что максимальный порядок элемента $(R/P^n)^\times$ равен q^{n-1} и что элементы этого порядка — в точности те элементы, которые удовлетворяют условию $u \not\equiv 1 \mod P^2$, так что

$$u \not\equiv 1 \mod P^2 \iff \operatorname{ord}(u) = q^{n-1}, \tag{3.17}$$

и

$$u \equiv 1 \mod P^2 \iff \operatorname{ord}(u) < q^{n-1}. \tag{3.18}$$

Выбрав элемент $u_1 \equiv 1+q\pi_1 \mod P^n$ с $\operatorname{ord}(u_1) = q^{n-1}$, обозначим подгруппу, порожденную u_1, как G_1, и тогда имеем очевидный изоморфизм $G_1 \cong \mathbb{Z}/q^{n-1}\mathbb{Z}$.

По основной теореме о конечных абелевых группах имеем

$$(R/P^n)_1^\times \cong G_1 \oplus G_1' \cong \mathbb{Z}/q^{n-1}\mathbb{Z} \oplus G_1';\ |G_1'| = q^{(r-1)(n-1)}.$$

Предположим индуктивно, что у нас есть представление

$$(R/P^n)_1^\times \cong G_1 \oplus \cdots \oplus G_t \cong \left(\bigoplus_{j=1}^{t} \mathbb{Z}/q^{n-1}\mathbb{Z} \right) \oplus G'_t.$$

Мы хотим показать, что если $t < r$, то подгруппа G'_t содержит элемент порядка q^{n-1}.

Рассуждая от противного, предположим, что G'_t не содержит такого элемента. Следовательно, поскольку максимальный порядок элемента $(R/P^n)_1^\times$ равен q^{n-1}, то имеем $\mathrm{ord}(u) < q^{n-1}$ для всех $u \in G'_t$.

Подсчитаем количество элементов в $(R/P^n)_1^\times$ с $\mathrm{ord}(u) = q^{n-1}$ двумя способами, чтобы получить искомое противоречие.

С одной стороны, (3.17) показывает, что элементы порядка q^{n-1} — в точности те, которые удовлетворяют условию $u \not\equiv 1 \mod P^2$. Согласно (3.13) число этих элементов равно

$$|R/P^{n-1}| - |R/P^{n-2}| = q^{r(n-1)} - q^{r(n-2)} = q^{r(n-2)}(q^r - 1). \tag{3.19}$$

С другой стороны, из элементарных свойств прямых сумм известно, что порядок элемента есть наименьшее общее кратное порядков его компонентов, и поскольку порядок любого элемента $(R/P^n)_1^\times$ имеет вид q^h, видим, что порядок элемента равен максимальному порядку его компонент.

Подсчитаем количество элементов порядка q^{n-1}, рассматривая порядки их компонент в $G_1, \ldots, G_t$ и G'_t.

Поскольку предполагалось, что G'_t не содержит ни одного элемента порядка q^{n-1}, мы видим, что компоненты порядка q^{n-1} могут появляться только в подгруппах $G_1, \ldots, G_t$.

Нам нужно подсчитать количество различных способов, которыми мы можем сначала выбрать упорядоченное подмножество из $k \le t$ элементов, такое, что каждый элемент берется из набора $\Phi(q^{n-1})$ элементов, а затем выбираем оставшиеся $t+1-k$ компоненты ($t-k$ компоненты в остальных слагаемых вида $\mathbb{Z}/q^{n-1}\mathbb{Z}$ и одну компонента в G'_t), для всех $1 \le k \le t$.

Для этого сначала посчитаем все элементы, G_1-компонента которых имеет порядок q^{n-1}, затем посчитаем все элементы, G_2-компонента которых имеет порядок q^{n-1}, но чей G_1-компонент имеет порядок, строго меньше q^{n-1} (чтобы избежать повторения) и т. д. до подсчета количество элементов, чей компонент G_t- имеет порядок q^{n-1}, но чьи $G_1, \ldots, G_{t-1}-$компоненты имеют порядок, строго меньше q^{n-1}.

Из изоморфизма $G_i \cong \mathbb{Z}/q^{n-1}\mathbb{Z}$ ясно, что число элементов G_i порядка q^{n-1} равно $\Phi(q^{n-1})$,

так что, как легко видеть, что искомое число равно

$$\Phi(q^{n-1})q^{(r-1)(n-1)} + \Phi(q^{n-1})q^{(r-1)(n-1)-1} + \cdots + \Phi(q^{n-1})q^{(r-1)(n-1)-(t-1)} =$$
$$= \Phi(q^{n-1})q^{(r-1)(n-1)-(t-1)}(1 + q + \cdots + q^{t-1}) = q^{r(n-1)-t}(q^t - 1). \tag{3.20}$$

Сравнивая два значения в (3.19) и (3.20), мы видим, что

$$q^{r(n-1)-t}(q^t - 1) = q^{r(n-2)}(q^r - 1) \implies t = r,$$

что противоречит предположению, что $t < r$.

Следовательно, мы видим, что G'_t всегда содержит элемент порядка q^{n-1}, и поэтому индуктивно получим

$$(R/P^n)_1^\times \cong \bigoplus_{k=1}^{r} G_k \cong \left(\bigoplus_{j=1}^{r} \mathbb{Z}/q^{n-1}\mathbb{Z} \right).$$

□

Следствие 3.2. *Пусть P — простой идеал, и $N(P) = q^r$, где q — нечетное простое число, такое, что $q \nmid \Delta$, и пусть $n \geq 1$ — целое число.*

Тогда имеем разложение в прямую сумму

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r} \mathbb{Z}/q^{n-1}\mathbb{Z} \right) \oplus (R/P)^\times \cong \left(\bigoplus_{j=1}^{r} \left(\mathbb{Z}/q^n\mathbb{Z} \right)_1^\times \right) \oplus (R/P)^\times.$$

В соответствии со следствием 3.2, каждое $u \in (R/P^n)^\times$ выражается однозначно в виде

$$u = (a, u_1, \ldots, u_r);\ a \in (R/P)^\times,\ 0 \leq u_j < q^{n-1}.$$

Называем разложение выше стандартным разложением u.

Следствие 3.3. *Пусть P — простой идеал, и $N(P) = q^r$, где q — нечетное простое число, такое, что $q \nmid \Delta$, и пусть $n \geq 1$ — целое число. Тогда каждый элемент χ группы характеров $(R/P^n)^\times$ однозначно выражается как*

$$\chi(u) = e^{2\pi i \left(\sum_{j=1}^{r} \frac{m_j ind(1+qu_j)}{q^{n-1}} \right)} \chi_P(a),$$

где χ_P — характер группы $(R/P)^\times$, а m_j — целые числа, такие, что $1 \le m_j \le q^{n-1}$, и ind обозначает соответствующую функцию индекса в соответствующей подгруппе $(\mathbb{Z}/q^n\mathbb{Z})_1^\times$ в разложении в прямую сумму следствия 3.2 (см., например, [10], стр. 219).

Теорема 3.5. *Пусть P — простой идеал, и $N(P) = 2^r$, где $2 \nmid \Delta$, и пусть $n \ge 2$ — целое число. Тогда имеем разложение в прямую сумму*

$$(R/P^n)_1^\times \cong \left(\bigoplus_{j=1}^{r-1} \mathbb{Z}/2^{n-1}\mathbb{Z} \right) \oplus \mathbb{Z}/2^{n-2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

где группы справа — аддитивные.

