

Одеський національний університет імені І. І. Мечникова
Факультет математики, фізики та інформаційних технологій
Кафедра комп'ютерної алгебри та дискретної математики

Дипломна робота

на здобуття ступеня вищої освіти «магістр»

на тему: **«Суми Гауса над кільцем цілих гаусових чисел»**
«Gauss sums over a ring of the Gaussian integers»

Виконала: студентка денної форми навчання
спеціальності 111 Математика
Чабанюк Мирослава Валеріївна

Керівник: д. ф.-м. н., проф. Варбанець П. Д.

Рецензент: к. ф.-м. н., доц. Варбанець С. П.

Рекомендовано до захисту:
Протокол засідання кафедри
№ ____ від ____ р.

Захищено на засіданні ЕК №
протокол № ____ від ____ р.
Оцінка ____/____/____

Завідувач кафедри

Голова ЕК

ЗМІСТ

Вступ	3
Скінченні поля та мультиплікативні характери.....	5
Скінченні поля.....	5
Мультиплікативні характери	9
Приклад мультиплікативного характеру: символ Лежандра	12
Розширення поля та кільця цілих чисел.....	15
Розширення поля.....	15
Кільця алгебраїчних цілих чисел у полях розширення $\mathbb{Q}$	16
Кільце цілих Гауссових чисел $\mathbb{Z}[i]$	22
Кільце $\mathbb{Z}[\omega]$	25
Суми Гаусса і Якобі	31
Суми Гаусса	31
Суми Якобі.....	32
Рівняння виду $x^n + y^n = 1$ у F_p для $n = 2$ або 3	37
Закон взаємності квадратичних лишків	40
Закон взаємності кубічних лишків.....	42
Суми Гаусса (другого типу).....	45
Леми про дробові частини лінійної функції.....	48
Тригонометрична сума з многочленом другого степеня	52
Висновок	54
Список використаної літератури.....	55

ВСТУП

У цій роботі ми дослідимо структуру кільця цілих алгебраїчних чисел у будь-якому квадратичному розширенні поля раціональних чисел $\mathbb{Q}$, розробимо концепції сум Гаусса та Якобі та застосуємо теорію алгебраїчних цілих чисел та теорію суми Гаусса-Якобі для розв'язування задач, пов'язаних з конгруенціями (порівняння за модулем), степеневими сумами, а також доведення квадратних і кубічних законів взаємності.

Зокрема, ми розглянемо проблему, коли раціональне просте число (тобто просте у $\mathbb{Z}$) залишається простим у кільці алгебраїчних цілих чисел у будь-якому квадратичному розширенні $\mathbb{Q}$, розглянемо, коли раціональне просте число можна записати як суму двох квадратів і знайти кількість розв'язків рівнянь конгруентності виду $x^n + y^n \equiv 1 \pmod{p}$, коли $n = 2$ або 3 .

Поняття звичайних цілих чисел $0, \pm 1, \pm 2, \pm 3, \dots$, нам знайомі. Зауважимо, що кожне ціле число r – корінь полінома $x - r$, який являється монічним із звичайними цілими коефіцієнтами. Тоді для нас буде природно розширити поняття звичайних цілих чисел і визначити алгебраїчні цілі числа як комплексні числа, що є коренями деякого монічного многочлена із звичайними цілими коефіцієнтами. Отже, алгебраїчні цілі числа включають не лише звичайні цілі числа. Наприклад, $i = \sqrt{-1}$ – ціле алгебраїчне число, оскільки воно є коренем полінома $x^2 + 1$.

Тепер розглянемо множину $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. Легко перевірити, що всі елементи множини – цілі алгебраїчні числа, оскільки будь-який $a + bi \in \mathbb{Z}[i]$ являється коренем полінома $x^2 - 2a + (a^2 + b^2)$, і що множина $\mathbb{Z}[i]$ утворює кільце при звичайному додаванні та множенні комплексних чисел. $\mathbb{Z}[i]$ ми називаємо кільцем Гауссових цілих чисел.

