МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

*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.

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2024

Диссертация подготовлена на кафедре математических и компьютерных методов анализа механико-математического факультета
ФГБОУ ВО "Московский государственный университет имени М. В. Ломоносова".

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

Официальные оппоненты: **Добровольский Николай Михайлович,** доктор физико-математических наук, профессор, Тульский государственный педагогический университет имени Л.Н. Толстого, физико-математический факультет, кафедра алгебры, математического анализа и геометрии, заведующий кафедрой.

**Чирский Владимир Григорьевич,** доктор физико-математических наук, доцент, Московский государственный университет имени М.В. Ломоносова, механико-математический факультет, кафедра математического анализа, профессор.

**Рахмонов Зарулло Хусенович,** доктор физико-математических наук, профессор, Институт математики имени академика А. Джураева Национальной академии наук Республики Таджикистан, главный научный сотрудник.

Защита диссертации состоится 29 ноября 2024 года в 16 часов 45 минут на заседании диссертационного совета МГУ.011.4 Московского государственного университета имени М.В. Ломоносова по адресу: Российская Федерация, 119234, Москва, ГСП-1, Ленинские горы, д. 1, МГУ имени М.В. Ломоносова, механико-математический факультет, аудитория 1408.

E-mail: dissovet.msu.011.4@math.msu.ru.

С диссертацией можно ознакомиться в в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д.27) и на портале:

https://dissovet.msu.ru/dissertation/3184

Автореферат разослан

Ученый секретарь
диссертационного совета МГУ.011.4,
кандидат физико-математических наук

В.А. Кибкало

# Актуальность темы исследования

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[1], теоремы Лагранжа[2] и Якоби[3] о четырех квадратах, проблема Гильберта-Гамке[4] 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[5] 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[6] 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[7] 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[8] нашел нетривиальную оценку тригонометрических сумм в поле рациональных чисел. Последующие работы Чэнь Джун-руна[9][10] и В. И. Нечаева[11] улучшали оценку. В 1984 г. Ци Мингао и Дин Пин[12] нашли константу в оценке Хуа Ло-кена. В 1949 г. Хуа Ло-кен[13] обобщил свою оценку на случай

[1]Serre J-P., A Course in Arithmetic, Springer Verlag, New York 1973, p. 47.

[2]Ireland K., Rosen M., A Classical Introduction to Modern Number Theory, Springer, 1990.

[3]Hirschhorn M.D., A simple proof of Jacobi's four-square theorem, Proceedings of the American Mathematical Society, 101:3, 1987, p. 436.

[4]Архипов Г.И., Карацуба А.А., Чубариков В.Н. Теория кратных тригонометрических сумм. — М. : Наука, Физматлит, 1987, стр. 297.

[5]Serre J-P., A Course in Arithmetic, Springer Verlag, New York 1973, p. 41.

[6]Colliot-Thélène J.L., Coray D., Descente et principe de Hasse pour certaines variétés rationnelles, Journal für die reine und angewandte Mathematik, 320, 1980, 150–191.

[7]Виноградов И.М., Избранные труды, Издательство Академии наук СССР, 1952.

[8]Hua L-K., On An Exponential Sum, Journal of the London Mathematical Society, s1-13, 1938, 54–61.

[9]Chen Jingrun, On Professor Hua's Estimate of Exponential Sums, Scientia Sinica, Vol. 6, 1977, no. 20, 711–719.

[10]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, 264–270.

[11]Nechaev V.I., An estimate of the complete rational trigonometric sum, Math. Notes, Vol. 17, 1975, no. 6, 504–511.

[12]Qi Minggao, Ding Ping, On Estimate of complete trigonometric sums, China Ann. Math. B, 1:6, 1985, 109–120.

[13]Hua L-K., On Exponential Sums Over an Algebraic Number Field, Canadian Journal of Mathematics, 3, 1951.