Доказательство. Как и при доказательстве теоремы 3.4, мы видим, что любой элемент $u \in (R/P^n)_1^\times$ однозначно выражается как

$$u \equiv 1 + 2\pi \mod P^n,\ \pi \in R/P^{n-1}.$$

Аналогично (3.13) при доказательстве теоремы 3.4 видим, что

$$u \not\equiv 1 \mod P^s \iff \pi \not\equiv 0 \mod P^{s-1}, \tag{3.21}$$

для любого $2 \le s \le n$.

Для всех $u \in (R/P^n)_1^\times$ по лемме 3.2 имеем $\mathrm{ord}(u) = 2^h$ для некоторого $h \ge 0$, и, как это было сделано при доказательстве теоремы 3.4, аналогично видно, что $\mathrm{ord}(u) \le 2^{n-1}$.

Сначала покажем, что для любого элемента u имеем

$$\mathrm{ord}(u) = 2^{n-1} \iff u \not\equiv 1 \mod P^2,\ \pi \not\equiv 1 \mod P. \tag{3.22}$$

Для любого $h \ge 0$ пишем

$$(1 + 2\pi)^{2^h} = 1 + \sum_{j=1}^{2^h} \binom{2^h}{j} 2^j \pi^j. \tag{3.23}$$

Взяв $h = n - 2$ и применив предложение 3.2 к слагаемым в (3.23) с $j \ge 3$, получим

$$j - V_2(j) \ge 2 \implies V_2\left(\binom{2^{n-2}}{j} 2^j \right) \ge n \implies \binom{2^{n-2}}{j} q^j \in P^n,$$

что дает

$$(1+2\pi)^{2^{n-2}} \equiv 1 + 2^{n-1}\pi + 2^{n-1}(2^{n-1}-1)\pi^2 \mod P^n,$$

и поэтому

$$\operatorname{ord}(u) = 2^{n-1} \iff 2^{n-1}\pi + 2^{n-1}(2^{n-1}-1)\pi^2 \equiv 0 \mod P^n \iff$$

$$\iff \pi + (2^{n-1}-1)\pi^2 \equiv 0 \mod P \iff \pi - \pi^2 \equiv 0 \mod P. \tag{3.24}$$

Если условия (3.22) выполнены, то (3.21) показывает, что $\pi \not\equiv 0 \mod P$, а значит (3.24) показывает, что $\operatorname{ord}(u) = 2^{n-1}$.

Если какое-либо из условий в (3.22) не выполняется, то (3.21) показывает, что либо $\pi \equiv 0 \mod P$, либо $\pi \equiv 1 \mod P$, и в обоих случаях (3.24) показывает, что что $\operatorname{ord}(u) < 2^{n-1}$.

Сначала рассмотрим слагаемые, соответствующие $\mathbb{Z}/2^{n-1}\mathbb{Z}$ в формулировке теоремы.

Если $r = 1$, то либо $\pi \equiv 0 \mod P$, либо $\pi \equiv 1 \mod P$, так что условия (3.22) не могут быть выполнены, и поэтому в этом случае элементов порядка 2^{n-1} нет, что соответствует тому, что показатель степени $\mathbb{Z}/2^{n-1}\mathbb{Z}$ в прямой сумме в формулировке теоремы равен $r - 1 = 0$.

Предположим, что $r \geq 2$. Будем действовать так же, как при доказательстве теоремы 3.4.

Из (3.22) знаем, что существует элемент $u_1 = 1+2\pi_1$ с $\operatorname{ord}(u_1) = 2^{n-1}$. Обозначим подгруппу, порожденную u_1, как G_1, и тогда имеем очевидный изоморфизм $G_1 \cong \mathbb{Z}/2^{n-1}\mathbb{Z}$.

По основной теореме о конечных абелевых группах имеем

$$(R/P^n)_1^\times \cong G_1 \oplus G_1' \cong \mathbb{Z}/2^{n-1}\mathbb{Z} \oplus G_1';\ |G_1'| = 2^{(r-1)(n-1)}.$$

Предположим индуктивно, что у нас есть представление

$$(R/P^n)_1^\times \cong G_1 \oplus \cdots \oplus G_t \cong \left(\bigoplus_{j=1}^{t} \mathbb{Z}/2^{n-1}\mathbb{Z}\right) \oplus G_t'. \tag{3.25}$$

Мы хотим показать, что если $t < r-1$, то подгруппа G_t' содержит элемент порядка 2^{n-1}.

Рассуждая от противного, предположим, что G_t' не содержит такого элемента. Следовательно, поскольку максимальный порядок элемента $(R/P^n)_1^\times$ равен 2^{n-1}, то имеем $\operatorname{ord}(u) < 2^{n-1}$ для всех $u \in G_t'$.

Подсчитаем количество элементов в $(R/P^n)_1^\times$ с $\operatorname{ord}(u) = 2^{n-1}$ двумя способами, чтобы получить искомое противоречие.

С одной стороны, (3.21) и (3.22) показывают, что число элементов порядка 2^{n-1} равно

$$|R/P^{n-1}| - 2|R/P^{n-2}| = 2^{r(n-1)} - 2^{r(n-2)+1} = 2^{r(n-2)+1}(2^{r-1} - 1). \tag{3.26}$$

С другой стороны, совершенно аналогично доказательству теоремы 3.4, (3.25) показывает, что число этих элементов равно

$$2^{t(n-2)+r(n-1)-t(n-1)}(2^t - 1) = 2^{r(n-1)-t}(2^t - 1). \tag{3.27}$$

Сравнивая два значения в (3.26) и (3.27), мы видим, что

$$2^{r(n-1)-t}(2^t - 1) = 2^{r(n-2)+1}(2^{r-1} - 1) \implies t = r - 1,$$

что противоречит предположению, что $t < r - 1$.

Таким образом, мы получаем

$$(R/P^n)_1^\times \cong \left(\bigoplus_{j=1}^{r-1} \mathbb{Z}/2^{n-1}\mathbb{Z} \right) \oplus G'_{r-1};\ |G'_{r-1}| = 2^{n-1}. \tag{3.28}$$

Для завершения доказательства покажем, что $G'_{r-1} \cong \mathbb{Z}/2^{n-2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, показав, что G'_{r-1} содержит элемент порядка 2^{n-2}.

$$u \equiv 1 \mod P^3 \implies \operatorname{ord}(u) \leq 2^{n-3}. \tag{3.29}$$

Согласно (3.21) мы знаем, что $\pi \equiv 0 \mod P^2$, и поэтому, взяв $h = n - 3$ и применив предложение 3.2 к (3.23), получим, что

$$j - V_2(j) \geq 1 \implies V_2\left(\binom{2^{n-3}}{j} 2^j \pi^j \right) \geq n \implies \binom{2^{n-3}}{j} q^j \pi^j \in P^n,$$

что дает

$$(1 + 2\pi)^{2^{n-3}} \equiv 1 \mod P^n \implies \operatorname{ord}(u) \leq 2^{n-3}.$$

Теперь покажем, что

$$u \equiv 1 \mod P^2,\ u \not\equiv 1 \mod P^3 \implies \operatorname{ord}(u) = 2^{n-2}. \tag{3.30}$$

Действительно, (3.21) показывает, что $\pi \equiv 0 \mod P$, и поэтому, взяв $h = n - 2$ и применив

предложение 3.2 к (3.23), получим, что

$$(1+2\pi)^{2^{n-2}} \equiv 1 \mod P^n \implies \operatorname{ord}(u) \leq 2^{n-2}.$$

Теперь, взяв $h = n-3$ и применив предложение 3.2 к слагаемым в (3.23) с $j \geq 2$, получим, что

$$(1+2\pi)^{2^{n-3}} \equiv 1 + 2^{n-2}\pi \not\equiv 1 \mod P^n,$$

поскольку (3.21) показывает, что $\pi \not\equiv 0 \mod P^2$, и это завершает доказательство (3.30).