Зауважимо, що звичайне просте число $p \in \mathbb{Z}$ має таку властивість: якщо ab ділиться на p для $a, b \in \mathbb{Z}$, то a ділиться на p , або b ділиться на p (Тут, $x \in \mathbb{Z}$ ділиться на p означає $x = pq$ для деякого $q \in \mathbb{Z}$). Звичайно, ми можемо розширити як поняття подільності, так і простих елементів на $\mathbb{Z}[i]$, визначивши елемент $p \in \mathbb{Z}[i]$ як простий, коли p задовольняє властивість, що якщо ab ділиться на p на $a, b \in \mathbb{Z}[i]$, тоді a ділиться на p , або b ділиться на p (Тут $x \in \mathbb{Z}[i]$ ділиться на p означає $x = pq$ для деякого $q \in \mathbb{Z}[i]$). Тоді ми виявимо, що 2 більше не є простим числом у $\mathbb{Z}[i]$, оскільки добуток $1 + i$ ділиться на 2 та $1 - i$, але не ділить жодного з них окремо в $\mathbb{Z}[i]$. З іншого боку, 3 є простим і в $\mathbb{Z}$, і в $\mathbb{Z}[i]$. Це спостереження призводить до цікавого питання: коли просте число в $\mathbb{Z}$

залишається простим у $\mathbb{Z}[i]$? Більш загально, коли просте число в $\mathbb{Z}$ залишається простим у кільці цілих алгебраїчних чисел у будь-якому квадратному розширенні $\mathbb{Q}$? Щоб уникнути плутанини, ми будемо говорити про прості числа в $\mathbb{Z}$ як про раціональні прості числа.

Іншим цікавим (і класичним) питанням в теорії чисел є те, за яких умов раціональне просте число можна записати як суму квадратів двох цілих чисел у $\mathbb{Z}$. Якщо ми визначимо норму Гауссового цілого числа $a + bi \in \mathbb{Z}[i]$ через $N(a + bi) = a^2 + b^2$, наведене вище питання еквівалентно тому, за яких умов раціональне просте число буде нормою деякого цілого Гауссового числа. Виявляється, раціональне просте p – це сума квадратів двох цілих чисел у $\mathbb{Z}$ тоді і тільки тоді, коли $p = 2$ або $p \equiv 1 \pmod{4}$, як ми побачимо далі.

Звичайно, крім кільця цілих Гауссових чисел $\mathbb{Z}[i]$, існують і інші кільця алгебраїчних цілих чисел. Нехай $\omega = \frac{-1+\sqrt{-3}}{2}$ у цій роботі. Кільце $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ представлятиме для нас особливий інтерес, оскільки закон кубічної взаємності буде викладений через кубічні характери примарних елементів у $\mathbb{Z}[\omega]$. Щоб довести закон кубічної взаємності, ми розробимо концепції сум Гаусса і Якобі, які також будуть використані для доведення закону квадратної взаємності та для підрахунку кількості розв'язків рівнянь конгруентності виду $x^n + y^n \equiv 1 \pmod{p}$, коли $n = 2$ або 3 .

ВИСНОВОК

У цій роботі було досліджено структуру кільця цілих алгебраїчних чисел у будь-якому квадратичному розширенні поля раціональних чисел $\mathbb{Q}$, розроблені концепції сум Гаусса та Якобі, застосована теорія алгебраїчних цілих чисел та теорія суми Гаусса-Якобі для розв'язування задач, пов'язаних з конгруенціями (порівняння за модулем), степеневими сумами, а також доведення квадратних і кубічних законів взаємності.

Як бачимо, концепції цілих алгебраїчних чисел і сум Гаусса та Якобі надзвичайно сильні; дійсно, їх можна використовувати для вирішення широкого кола завдань теорії чисел.

Список використаної літератури

1. Виноградов И.М. Основы теории чисел. / И.М. Виноградов. – М.: Наука, 1963. – 180 с.
2. Бухштаб А.А. Теория чисел. / А.А. Бухштаб. – М.: Учпедгиз, 1966. – 384 с.
3. Лидл Р. Конечные поля. / Р. Лидл, Г. Нидеррайтер. – Т.І. – М.: Мир, 1988. – 426 с.
4. Давентроп Г. Мультипликативная теория чисел. / Г. Давентроп – М.: Мир, 1966. – 198 с.
5. Даммет Д. Абстрактная алгебра/ Д. Даммет, Р. Фут – М.: Wiley, 2003. – 944 с.
6. Айерленд К. Классическое введение в современную теорию чисел. /К. Айерленд, М. Роузен. – М.:Мир, 1987. – 419 с.