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[14][15] для построения решений полиномиальных сравнений по модулю рационального простого числа, используемого в решении проблемы сходимости особого ряда в проблеме Пруэ-Терри-Эскота[16], 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[17]. 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[18], 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[19]. 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.

[14]Hua L-K., On the number of solutions of Tarry's problem, Acta Sci. Sinica, 1, 1952, 1–76.

[15]Чубариков В.Н. Деревья Хуа Ло-кена в теории сравнений, Математические вопросы кибернетики, Вып. 16. — М. : Физматлит, 2007, 73–78.

[16]Архипов Г.И., Карацуба А.А., Чубариков В.Н., Теория кратных тригонометрических сумм. — М. : Наука, Физматлит, 1987, стр. 26.

[17]Knapp A., Advanced Algebra, Birkhäuser Boston, 2006, p. 50.

[18]Постников А.Г., О сумме характеров по модулю, равного степени простого числа, Изв. АН СССР. Сер. матем., 19:1 (1955), 11–16.

[19]Виноградов И.М., Избранные труды, Издательство Академии наук СССР, 1952.

## 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.

# Содержание диссертации

**Введение** представляет краткую историю вопросов, актуальность тем, терминологию, цели работы, методы и основные результаты.

В **первой главе** обобщается теорема Лежандра о трех квадратах на представления двух целых чисел вместо одного. На основе обобщения Коллио-Телена и Корэ[20] 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,

[20]Colliot-Thélène J.L., Coray D., Descente et principe de Hasse pour certaines variétés rationnelles, Journal für die reine und angewandte Mathematik, 320, 1980, 150–191, theoreme 3.2.

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[21]. Основным результатом данной главы является теорема 1.2.

Дадим два полезных определения.

**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 либо

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

либо

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

Сформулируем основной результат данной главы.

**Теорема 1.2.** 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 такое, что $q$ нечетно и взаимно просто с $a$.

План доказательства следующий.

Рассматриваем систему с $q = 1$ в рациональных числах $a, b_1, b_2, c_1, c_2$.

Сначала мы покажем, что для любой пары $(m, m')$, система с $q = 1$ имеет нетривиальное решение в кольце $\mathbb{Z}/p\mathbb{Z}$ для любого простого числа $p$.

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

[21] Serre J-P., A Course in Arithmetic, Springer Verlag, New York. 1973, p. 46.

Затем мы покажем, что если $v_2(\text{НОД}(m,m')) \leq 1$, то система с $q=1$ имеет нетривиальное 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 с $q=1$ в $p-$адических полях $\mathbb{Q}_p$ при $v_2(\text{НОД}(m,m')) \leq 1$, и, поскольку разрешимость в $\mathbb{R}$ очевидна, мы используем форму локально-глобального принципа Хассе[22] для перехода к решениям системы с $q=1$ в $\mathbb{Q}$, при $v_2(\text{НОД}(m,m')) \leq 1$.

После этого, мы используем теорему Давенпорта-Касселса[23] для перехода от решений системы с $q=1$ в $\mathbb{Q}$ к решениям системы в целых числах $a, b_1, b_2, c_1, c_2$, при $v_2(\text{НОД}(m,m')) \leq 1$.

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

Предположим в дальнейшем, что $v_2(\text{НОД}(m,m')) \leq 1$, пока не сказано иное.

Пусть $p$ — некоторое простое число, и $k \geq 1$ — целое. Рассматриваем систему по модулю $p^k$:

$$t^2+x^2+y^2 \equiv m \mod p^k,$$
$$t^2+z^2+w^2 \equiv m' \mod p^k,$$

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

Используем следующую лемму для доказательства теоремы 1.3.

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

$$x^2+y^2 \equiv m \mod p$$

разрешимо.

**Теорема 1.3.** Если $p \neq 2$ и $k=1$, то система по модулю $p$ разрешима для всех $m, m'$.

Теорема 1.4 следует непосредственно.