Теперь покажем, что если $n \geq 5$ и $u \not\equiv 1 \mod P^2$, то

$$\pi \equiv 3 \mod P^2 \iff \operatorname{ord}(u) < 2^{n-2}. \tag{3.31}$$

Если $\pi \not\equiv 1 \mod P$, то (3.22) показало, что $\operatorname{ord}(u) = 2^{n-1}$, и поэтому предполагаем, что $\pi \not\equiv 1 \mod P$.

Взяв $h = n-3$ и применив предложение 3.2 к (3.23), получим, что

$$(1+2\pi)^{2^{n-3}} \equiv 1 + 2^{n-2}\pi + 2^{n-2}(2^{n-3}-1)\pi^2 + 16\binom{2^{n-3}}{4}\pi^4 \mod P^n,$$

и поскольку $n \geq 5$, знаем, что $2^{n-3} \geq 4$, и поэтому $2^{n-3} \equiv 0 \mod P^2$, что, поскольку (3.21) показывает, что $\pi \not\equiv 0 \mod P$, дает

$$(1+2\pi)^{2^{n-3}} \equiv 1 \mod P^n \iff 1 - \pi - 2\pi^3 \equiv 0 \mod P. \tag{3.32}$$

Поскольку мы предположили, что $\pi \equiv 1 \mod P$, мы можем записать $\pi = 1 + \mu$ в (3.32), где $\mu \in P$, и тогда получим

$$(1+2\pi)^{2^{n-3}} \equiv 1 \mod P^n \iff 2 + 7\mu \equiv 0 \mod P^2 \iff \mu \equiv 2 \mod P^2, \tag{3.33}$$

где последняя эквивалентность следует из того, что $8 = 2^3 \equiv 0 \mod P^2$.

Теперь легко видеть, что (3.31) следует из (3.33) и (3.22).

При $n = 4$ аналогично получаем

$$\pi \equiv -1 \mod P^2 \iff \operatorname{ord}(u) < 2^{n-2}, \tag{3.34}$$

а для $n = 2, 3$ доказывать нечего.

Теперь посчитаем количество элементов порядка 2^{n-2} двумя способами, чтобы получить искомое противоречие.

С одной стороны, (3.22), (3.29), (3.30) и (3.31) если $n \geq 5$ или (3.34) если $n = 4$, мы видим, что это число равно

$$(2^{r(n-2)} - 2^{r(n-3)}) + (2^{r(n-2)} - 2^{r(n-3)}) = 2^{r(n-3)+1}(2^r - 1). \tag{3.35}$$

С другой стороны, аналогично доказательству теоремы 3.4 (но с учетом того, что мы посчитаем элементы порядка 2^{n-2}, а не 2^{n-1}), (3.28) показывает, что это число равно

$$2^{n-1}2^{(r-1)(n-3)}(2^{r-1} - 1) = 2^{r(n-3)+n-1}(2^r - 1). \tag{3.36}$$

Сравнение двух значений в (3.35) и (3.36) дает противоречие, которое показывает, что подгруппа G'_{r-1} содержит элемент порядка 2^{n-2}, тем самым завершая доказательство теоремы. □

Следствие 3.4. *Пусть P — простой идеал, и $N(P) = 2^r$, где $2 \nmid \Delta$, и пусть $n \geq 3$ — целое число.*

Тогда имеем разложение в прямую сумму

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r-1} \mathbb{Z}/2^{n-1}\mathbb{Z} \right) \oplus \mathbb{Z}/2^{n-2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus (R/P)^\times \cong$$

$$\cong \left(\bigoplus_{j=1}^{r-1} \left(\mathbb{Z}/2^{n+1}\mathbb{Z} \right)^\times_{1,1} \right) \oplus \left(\mathbb{Z}/2^n\mathbb{Z} \right)^\times_{1,1} \oplus \left(\mathbb{Z}/4\mathbb{Z} \right)^\times_{1,1} \oplus (R/P)^\times.$$

В соответствии со следствием 3.4 каждое $u \in (R/P^n)^\times$ выражается однозначно в виде

$$u = (a, u_1, \ldots, u_r, u_{r+1}),$$

с

$$a \in R/P^\times,\ 0 \leq u_1, \ldots, u_{r-1} < 2^{n-1},\ 0 \leq u_r < 2^{n-2},\ u_{r+1} \in \{0, 1\}.$$

Также называем разложение выше стандартным разложением u.

Следствие 3.5. *Пусть P — простой идеал, и $N(P) = 2^r$, где $2 \nmid \Delta$, и пусть $n \geq 2$ — целое число. Тогда каждый элемент χ группы характеров $(R/P^n)^\times$ однозначно выражается как*

$$\chi(u) = \pm e^{2\pi i\left(\sum_{j=1}^{r-1} \frac{m_j ind(1+2u_j)}{2^{n-1}}\right)} e^{2\pi i \frac{m_r ind(1+2u_r)}{2^{n-2}}} \chi_P(a),$$

где χ_P — характер группы $(R/P)^\times$, а m_j — целые числа, такие, что $1 \leq m_1, \ldots, m_{r-1} \leq 2^{n-1}, 1 \leq m_r \leq 2^{n-2}$, и где ind обозначает соответствующую функцию индекса в соответствующей подгруппе $(\mathbb{Z}/2^{n+1}\mathbb{Z})^\times_{1,1}$ или $(\mathbb{Z}/2^n\mathbb{Z})^\times_{1,1}$ в разложении в прямую сумму следствия 3.4 (см., например, [10], стр. 219).

3.5 Мультипликативная структура приведенных систем вычетов по модулю идеала, равного степени простого идеала, делящего дифференту

В данном разделе формулируются частично теоремы 2, 3 и 4 из [28].

Рассмотрим разветвленный простой идеал P с индексом ветвления $e \geq 2$. Для целого числа $n \geq 1$ положим $0 \leq n_e \leq e-1$ такое, что $n \equiv n_e \mod e$, и $1 \leq w \leq e$ такое, что $n-1 \equiv w \mod e$.

Теорема 3.6. *Пусть P — простой идеал, и $N(P) = q^r$, где q — нечетное простое число, такое, что $q|\Delta$, и пусть $n \geq 1$ — целое число. Предположим, что $\mathbb{K}$ не содержит приведенный корень из единицы степени q.*

Если $n \leq e$, то

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r(n-1)} \mathbb{Z}/q\mathbb{Z}\right) \oplus (R/P)^\times.$$

Если $n > e$ и $n \equiv 0 \mod e$, то

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r} \mathbb{Z}/q^{\frac{n}{e}-1}\mathbb{Z}\right) \oplus \left(\bigoplus_{j=1}^{r(e-1)} \mathbb{Z}/q^{\frac{n}{e}}\mathbb{Z}\right) \oplus (R/P)^\times.$$

Если $n > e$ и $n \equiv 1 \mod e$, то

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{re} \mathbb{Z}/q^{\frac{n-1}{e}}\mathbb{Z}\right) \oplus (R/P)^\times.$$

Если $n > e$ *и* $n_e \neq 0, 1$, *то*

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r(n_e-1)} \mathbb{Z}/q^{\frac{n-n_e}{e}+1}\mathbb{Z} \right) \oplus \left(\bigoplus_{j=1}^{r(e-n_e+1)} \mathbb{Z}/q^{\frac{n-n_e}{e}}\mathbb{Z} \right) \oplus (R/P)^\times.$$

Теорема 3.7. *Пусть* P *— простой идеал, и* $N(P) = q^r$, *где* q *— нечетное простое число такое, что* $q|\Delta$, *и пусть* $n \geq 1$ *— целое число. Предположим, что* $\mathbb{K}$ *содержит приведенный корень из единицы степени* q.

Если $n \leq e + 1$, *то*

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r(n-1)} \mathbb{Z}/q\mathbb{Z} \right) \oplus (R/P)^\times.$$

Если $e + 2 \leq n \leq \frac{qe}{q-1}$ *(если* $e + 2 > \frac{qe}{q-1}$ *тогда этот случай не учитывается), то*

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r(n_e-1)} \mathbb{Z}/q^2\mathbb{Z} \right) \oplus \left(\bigoplus_{j=1}^{r(e-n_e+1)} \mathbb{Z}/q\mathbb{Z} \right) \oplus (R/P)^\times.$$

Если $\frac{qe}{q-1} + 1 \leq n \leq 2e + 1$, *то*

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r(w-1)} \mathbb{Z}/q^2\mathbb{Z} \right) \oplus \left(\bigoplus_{j=1}^{r(e-w+2)} \mathbb{Z}/q\mathbb{Z} \right) \oplus (R/P)^\times.$$

Если $2e + 2 \leq n$, *то*

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r(w-1)} \mathbb{Z}/q^{\frac{n-n_e}{e}+1}\mathbb{Z} \right) \oplus \left(\bigoplus_{j=1}^{r(e-w+1)} \mathbb{Z}/q^{\frac{n-n_e}{e}}\mathbb{Z} \right) \oplus \left(\bigoplus_{j=1}^{r} \mathbb{Z}/q\mathbb{Z} \right) \oplus (R/P)^\times.$$

Теорема 3.8. *Пусть* P *— простой идеал, и* $N(P) = 2^r$ *такое, что* $2|\Delta$, *и пусть* $n \geq 2$ *— целое число.*

Если $n \leq e$, *то*

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r(n-1)} \mathbb{Z}/2\mathbb{Z} \right) \oplus (R/P)^\times.$$

Если $e + 1 \leq n$, *то*

$$(R/P^n)^\times \cong \left(\bigoplus_{k=1}^{e} \left(\bigoplus_{j=1}^{r} \mathbb{Z}/2^{\lceil \frac{n-k}{e} \rceil}\mathbb{Z} \right) \right) \oplus (R/P)^\times.$$

3.6 Оценки некоторых сумм характеров в полях алгебраических чисел

Для полноты изложения приведем здесь формулу А.Г. Постникова для степеней нечетных простых чисел [26].

Пусть $n \geq 2$ — натуральное. Если n представляется в виде $n = \alpha q^{\tilde{f}} - \mu(\tilde{f})$, где $\tilde{f}, \mu(\tilde{f}) \in \mathbb{Z}, 0 \leq \mu(\tilde{f}) \leq \tilde{f} - 1$ и $(\alpha, q) = 1$, тогда положим f, равным максимальному значению среди таких $\tilde{f}$, т.е.

$$f = \max \{\tilde{f}; n = \alpha q^{\tilde{f}} - \mu(\tilde{f});\ \tilde{f}, \mu(\tilde{f}) \in \mathbb{Z}, 0 \leq \mu(\tilde{f}) \leq \tilde{f} - 1, (\alpha, q) = 1\}.$$

Определим

$$\mu = \begin{cases} \mu(f) \text{ если } n = \alpha q^{\tilde{f}} - \mu(\tilde{f}), \\ -1 \text{ в противном случае.} \end{cases}$$

Теорема 3.9. ***(А.Г. Постников)*** *Пусть q — нечетное простое число. Существует многочлен*

$$f(u) = a_{n+\mu}u^{n+\mu} + \cdots + a_1 u$$

степени $n + \mu$ с целыми коэффициентами такой, что для любой образующей g подгруппы $(\mathbb{Z}/q^n\mathbb{Z})_1^\times$ при любом целом u справедливо сравнение

$$\frac{ind_g(1 + qu)}{q - 1} \equiv \Lambda f(u) \mod q^{n-1}. \tag{3.37}$$

Пусть $k = k'q^\tau$, где $\tau, k' \in \mathbb{Z}$, и $(k', q) = 1$.

Тогда

$$a_k = (-1)^{k+1} q^{k-1-\tau} x_k \tag{3.38}$$

(очевидно, a_k можно брать с точностью до кратных q^{n-1}), где x_k есть решение сравнения

$$k'x_k \equiv 1 \mod q^{n-k+\tau},$$

а Λ *— решение сравнения*

$$\frac{ind_g(1+q)}{q-1} \equiv \Lambda f(1) \mod q^{n-1}$$

причем сравнение разрешимо и $(\Lambda, q) = 1$.

Доказательство. Поскольку подгруппа $(\mathbb{Z}/q^n\mathbb{Z})_1^\times$ является циклической порядка q^{n-1} и порождается $1+q$ (см., например, [10], с. 209), то ясно, что $q-1|\mathrm{ind}_g(1+q)$, и $(\frac{\mathrm{ind}_g(1+q)}{q-1}, q) = 1$.

Для любого q-адического целого числа u, сходится ряд

$$\sum_{k=1}^{\infty}(-1)^{k+1}\frac{(qu)^k}{k} = \ln(1+qu).$$

Кроме того, для любых двух таких целых чисел u_1 и u_2 имеем

$$\ln\big((1+qu_1)(1+qu_2)\big) = \ln(1+qu_1) + \ln(1+qu_2).$$

Определим

$$\overline{F}(1+qu) = \sum_{k=1}^{n-1}(-1)^{k+1}\frac{(qu)^k}{k},$$

и тогда, рассуждая аналогично лемме 3.1, видим, что имеет место тождество

$$\overline{F}((1+qu_1)(1+qu_2)) \equiv \overline{F}(1+qu_1) + \overline{F}(1+qu_2) \mod q^n.$$

Следовательно, определим

$$\hat{F}(1+qu) = \frac{\overline{F}(1+qu)}{q} = \sum_{k=1}^{n-1}(-1)^{k+1}\frac{q^{k-1}u^k}{k},$$

и получим

$$\hat{F}((1+qu_1)(1+qu_2)) \equiv \hat{F}(1+qu_1) + \hat{F}(1+qu_2) \mod q^{n-1}. \tag{3.39}$$

Мы можем заменить каждый коэффициент $\hat{F}$ по модулю q^{n-1} целым числом, и сделаем это следующим образом.

Пусть a_k определено как в (3.38). Тогда

$$a_k = (-1)^{k+1} q^{k-1-\tau} x_k \equiv (-1)^{k+1} \frac{q^{k-1-\tau}}{k'} \equiv (-1)^{k+1} \frac{q^{k-1}}{k} \mod q^{n-1}.$$

Очевидно, что $a_1 = 1$.