**Теорема 1.4.** Если $p \neq 2$, то система по модулю $p^k$ разрешима для всех $m, m'$.

Теперь рассмотрим разрешимость при $p=2$.

**Лемма 1.2.** Если $p=2$ и $m, m'$ нечетны, то система по модулю $2^k$ разрешима.

Для доказательства теоремы 1.5 воспользуемся следующим предложением.

**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 $u \equiv 1 \mod 8$.

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

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.

Следующая лемма[24] дает разрешимость системы с $q=1$ в $p-$адических полях $\mathbb{Q}_p$.

**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 приведения по модулю $p^k$.

[22] Colliot-Thélène J.L., Coray D., Descente et principe de Hasse pour certaines variétés rationnelles, Journal für die reine und angewandte Mathematik, 320, 1980, 150–191, theoreme 3.2.

[23] Serre J-P., A Course in Arithmetic, Springer Verlag, New York. 1973, p. 46.

[24] Serre J-P., A Course in Arithmetic, Springer Verlag, New York. 1973, p. 14.

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 $k > 1$.

Для доказательства разрешимости системы с $q = 1$ в $\mathbb{Q}$ воспользуемся следующим результатом Д.Л. Коллио-Телена, Д. Корэ и Д.Д. Сансука[25].

**Теорема 1.6.** Пусть $\mathbb{K}$ — числовое поле и $\phi, \phi_1, \phi_2$ — 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 $\phi_1$ или $\phi_2$ 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.

Воспользуемся леммой 1.5 для перехода к решениям системы в $\mathbb{Z}$. Лемма 1.5 доказывается известной теоремой Давенпорта-Касселса[26].

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

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

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

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

Наконец, мы используем следующую лемму для перехода от решений в случае $v_2(\text{НОД}(m, m')) \leq 1$ к решениям в общем случае.

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

Во **второй главе** усилится оценка Хуа Ло-кена[27] 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[28] в обобщении метода деревьев Хуа Ло-кена[29][30] на поля алгебраических чисел, и использует это обобщение для получения соответствующих оценок тригонометрических сумм.

---

[25] Colliot-Thélène J.L., Coray D., Descente et principe de Hasse pour certaines variétés rationnelles, Journal für die reine und angewandte Mathematik, 320, 1980, 150–191, theoreme 3.2.

[26] Serre J-P., A Course in Arithmetic, Springer Verlag, New York. 1973, p. 46.

[27] Hua L-K., On Exponential Sums Over an Algebraic Number Field, Canadian Journal of Mathematics, 3, 1951, 44–51.

[28] Чубариков В.Н., О кратных рациональных тригонометрических суммах над полем алгебраических чисел, Чебышевский сб., 22:4 (2021), 306–323.

[29] Чубариков В.Н., Деревья Хуа Ло-кена в теории сравнений, Математические вопросы кибернетики, Вып. 16. — М. : Физматлит, 2007, 73–78.

[30] Hua L-K., On the number of solutions of Tarry's problem, Acta Sci. Sinica, 1, 1952, 1–76.

Для целого идеала $Q$ рассмотрим тригонометрическую сумму

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

где

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

многочлен, коэффициенты которого порождают дробный идеал вида $A(f)=\frac{B\delta^{-1}}{Q}$, где $\delta$ — дифферента, а $B$ — целый идеал с $(B,Q)=1$.

В частности, мы получим разные оценки таких сумм.

Во-первых, нам нужны некоторые результаты о сравнениях по модулю простого идеала и некоторых общих свойствах тригонометрических сумм.

**Лемма 2.1.**[31] 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 $m$.

**Предложение 2.1.**[31] 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. Тогда число решений сравнения

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

учитывая их кратность, не превосходит $m$.

**Лемма 2.2.**[31] Пусть $P$ — простой идеал, а $f$ — многочлен с целыми коэффициентами. Пусть $a$ — корень кратности $\lambda$ 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 $\lambda$.

[31] Wang Yuan, Diophantine Equations and Inequalities in Algebraic Number Fields, Springer Verlag, Berlin, Heidelberg, 1991, p. 15.

Следующая лемма показывает свойство ортогональности тригонометрических сумм.

**Лемма 2.3.**[32] Пусть $Q$ — целый идеал, а $\alpha \in R$ — целое число. Пусть $\eta$ пробегает полную систему вычетов $(Q\delta)^{-1}$ по модулю $\delta^{-1}$. Тогда

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

Следующая лемма показывает свойство мультипликативности тригонометрических сумм.

**Лемма 2.4.**[32] Пусть $A = (\alpha_m, \ldots, \alpha_1), Q, Q_1, Q_2, B$ — целые идеалы такие, что

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

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

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

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

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

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

Более того, $\pi$ всегда обозначает элемент $R$ такой, что $\pi \in P, \pi \notin P^2$[33].

Сначала мы представляем обобщение метода деревьев Хуа Ло-кена и получаем соответствующие оценки тригонометрических сумм.

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

Рассматриваем суммы

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

где

[32] Wang Yuan, Diophantine Equations and Inequalities in Algebraic Number Fields, Springer Verlag, Berlin, Heidelberg, 1991, p. 16.

[33] Knapp A., Basic Algebra, Birkhäuser Boston, 2006, p. 441.

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

**Лемма 2.5.**[34] Если $l \geq 2(t+1)$, и $v$ не является решением сравнения $\pi^{n-t} f'(v) \equiv 0 \mod P$, то

$$S_v = 0.$$

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

$$f_1(y) = f(\pi y + v) - f(v) = \sum_{j=1}^{m} \pi^j \tilde{\alpha}_{j,1} y^j = \sum_{j=1}^{m} \alpha_{j,1} y^j,$$

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

**Лемма 2.6.**[35] 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 $P$.

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. Также пусть $t_k$ — наибольшее рациональное целое число такое, что $P^{t_k} | A(f_k')A(f_k)^{-1}$. Определим $w$ как наибольшее рациональное целое число такое, что $P^w | k$ для некоторого $1 \leq k \leq m$. Повторяем эту конструкцию до шага с номером $h$, который определяется условиями

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

Используя следующее предложение и индукцию по лемме 2.6, получаем теорему 2.1.

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

$$t_k \leq w.$$

**Теорема 2.1.** Если $h > 0$, то

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

[34] Чубариков В.Н., О кратных рациональных тригонометрических суммах над полем алгебраических чисел, Чебышевский сб., 22:4 (2021), 306–323.

[35] Чубариков В.Н., О кратных рациональных тригонометрических суммах над полем алгебраических чисел, Чебышевский сб., 22:4 (2021), 306–323.

где $U_k = \sum_{j=1}^{k} u_k$, и штрих означает, что суммирование ведется по решениям сравнений $\pi^{n-U_k-t_k} f_k'(v_k) \equiv 0 \mod P$, для $0 \le k \le h-1$, в полной системе вычетов по модулю $P$.

Приведем три вспомогательных утверждения для доказательства оценки теоремы 2.2.

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

**Предложение 2.3.** Имеем

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

**Лемма 2.8.** Имеем цепочку неравенств

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

**Теорема 2.2.** Справедлива оценка

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

Теперь мы представим несколько усилений оценки Хуа Ло-кена для тригонометрических сумм. Представляем три вспомогательных результата для получения оценки в теореме 2.3.

**Предложение 2.4.**[36] Пусть $N > 1$ — вещественное число, а $k, r, \lambda_1, \dots, \lambda_r$ — рациональные целые числа такие, что $1 \le r \le k$ и $\lambda_1, \dots, \lambda_r > 0$. Тогда

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

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

**Лемма 2.10.** Справедливо тождество $w = (e+1)\left\lfloor \frac{\ln m}{\ln q} \right\rfloor$.

**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

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

Более того, справедлива конкретная оценка

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

где

[36] Архипов Г.И., Карацуба А.А., Чубариков В.Н., Теория кратных тригонометрических сумм. — М. : Наука, Физматлит, 1987, стр. 56.