Определим

$$f(u) = F(1+qu) = u + a_2 u^2 + \cdots + a_{n-1} u^{n-1},$$

где ясно, что для всех u имеем

$$F(1+qu) \equiv \hat{F}(1+qu) \mod q^{n-1}. \tag{3.40}$$

Из определения легко проверить, что коэффициенты $q | a_2, \ldots, a_{n-1}$, и поэтому

$$F(1+q) \equiv 1 \mod q \implies F(1+q) \not\equiv 0 \mod q.$$

Отсюда следует разрешимость сравнения

$$\frac{\mathrm{ind}_g(1+q)}{q-1} \equiv \Lambda F(1+q) \mod q^{n-1},$$

решение которого обозначим через Λ.

Так как $F(1+q) \not\equiv 0 \mod q$ и $\mathrm{ind}_g(1+q) \not\equiv 0 \mod q$, то $(\Lambda, q) = 1$.

Для $s = 1, 2, \ldots, q^{n-1}$, имеем

$$\frac{\mathrm{ind}_g(1+q)}{q-1} s \equiv \Lambda s F(1+q) \mod q^{n-q}.$$

Это, учитывая мультипликативные свойства обеих сторон по (3.39) и (3.40), означает, что

$$\frac{\mathrm{ind}_g((1+q)^s)}{q-1} \equiv \Lambda F((1+q)^s) \mod q^{n-1}. \tag{3.41}$$

Так как $1+q$ является порождающим подгруппы $(\mathbb{Z}/q^n\mathbb{Z})_1^\times$, то элементы $(1+q)^s$ для $s = 1, 2, \ldots, q^{n-1}$ пробегают всю подгруппу $(\mathbb{Z}/q^n\mathbb{Z})_1^\times$, и, следовательно, (3.37) следует из (3.41):

$$\frac{\mathrm{ind}_g(1+qu)}{q-1} \equiv \Lambda F(1+qu) \equiv \Lambda f(u) \mod q^{n-1}.$$

□

В теоремах 3.4,3.5,3.6,3.7 и 3.8 видим, что имеет место общий изоморфизм

$$(R/P^n)^\times \cong \bigoplus_{j=1}^{L} \mathbb{Z}/q^{k_j}\mathbb{Z},$$

для некоторых целых $L, \{k_j\}_{j=1}^{L}$, где группы справа — аддитивные.

Используя эту терминологию, мы приходим к основному результату третьей части данной главы.

Теорема 3.10. *Пусть $1 \le h \le L$ — рациональное целое, и $\{k_{j_1}, \dots, k_{j_h}\} \subseteq \{k_1, \dots, k_L\}$, так, что $k_{j_t} \ge 4$, если $q = 2$, и $k_{j_t} \ge 3$ если $q \ne 2$.*

Пусть $A \subseteq (R/P)^\times, A' \subseteq \bigoplus_{t=1}^{h} \mathbb{Z}/q^{k_{j_t}}\mathbb{Z}$ — некоторые подмножества, и пусть, для $j \notin \{j_1, \dots, j_h\}$, b_j, c_j — рациональные целые, такие, что $0 \le b_j \le c_j < q^{k_j}$. Пусть

$$S = \{u \in (R/P^n)^\times; a \in A, (u_{j_1}, \dots, u_{j_h}) \in A', b_j \le u_j \le c_j \le q^{k_j}; j \notin \{j_1 \dots, j_h\}\}.$$

Пусть

$$l = n - 1 + \mu,$$

тогда, полагая

$$K_1 = \sum_{j \notin \{j_1 \dots, j_h\}} k_j, K_2 = \sum_{t=1}^{h} k_{j_t},$$

справедлива общая оценка

$$\Big| \sum_{S} \chi(u) \Big| \le 2^{n-h} (8l)^{\frac{(L-h)l}{2} \ln (12l(l+1)(n-2))} (q^r - 1) q^{(1 - \frac{1}{3l^2(n-2)\ln(12l(l+1)(n-2))})K_1 + K_2},$$

и l удовлетворяет неравенствам

$$n - 2 \le l \le n - 2 + \frac{\ln(\frac{9n}{8})}{\ln q}.$$

Кроме того, полагая

$$\tau(x)=\begin{cases}1 \text{ если } q^{1+\frac{1}{n-2}}\le x\le q^2,\\ \frac{\ln q}{\ln\frac{x}{q}} \text{ если } x\ge q^2,\end{cases}\qquad w(x)=\frac{\tau(x)}{3l^2\ln\left(\frac{12l(l+1)}{\tau(x)}\right)},$$

то справедлива конкретная оценка

$$\Big|\sum_S\chi(u)\Big|\le|A||A'|\prod_{j\notin\{j_1\dots,j_h\}}\Big((8l)^{\frac{\tau(b_j)}{6lw(b_j)}}b_j^{1-w(b_j)}+(8l)^{\frac{\tau(c_j)}{6lw(c_j)}}c_j^{1-w(c_j)}\Big).$$

Доказательство. Мы докажем теорему для $q\ne 2$, а для $q=2$ доказательство полностью аналогично.

По следствию 3.3 имеем

$$\sum_S\chi(u)=\sum_{a\in A}\chi_P(a)\sum_{(u_{j_1},\dots,u_{j_h})\in A'}e^{2\pi i\sum_{t=1}^h\left(\frac{m_{j_t}\mathrm{ind}(1+qu_{j_t})}{q^{k_{j_t}}}\right)}\sum_{j\notin(j_1,\dots,j_h)}\sum_{u_j=b_j}^{c_j}e^{2\pi i\frac{m_j\mathrm{ind}(1+qu_j)}{q^{k_j}}}=$$

$$=\sum_{a\in A}\chi_P(a)\sum_{(u_{j_1},\dots,u_{j_h})\in A'}e^{2\pi i\sum_{t=1}^h\left(\frac{m_{j_t}\Lambda_{j_t}f_{j_t}(u_{j_t})}{q^{k_{j_t}}}\right)}\sum_{j\notin(j_1,\dots,j_h)}\sum_{u_j=b_j}^{c_j}e^{2\pi i\frac{m_j\Lambda_jf_j(u_j)}{q^{k_j}}},$$

где последнее равенство следует из применения к каждой сумме теоремы 3.9, с учетом того, что умножение функции индекса в $(\mathbb{Z}/q^{k_j}\mathbb{Z})_1^\times$ на $(q-1)$ дает функцию индекса в $(\mathbb{Z}/q^{k_j}\mathbb{Z})^\times$.

Используя неравенство треугольника и теорему 3.2 (оценка И.М. Виноградова), получаем

$$\Big|\sum_S\chi(u)\Big|\le|A||A'|\prod_{j\notin(j_1,\dots,j_h)}\Big|\sum_{u_j=b_j}^{c_j}e^{2\pi i\frac{m_j\Lambda_jf(u_j)}{q^{k_j}}}\Big|\le$$

$$\le|A||A'|\prod_{j\notin(j_1,\dots,j_h)}\Big((8l)^{\frac{\tau(b_j)}{6lw(b_j)}}b_j^{1-w(b_j)}+(8l)^{\frac{\tau(c_j)}{6lw(c_j)}}c_j^{1-w(c_j)}\Big),$$

что и есть конкретная оценка.