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

Теперь в теореме 2.4 представляем усиленную версию теоремы 2.3 в частном случае, когда $\mathbb{K}$ имеет число классов равен 1, и $A=\frac{B}{P^n}$, где $(B,P)=1$. В доказательстве используется следующая лемма об ортогональности.

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

Тогда

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

**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

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

Используя следующее предложение, теорему 2.4 и свойства ортогональности, получаем теорему 2.5 в нашем частном случае.

**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 $d$.

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

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

Наконец, возвращаясь к общему случаю, объединяем теоремы 2.1 и 2.3 и получаем следующую новую оценку.

**Теорема 2.6.** Справедлива оценка

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

В **третьей главе** обобщается формула А.Г. Постникова[37] 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,[38][39] касающегося мультипликативной структуры систем приведенных вычетов по модулю степени простого идеала.

Начнем со следующей технической леммы, которая нам понадобится для обобщения формулы А. Г. Постникова на случай степени двойки.

**Лемма 3.1.** Имеет место неравенство

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

для любого целого $t \geq 1$.

Приведем наше обобщение формулы А.Г. Постникова[40].

**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

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

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

Тогда

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

(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 $\Lambda$ — решение сравнения

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

причем сравнение разрешимо и $\Lambda$ нечетное.

---

[37]Постников А.Г., О сумме характеров по модулю, равного степени простого числа, Изв. АН СССР. Сер. матем., 19:1 (1955), 11–16.

[38]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, Vol. 5, 2010, no. 56, 2795–2808.

[39]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, Vol. 6, 2011, no. 12, 565–589.

[40]Аль-Ассад Х., О сумме характеров по модулю, равного степени простого числа 2, Чебышевский сб., 23:2 (2022), 201–208.

Приведем классическую оценку И.М. Виноградова[41] для сумм Вейля, которая нам понадобится для получения оценки сумм характеров.

**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

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

то имеет место оценка

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

Получаем оценку сумм характеров по модулю степени числа 2, используя вышеприведенное обобщение формулы А. Г. Постникова и оценки И. М. Виноградова.

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

Тогда имеет место оценка

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

Используем следующее предложение, чтобы доказать полезное следствие теоремы 3.3.

**Предложение 3.1.** Максимальное значение суммы

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

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

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

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

Теперь опишем мультипликативную структуру приведенных систем вычетов по модулю степени простого идеала.

[41] Виноградов И.М., Избранные труды, Издательство Академии наук СССР, 1952, стр. 389.

Сначала получаем следующее простое разложение.

**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

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

Теперь представим одну вспомогательную лемму и одно техническое предложение, которые нам понадобятся в описании мультипликативной структуры приведенных систем вычетов по модулю степени простого идеала.

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

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

**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

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

Следующие две теоремы (частные случаи теоремы 4[42]) и соответствующие им следствия описывают мультипликативную структуру приведенных систем вычетов по модулю степени неразветвленного простого идеала, и структуру соответствующей группы характеров.

**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.

**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

[42]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, Vol. 5, 2010, no. 56, 2795–2808.