Общая оценка непосредственно следует из простых неравенств

$$|A|\le|(R/P)^\times|=q^r-1,\ \ b_k\le c_k\le q^{k_j}.$$

Осталось доказать неравенства для l. Нижняя оценка $l\ge n-2$ вытекает непосредственно из определения.

Для верхней оценки, поскольку $\mu\le h-1$, имеем

$$n = \alpha q^f - \mu \implies n \geq q^f - f + 1 \implies \ln n \geq f \ln(q) + \ln\Big(1 - \frac{f-1}{q^f}\Big).$$

Легко видеть, что $\frac{f-1}{q^f} \leq \frac{1}{9}$, и поэтому

$$\ln n \geq f \ln(q) + \ln\Big(\frac{8}{9}\Big) \implies \frac{\ln \frac{9n}{8}}{\ln q} \geq f \geq \mu + 1 \implies n - 2 + \frac{\ln \frac{9n}{8}}{\ln q} \geq n + \mu - 1 = l.$$

□

Заключение

В данной работе представлены исследования трех вопросов теории чисел.

В первой части мы обобщили теорему Лежандра о трёх квадратах, в частности, мы доказали теорему 1.2 о представлениях пар положительных целых чисел в виде сумм трех квадратов, таких, что представления имеют хотя бы один общий квадрат.

Теорема. *Пусть $m, m' \in \mathbb{Z}$ — пара Лежандровых положительных целых чисел.*

Система

$$q^2 m = a^2 + b_1^2 + c_1^2,$$

$$q^2 m' = a^2 + b_2^2 + c_2^2$$

имеет решение в положительных q, a, b_1, b_2, c_1, c_2 тогда и только тогда, когда пара (m, m') не сравнима с $(0, 3)$ или $(3, 4)$ по модулю 8 и не сравнима ни с одной из

$$(0, 3 \cdot 2^{k-3}),$$

$$(0, 3 \cdot 2^{k-2}),$$

$$(0, 7 \cdot 2^{k-3}),$$

$$(2^{k-3}, 3 \cdot 2^{k-2}),$$

$$(5 \cdot 2^{k-3}, 3 \cdot 2^{k-2})$$

по модулю 2^k, для любого четного целого $k \geq 4$.

Более того, существует решение системы (1.2) такое, что q нечетно и взаимно просто с a.

В этом направлении автор предлагает определить наименьшее возможное значение q для

заданной пары (m, m'), удовлетворяющей условиям теоремы 1.2.

Стоит отметить, что вычисления показывают, что $q = 3$ встречается чрезвычайно часто, а $q > 3$ встречается очень редко.

Во второй части мы представили ряд результатов, касающихся оценок тригонометрических сумм в полях алгебраических чисел на основе методов, разработанных Хуа Ло-кеном.

Сначала в теореме 2.2 мы оценили тригонометрическую сумму многочлена f по простому идеалу P в терминах делимости идеала, порожденного коэффициентами f, на P, опираясь на обобщение метода деревьев Хуа Ло-кена на случай рационального поля $\mathbb{Q}$.

Теорема. *Справедлива оценка*

$$|S(f, P^n)| \leq (m-1)N(P^{n-h}),$$

где h — положительное целое число, зависящее от делимости идеала, порожденного коэффициентами многочлена f, на простой идеал P.

Затем в теореме 2.3 мы представили усиленную форму оценки Хуа Ло-кена в случае идеала, равного степени простого идеала, где оценивали тригонометрическую сумму f по P в терминах m — степень f.

Теорема. *Пусть $N(P) = q^r$, где $r \geq 1$ рациональное целое число. Справедлива общая оценка*

$$|S(f, P^n)| \leq C_d(m)N(P)^{n(1-\frac{1}{m})},$$

где

$$C_d(m) = \begin{cases} m^d \quad \textit{если } q > m, N(P) \geq (m-1)^{\frac{m}{m-2}}, \\ \frac{m-1}{m} m^{\frac{3}{m}} \quad \textit{если } q > m, N(P) \leq (m-1)^{\frac{m}{m-2}}, \\ m^{\frac{d(2d+1)}{m}} \quad \textit{если } q \leq m, N(P) \geq (m-1)^{\frac{m}{m-2}}, \\ (m-1)m^{\frac{d(2d+1)}{m}} \quad \textit{если } q \leq m, N(P) \leq (m-1)^{\frac{m}{m-2}}. \end{cases}$$

Более того, справедлива конкретная оценка

$$|S(f, P^n)| \leq C_d(m, P)N(P)^{n(1-\frac{1}{m})},$$

где

$$C_d(m,P)=\begin{cases} m^d \quad \textit{если } q>m, N(P)\geq (m-1)^{\frac{m}{m-2}},\\ \frac{m-1}{m}m^{\frac{3}{m}} \quad \textit{если } q>m, N(P)\leq (m-1)^{\frac{m}{m-2}},\\ m^{\frac{c(2e+3)}{m}} \quad \textit{если } q\leq m, N(P)\geq (m-1)^{\frac{m}{m-2}},\\ (m-1)m^{\frac{c(2e+3)}{m}} \quad \textit{если } q\leq m, N(P)\leq (m-1)^{\frac{m}{m-2}}. \end{cases}$$

После этого в теореме 2.4 мы представили уточненную форму теоремы 2.3, когда число классов $\mathbb{K}$ равно 1, а идеал A, порожденный коэффициентами f, имеет вид $A=\frac{B}{P^n}$, где $(B,P)=1$.

Теорема. *Пусть число классов $\mathbb{K}$ равно 1, а идеал A, порожденный коэффициентами f, имеет вид $A=\frac{B}{P^n}$, где $(B,P)=1$.*

Пусть $N(P)=q^r$, где $r\geq 1$ — целое рациональное число. Тогда мы имеем общую оценку

$$|S(f,P^n)|\leq C_d(m)N(P)^{n(1-\frac{1}{m})},$$

где

$$C_d(m)=\begin{cases} 1 \quad \textit{если } q>m, N(P)\geq (m-1)^{\frac{2m}{m-2}},\\ (m-1)^{\frac{2}{m}} \textit{если } q>m, (m-1)^{\frac{2m}{m-2}}>N(P)\geq (m-1)^{\frac{m}{m-2}},\\ \frac{m-1}{m}m^{\frac{3}{m}} \quad \textit{если } q>m, N(P)<(m-1)^{\frac{m}{m-2}},\\ m^{\frac{d(2d+1)}{m}} \quad \textit{если } q\leq m, N(P)\geq (m-1)^{\frac{m}{m-2}},\\ (m-1)m^{\frac{d(2d+1)}{m}} \quad \textit{если } q\leq m, N(P)<(m-1)^{\frac{m}{m-2}}. \end{cases}$$

Затем мы использовали теорему 2.4, чтобы получить в том же частном случае теорему 2.5, которая является уточненной формой оценки Хуа Ло-кена для целого неразветвленного идеала Q.

Теорема. *Пусть Q — целый идеал с $(Q,\delta)=1$. Тогда справедлива оценка*

$$|S(f,Q)|\leq e^{\frac{5}{2}d^2(2d+1)}e^{3.442md}N(Q)^{1-\frac{1}{m}}.$$

В конце мы объединили оценки, полученные обоими методами и получили новую оценку в теореме 2.6.