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r} \mathbb{Z}/q^{n-1}\mathbb{Z}\right) \oplus (R/P)^\times \cong \left(\bigoplus_{j=1}^{r} \left(\mathbb{Z}/q^n\mathbb{Z}\right)^\times_1\right) \oplus (R/P)^\times.$$

Следовательно, каждое $u \in (R/P^n)^\times$ выражается однозначно в виде

$$u = (a, u_1, \ldots, u_r);\ a \in (R/P)^\times,\ 0 \le u_j < q^{n-1}.$$

**Следствие 3.3.** Пусть $P$ — простой идеал, и $N(P) = q^r$, где $q$ — нечетное простое число такое, что $q \nmid \Delta$, и пусть $n \ge 1$ — целое число. Тогда каждый элемент $\chi$ группы характеров $(R/P^n)^\times$ однозначно выражается как

$$\chi(u) = e^{2\pi i\left(\sum_{j=1}^{r} \frac{m_j \mathrm{ind}(1+qu_j)}{q^{n-1}}\right)} \chi_P(a),$$

где $\chi_P$ — характер группы $(R/P)^\times$, а $m_j$ — целые числа такие, что $1 \le m_j \le q^{n-1}$, ind обозначает соответствующую функцию индекса в соответствующей подгруппе $(\mathbb{Z}/q^n\mathbb{Z})^\times_1$ в разложении в прямую сумму следствия 3.2[43], а $a$ и $u_j$ определены в следствии 3.2.

**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

$$(R/P^n)^\times_1 \cong \left(\bigoplus_{j=1}^{r-1} \mathbb{Z}/2^{n-1}\mathbb{Z}\right) \oplus \mathbb{Z}/2^{n-2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

где группы справа — аддитивные.

**Следствие 3.4.** Пусть $P$ — простой идеал, и $N(P) = 2^r$, где $2 \nmid \Delta$, и пусть $n \ge 3$ — целое число.

Тогда имеем разложение в прямую сумму

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r-1} \mathbb{Z}/2^{n-1}\mathbb{Z}\right) \oplus \mathbb{Z}/2^{n-2}\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus (R/P)^\times \cong$$

$$\cong \left(\bigoplus_{j=1}^{r-1} \left(\mathbb{Z}/2^{n+1}\mathbb{Z}\right)^\times_{1,1}\right) \oplus \left(\mathbb{Z}/2^n\mathbb{Z}\right)^\times_{1,1} \oplus \left(\mathbb{Z}/4\mathbb{Z}\right)^\times_{1,1} \oplus (R/P)^\times.$$

Следовательно, каждое $u \in (R/P^n)^\times$ выражается в виде $u = (a, u_1, \ldots, u_r, u_{r+1})$, с

$$a \in R/P^\times,\ 0 \le u_1, \ldots, u_{r-1} < 2^{n-1},\ 0 \le u_r < 2^{n-2},\ u_{r+1} \in \{0, 1\}.$$

**Следствие 3.5.** Пусть $P$ — простой идеал, и $N(P) = 2^r$, где $2 \nmid \Delta$, и пусть $n \ge 2$ — целое число. Тогда каждый элемент $\chi$ группы характеров $(R/P^n)^\times$ однозначно выражается как

$$\chi(u) = \pm e^{2\pi i\left(\sum_{j=1}^{r-1} \frac{m_j \mathrm{ind}(1+2u_j)}{2^{n-1}}\right)} e^{2\pi i \frac{m_r \mathrm{ind}(1+2u_r)}{2^{n-2}}} \chi_P(a),$$

[43] Apostol T., Introduction to Analytic Number Theory, Springer-Verlag, 1976, p.219.

где $\chi_P$ — характер группы $(R/P)^\times$, а $m_j$ — целые числа такие, что $1 \leq m_1, \ldots, m_{r-1} \leq 2^{n-1}, 1 \leq m_r \leq 2^{n-2}$, 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[44], а $a$ и $u_j$ определены в следствии 3.4.

Следующие три теоремы (частично теоремы 2, 3 и 4[45]) описывают мультипликативную структуру приведенных систем вычетов по модулю степени разветвленного простого идеала. Следствия о структуре соответствующих групп характеров аналогичны следствиям после теорем 3.4 и 3.5, поэтому не будем их приводить.

**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 приведенного $q-$корня из единицы.

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 $q-$корень из единицы.

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

[44] Apostol T., Introduction to Analytic Number Theory, Springer-Verlag, 1976, p. 219.

[45] 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, Vol. 6, 2011, no. 12, 565–589.

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r(n_e-1)} \mathbb{Z}/q^2\mathbb{Z}\right) \oplus \left(\bigoplus_{j=1}^{r(e-n_e+1)} \mathbb{Z}/q\mathbb{Z}\right) \oplus (R/P)^\times.$$

Если $\frac{qe}{q-1} + 1 \le n \le 2e+1$, 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 $2e+2 \le n$, 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 $n \ge 2$ — целое число.

Если $n \le e$, то

$$(R/P^n)^\times \cong \left(\bigoplus_{j=1}^{r(n-1)} \mathbb{Z}/2\mathbb{Z}\right) \oplus (R/P)^\times.$$

Если $e+1 \le n$, то

$$(R/P^n)^\times \cong \left(\bigoplus_{k=1}^{e} \left(\bigoplus_{j=1}^{r} \mathbb{Z}/2^{\lceil \frac{n-k}{e} \rceil}\mathbb{Z}\right)\right) \oplus (R/P)^\times.$$

Для полноты приведем оригинальную формулу А.Г. Постникова[46].

**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

$$\frac{\mathrm{ind}_g(1+qu)}{q-1} \equiv \Lambda f(u) \mod q^{n-1}.$$

Пусть $k = k'q^\tau$, где $\tau, k' \in \mathbb{Z}$, и $(k', q) = 1$.

Тогда

[46]Постников А.Г., О сумме характеров по модулю, равного степени простого числа, Изв. АН СССР. Сер. матем., 19:1 (1955), 11–16.

$$a_k = (-1)^{k+1} q^{k-1-\tau} x_k$$

(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 $\Lambda$ — решение сравнения

$$\frac{\mathrm{ind}_g(1+q)}{q-1} \equiv \Lambda f(1) \mod q^{n-1}$$

причем сравнение разрешимо и $(\Lambda, q) = 1$.

Теперь сформулируем основной результат этой главы. Используя теоремы 3.4, 3.5, 3.6, 3.7 и 3.8 и их соответствующие следствия о соответствующих группах характеров, а также оригинальную формулу А.Г. Постникова и ее обобщение, мы преобразуем некоторые суммы характеров в $\mathbb{K}$ в суммы Вейля в $\mathbb{Q}$, которые затем оцениваем с помощью классической оценки И.М. Виноградова.

**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

$$\Big| \sum_S \chi(u) \Big| \le |A||A'| \prod_{j \notin \{j_1 \dots, j_h\}} \Big( (8l)^{\frac{\tau(b_j)}{6lw(b_j)}} b_j^{1-w(b_j)} + (8l)^{\frac{\tau(c_j)}{6lw(c_j)}} c_j^{1-w(c_j)} \Big).$$

# Заключение

Перечислим основные результаты работы:

- Характеризуются, с точностью до кратных квадратов целых рациональных чисел, пары целых рациональных чисел, которые можно представить в виде суммы трех квадратов с общим квадратом.
- Получена усиленная оценка Хуа Ло-кена для тригонометрических сумм в полях алгебраических чисел в ряде случаев.
- Обобщается метод деревьев Хуа Ло-кена на поля алгебраических чисел и получены соответствующие оценки тригонометрических сумм.
- Обобщается формула А.Г. Постникова на случай степени числа 2.
- Применяется формула А.Г. Постникова для оценки некоторых сумм характеров в полях алгебраических чисел.

# Благодарность

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.

# Публикации автора по теме диссертации

**Статьи в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ**

1. *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).
   (0,69 п.л./ авторский вклад 0,69 п.л.)
2. *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).
   (1,69 п.л./ авторский вклад 1,69 п.л.)

3. *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).
(0,5 п.л./ авторский вклад 0,5 п.л.)

4. *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).
(0,19 п.л./ авторский вклад 0,19 п.л.)