Теорема. *Справедлива оценка*

$$|S(f,P^n)| \le C_d(m)(m-1)N(P)^{n(1-\frac{1}{m})+\frac{U_h}{m}-h}.$$

В этом направлении автор предполагает, что справедлива оценка вида

$$|S(f,P)| \le C'N^{1-\frac{1}{m}-\epsilon};\ \epsilon>0,$$

для некоторой постоянной C', что позволяет нам получить, аналогично доказательству теоремы 2.4 и в тех же терминах, что

$$N^{\epsilon} \ge C' \implies C_d(m)=1,$$

что позволяет нам обобщить теорему 2.5 за пределы частного случая, когда номер класса $\mathbb{K}$ равно 1 и идеал A имеет конкретный вид, приведенный выше.

Кроме того, константы в теоремах 2.3, 2.4 и 2.5 можно улучшить, используя более сильные оценки.

В третьей части мы обобщили формулу А.Г. Постникова на случай степени простого числа 2 и получили оценки некоторых сумм характеров в полях алгебраических чисел.

В частности, в теореме 3.1 мы представили обобщение формулы А.Г. Постникова на случай степени простого числа 2.

Теорема. *Существует многочлен $f(u)=a_{d+\mu}u^{d+\mu}+\cdots+a_2u^2+u$ степени $d+\mu$ с целыми коэффициентами такой, что для любой образующей g подгруппы $(\mathbb{Z}/2^n\mathbb{Z})^{\times}_{1,1}$ при любом целом u справедливо сравнение*

$$ind_g(1+4u) \equiv \Lambda f(u) \mod 2^{n-2}. \tag{3.42}$$

Пусть $k=4^{\tau}k'$, где $\tau,k'\in\mathbb{Z}$, и $(k',4)\le 2$.

Тогда

$$a_k=\begin{cases}(-1)^{k+1}4^{k-1-\tau}x_k, & \text{если } (k',4)=1,\\ (-1)^{k+1}\frac{4^{k-1-\tau}}{2}x_k, & \text{если } (k',4)=2\end{cases} \tag{3.43}$$

(очевидно, a_k можно брать с точностью до кратных 2^{n-2}), где x_k есть решение сравнения

$$\begin{cases} k'x_k \equiv 1 \mod 2^{n-2}, & \textit{если } (k',4)=1, \\ \frac{k'}{2}x_k \equiv 1 \mod 2^{n-2}, & \textit{если } (k',4)=2, \end{cases}$$

а Λ *— решение сравнения*

$$ind_g(5) \equiv \Lambda f(1) \mod 2^{n-2},$$

причем сравнение разрешимо и Λ *нечетное,*

где d, μ — константы, зависящие от n.

Затем мы использовали этот результат для получения оценок некоторых сумм характеров над некоторыми множествами в полях алгебраических чисел в теореме 3.10.

Теорема. *Пусть* $1 \le h \le L$ *— рациональное целое, и* $\{k_{j_1}, \dots, k_{j_h}\} \subseteq \{k_1, \dots, k_L\}$*, так, что* $k_{j_t} \ge 4$*, если* $q = 2$*, и* $k_{j_t} \ge 3$ *если* $q \ne 2$*.*

Пусть $A \subseteq (R/P)^\times, A' \subseteq \bigoplus_{t=1}^h \mathbb{Z}/q^{k_{j_t}}\mathbb{Z}$ *— некоторые подмножества, и пусть, для* $j \notin \{j_1, \dots, j_h\}$*,* b_j, c_j *— рациональные целые, такие, что* $0 \le b_j \le c_j < q^{k_j}$*. Пусть*

$$S = \{u \in (R/P^n)^\times; a \in A, (u_{j_1}, \dots, u_{j_h}) \in A', b_j \le u_j \le c_j \le q^{k_j}; j \notin \{j_1 \dots, j_h\}\}.$$

Пусть

$$l = n - 1 + \mu,$$

тогда, полагая

$$K_1 = \sum_{j \notin \{j_1 \dots, j_h\}} k_j, K_2 = \sum_{t=1}^h k_{j_t},$$

справедлива общая оценка

$$\Big| \sum_S \chi(u) \Big| \le 2^{n-h} (8l)^{\frac{(L-h)l}{2} \ln (12l(l+1)(n-2))} (q^r - 1) q^{(1 - \frac{1}{3l^2(n-2)\ln(12l(l+1)(n-2))})K_1 + K_2},$$

и l *удовлетворяет неравенствам*

$$n-2 \le l \le n-2+\frac{\ln\left(\frac{9n}{8}\right)}{\ln q}.$$

Кроме того, полагая

$$\tau(x)=\begin{cases}1 \text{ если } q^{1+\frac{1}{n-2}} \le x \le q^2,\\ \frac{\ln q}{\ln \frac{x}{q}} \text{ если } x \ge q^2,\end{cases} \qquad w(x)=\frac{\tau(x)}{3l^2\ln\left(\frac{12l(l+1)}{\tau(x)}\right)},$$

то справедлива конкретная оценка

$$\Big|\sum_S \chi(u)\Big| \le |A||A'| \prod_{j\notin\{j_1\dots,j_h\}} \Big((8l)^{\frac{\tau(b_j)}{6lw(b_j)}} b_j^{1-w(b_j)} + (8l)^{\frac{\tau(c_j)}{6lw(c_j)}} c_j^{1-w(c_j)}\Big).$$

В этом направлении автор предполагает, что имеет место аналог формулы А.Г. Постникова для полей алгебраических чисел, который позволил бы получить оценки, аналогичные теореме 3.10, для более общего класса множеств.

Более того, существуют современные более сильные оценки сумм Вейля, чем оценка И.М. Виноградова в теореме 3.2, которые можно использовать для получения более сильных результатов, чем 3.10.

Автор приносит благодарность научному руководителю профессору Владимиру Николаевичу Чубарикову за постановку задачи и за неоценимую помощь, которую он оказывал на протяжении всей подготовки данной работы.

Благодарность

“Кто хочет сделать дело, тот ищет возможности” - говорит мне моя любимая мама, когда у меня что-то не ладится.

Я твердо знаю, что я в этом мире не один, и я иду по своему пути рядом с огромным количеством людей, которым я очень признателен, которым я хочу посвятить свой научный труд. Свою диссертацию я посвящаю...

...мученикам своей Родины — Сирии, и, в первую очередь, мученикам Сирийской арабской армии, без самоотверженных жертв которых нас всех бы не было,

моим родителям Башару и Асме, которым я благодарен за каждый миг своего существования, моим сестре и брату Зейн и Кариму, которые всегда поддерживали меня, и всей моей семье,

профессору Виктору Антоновичу Садовничему, ректору МГУ имени М.В. Ломоносова, выдающемуся руководителю нашего университета,

профессору Владимиру Николаевичу Чубарикову, моему научному руководителю, направляющему меня в моих научных изысканиях,

преподавателям и сотрудникам МГУ, которые делают университет ведущим центром обучения и инноваций, и тем местом, в которое хочется возвращаться с радостью вновь и вновь,

профессору Омрану Кубе, гению, наставнику и другу, который был рядом на каждом этапе моего становления, без руководства которого я бы не состоялся как ученый математик,

г-ну Фаресу Абу-Салеху, который познакомил меня со строгой математикой и пристально следил за моими результатами в науке,

преподавателям и сотрудникам HIAST, моему второму дому, где я провел лучших моментов жизни,

г-же Диане Бадра, которая нежно взлелеяла мою только зарождающуюся любовь к математике, чья страсть к этому предмету вдохновила меня и за чью бесконечную щедрость я буду благодарен вечно,

всем моим учителям, начиная детского сада, заканчивая старшими классами, с которыми я вырос, и которые оставили свой след в том, кем я являюсь сегодня,

и, наконец, всем моим друзьям, близким и далеким, с которыми я учился, смеялся и любил жизнь, и с которыми мои узы прочны и глубоки.

Список литературы

1. *Архипов Г.И., Карацуба А.А., Чубариков В.Н.* Теория кратных тригонометрических сумм. — М. : Наука, Физматлит, 1987. — 368 с.

2. *Чубариков В.Н.* О кратных рациональных тригонометрических суммах над полем алгебраических чисел // Чебышевский сб. — 2021. — Т. 22. — №4. — С. 306-323.

3. *Kouba O.* Algebra II. — HIAST, Damascus, 2017. — 494 pgs.

4. *Knapp A.* Basic Algebra. — Birkhäuser Boston, 2006. — 735 pgs.

5. *Knapp A.* Advanced Algebra. — Birkhäuser Boston, 2006. — 730 pgs.

6. *Виноградов И.М.* Избранные труды. — Издательство Академии наук СССР, 1952. — 436 с.

7. *Виноградов И.М.* Основы теории чисел. — М.: Физматлит, 1983. — 180 с.

8. *Serre J-P.* A Course in Arithmetic. — Springer Verlag, New York, 1973. — 115 pgs.

9. *Боревич З.И., Шафаревич И.Р.* Теория Чисел. — М. : Наука, Москва, 1964. — 566 с.

10. *Apostol T.* Introduction to Analytic Number Theory. — Springer-Verlag, 1976. — 338 pgs.

11. *Чубариков В.Н.* Обобщенная формула бинома Ньютона и формулы суммирования // Чебышевский сб. — 2020. — Т. 21. — №4. — С. 270-301.

12. *Colliot-Thélène J.L., Sansuc J.J., Swinnerton-Dyer P.* Intersections of two quadrics and Châtelet surfaces // Journal für die reine und angewandte Mathematik. — 1987. — V. 373. — P. 37-107.

13. *Colliot-Thélène J.L., Coray D.* Descente et principe de Hasse pour certaines variétés rationnelles // Journal für die reine und angewandte Mathematik. — 1980. — V. 320. — P. 150-191.

14. *Salberger P.* On the arithmetic of intersections of two quadrics containing a conic // arXiv:2305.02289 [math.NT].

15. *Hua L-K.* On Exponential Sums Over an Algebraic Number Field // Canadian Journal of Mathematics. — 1951. — V. 3. — P. 44-51.

16. *Hua L-K.* On the number of solutions of Tarry's problem // Acta Sci. Sinica. — 1952. — V. 1. — P. 1-76.

17. *Hua L-K.* On An Exponential Sum // Journal of the London Mathematical Society. — 1938. — V. s1-13. — №1. — P. 54-61.

18. *Wang Yuan* Diophantine Equations and Inequalities in Algebraic Number Fields. — Springer Verlag, Berlin, Heidelberg, 1991. — 168 pgs.

19. *Weil, A.* On Some Exponential Sums // Proceedings of the National Academy of Sciences of the United States of America. — 1948. — V. 34. — №5. — P. 204-207.

20. *Чубариков В.Н.* Деревья Хуа Ло-кена в теории сравнений // Математические вопросы кибернетики. — 2007. — Т. 16. — С. 73-78.

21. *Chen Jingrun* On Professor Hua's Estimate of Exponential Sums // Scientia Sinica. — 1977. — V. 20. — №6. — P. 711-719.

22. *Chen Jingrun* On the representation of natural number as a sum of terms of the form $\frac{x(x+1)\cdots(x+k-1)}{k!}$ // Acta Mathematica Sinica. — 1959. — V. 9. — P. 264-270.

23. *Nechaev V.I.* An estimate of the complete rational trigonometric sum // Math. Notes. — 1975. — V. 17. — P. 504-511.

24. *Qi Minggao, Ding Ping* On Estimate of complete trigonometric sums // China Ann. Math. — 1985. — V. 6. — №1. — P. 109-120.

25. *Mordell L.J.* On a sum analogous to a Gauss's sum // Quart. J. Math. (Oxford). — 1932. — V. os-3. — №1. — P. 161-167.

26. *Постников А.Г.* О сумме характеров по модулю, равного степени простого числа // Изв. АН СССР. Сер. матем. — 1955. — Т. 19. — №1. — С. 11-16.

27. *Elia M., Interlando J.C., Rosenbaum R.* On the Structure of Residue Rings of Prime Ideals in Algebraic Number Fields Part I: Unramified Primes // International Mathematical Forum. — 2010. — P. 2795-2808.

28. *Elia M., Interlando J.C., Rosenbaum R.* On the Structure of Residue Rings of Prime Ideals in Algebraic Number Fields Part II: Ramified Primes // International Mathematical Forum. — 2011. — P. 565-589.

29. *Ireland K., Rosen M.* A Classical Introduction to Modern Number Theory. — Springer, 1990. — 389 pgs.

30. *Hirschhorn M.D.* A simple proof of Jacobi's four-square theorem // Proceedings of the American Mathematical Society. — 1987. — V. 101. — №3. — P. 436-438.

Публикации автора по теме диссертации

Статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ

31. *Аль-Ассад Х.* Обобщение теоремы Лежандра о трёх квадратах // Чебышевский сб. — 2024. — Т. 25. — №1. — С. 127-137. — (Входит в перечень ВАК РФ, РИНЦ, двухлетний импакт-фактор РИНЦ: 0,498). Перевод:

Al-Assad H. A generalisation of Legendre's three-square theorem // Chebyshevskii Sb. — 2024. — V. 25. — №1. — P. 127-137. — (Scopus, RSCI. Impact Factor 2023: SJR 0.296).

32. *Аль-Ассад Х.* Об оценках Хуа Ло-кена тригонометрических сумм в полях алгебраических чисел // Чебышевский сб. — 2024. — Т. 25. — №2. — С. 181-207. — (Входит в перечень ВАК РФ, РИНЦ, двухлетний импакт-фактор РИНЦ: 0,498). Перевод:

Al-Assad H. On Hua Loo-Keng's estimates of exponential sums in algebraic number fields // Chebyshevskii Sb. — 2024. — V. 25. — №2. — P. 181-207. — (Scopus, RSCI. Impact Factor 2023: SJR 0.296).

33. *Аль-Ассад Х.* О сумме характеров по модулю, равного степени простого числа 2 // Чебышевский сб. — 2022. — Т. 23. — №2. — С. 201-208. — (Входит в перечень ВАК РФ, РИНЦ, двухлетний импакт-фактор РИНЦ: 0,498). Перевод:

Al-Assad H. On character sums modulo a power of the prime number 2 // Chebyshevskii Sb. — 2022. — V. 23. — №2. — P. 201-208. — (Scopus, RSCI. Impact Factor 2022: SJR 0.305).

34. *Al-Assad H.* Applying A.G. Postnikov's Formula in Algebraic Number Fields // Dokl. Math. — 2024. — V. 109. — №3. — P. 213-215. — (RSCI, Web of Science, Scopus. Impact Factor 2023: JIF 0.5, SJR 0.458).