Прикарпатський національний університет імені Василя Стефаника

Факультет математики та інформатики

Кафедра алгебри та геометрії

ДИПЛОМНА РОБОТА

на здобуття першого (бакалаврського) рівня вищої освіти

на тему «Застосування цілих гаусових чисел»

Виконала: студентка 4 курсу, групи М-41

спеціальності Е7 «Математика»

Казибрід М. М.

Керівник: к.ф.-м.н., доц. Гаврилків В. М.

Рецензент: к.ф.-м.н., доц. Мазуренко Н. І

Івано-Франківськ – 2025 р.

Прикарпатський національний університет імені Василя Стефаника

Факультет математики та інформатики

Кафедра алгебри та геометрії

Освітній рівень: «бакалавр»

Спеціальність: Е7 Математика

Затверджено на засіданні кафедри алгебри та геометрії

Протокол № 2 від 21.10.2024 р.

Завідувач кафедри Никифорчин О. Р.

ЗАВДАННЯ

НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Казибрід Марії Михайлівні

1. Тема роботи: «Застосування цілих гаусових чисел»

2. Керівник роботи: к.ф.-м.н., доцент Гаврилків В. М.

3. Перелік питань, які потрібно розробити: Розкрити алгебраїчну природу кільця цілих гаусових чисел: означення, основні властивості, норма, простота, факторизація; проаналізувати геометричне та аналітичне подання гаусових чисел, побудувати ґраткову структуру на комплексній площині; дослідити застосування гаусових чисел у розв’язуванні діофантових рівнянь; розглянути роль гаусових чисел у криптографії, зокрема в решіткових криптографічних схемах; показати застосування гаусових чисел в обробці сигналів (FFT) та економічних розрахунках; реалізувати прикладні алгоритми у Python та проаналізувати результати.

4. Дата видачі завдання: 21.10.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Строк виконання етапів роботи	Примітка
1.	Попереднє вивчення стану питання у науці й практиці	21.10.2024-29.10.2024	Виконано
2.	Обґрунтування актуальності дослідження	01.11.2024-04.11.2024	Виконано
3.	Вивчення алгебраїчних та геометричних властивостей гаусових чисел	05.11.2024-27.11.2024	Виконано
4.	Аналіз застосування гаусових чисел у теорії чисел, криптографії та економіці	03.12.2024-07.01.2025	Виконано
5.	Реалізація алгоритмів у Python	15.01.2025-17.02.2025	Виконано
6.	Аналіз та узагальнення результатів	21.02.2025-16.03.2025	Виконано
7.	Оформлення результатів дослідження	18.03.2025-02.05.2025	Виконано
8.	Підготовка матеріалів до захисту дипломної роботи	01.06.2025-17.06.2025	Виконано

АНОТАЦІЯ

до дипломної роботи на здобуття першого (бакалаврського) рівня вищої освіти

Казибрід Марії Михайлівни

на тему:

«Застосування цілих гаусових чисел»

Дипломна робота присвячена дослідженню алгебраїчних, геометричних та прикладних властивостей цілих гаусових чисел — комплексних чисел із цілими дійсною та уявною частинами. Метою дослідження є аналіз структури кільця гаусових чисел та вивчення можливостей його застосування у теоретичних і прикладних задачах сучасної математики.

У дипломній роботі проаналізовано алгебраїчну природу гаусових чисел, зокрема їх подільність, простоту, факторизацію, а також властивість евклідовості, що забезпечує можливість ділення з остачею. Розглянуто геометричне уявлення гаусових чисел як ґратки на комплексній площині та використання норми як метричної характеристики. Особливу увагу приділено застосуванню гаусових чисел у розв’язуванні діофантових рівнянь, побудові криптографічних схем на основі решіток, цифровій обробці сигналів із використанням алгоритмів швидкого перетворення Фур'є (FFT), а також в економічному моделюванні. У роботі реалізовано низку алгоритмів на мові Python та подано приклади їх практичного застосування в задачах оптимізації, кодування та візуалізації даних.

Загальний обсяг роботи становить 55 сторінок, з них основний текст — 40.

Ключові слова: гаусові числа, алгебраїчна структура, факторизація, діофантові рівняння, криптографія, ґратка, FFT, Python, математичне моделювання.

ABSTRACT

to the diploma paper for obtaining the first (bachelor) level of higher education

Mariia Mykhailivna Kazybrid

on the topic:

«Application of Gaussian Integers»

The paper is devoted to the study of the algebraic, geometric, and applied properties of Gaussian integers — complex numbers with integer real and imaginary parts. The aim of the research is to analyze the structure of the ring of Gaussian integers and to explore its applications in both theoretical and applied areas of modern mathematics.

The thesis investigates the algebraic nature of Gaussian integers, including divisibility, primality, factorization, and the Euclidean property, which allows division with remainder. A geometric interpretation of Gaussian integers is presented as a regular lattice on the complex plane, with special focus on the use of the norm as a metric characteristic. Particular attention is paid to the application of Gaussian integers in solving Diophantine equations, constructing lattice-based cryptographic systems, digital signal processing (especially via Fast Fourier Transform), and economic modeling. The practical part of the thesis includes algorithm implementation in Python, with examples in optimization, coding, and data visualization.

The total volume of the work is 55 pages, of which the main text is 40.

Keywords: Gaussian integers, algebraic structure, factorization, Diophantine equations, cryptography, lattice, FFT, Python, mathematical modeling.

ЗМІСТ

ВСТУП

У сучасній математиці важливу роль відіграє дослідження структури чисел, які виходять за межі звичайної арифметики. Одним із таких об’єктів є цілі гаусові числа — комплексні числа з цілими дійсною та уявною частинами. Вони становлять не лише інтерес як алгебраїчна структура, а й відкривають нові можливості для розв’язання фундаментальних задач у теорії чисел, криптографії, обробці сигналів та математичному моделюванні. Гаусові числа є підмножиною комплексних чисел виду $a + bi$, де $a, b \in Z$, а $i^2 = -1$. Вони утворюють комутативне кільце $Z[i]$, у якому можна виконувати звичні арифметичні операції, розглядати подільність, прості елементи, розклади та інші алгебраїчні властивості.

Актуальність теми:

Актуальність дослідження зумовлена широким спектром застосування гаусових чисел у сучасній математиці та суміжних галузях. Завдяки їхній структурі та нормі, вони є ключовим інструментом для вирішення діофантових рівнянь, побудови ефективних алгоритмів факторизації, кодування інформації та побудови криптографічних схем. Особливо важливим є те, що гаусові числа дозволяють розширити класичну арифметику цілих чисел на комплексну площину, зберігаючи при цьому багато її фундаментальних властивостей.

Також важливо зазначити, що концепція гаусових чисел має глибоке історичне коріння. Вперше ці об'єкти були досліджені Карлом Фрідріхом Гаусом у контексті вивчення двочленних форм та теорії квадратичних форм. Його праці започаткували нову епоху в алгебрі та теорії чисел, яка й донині розвивається в сучасних математичних дослідженнях.

У наш час гаусові числа активно використовуються не лише в теоретичній математиці, але й у прикладних напрямах, таких як цифрова обробка сигналів (особливо в реалізації алгоритмів БПФ — швидкого перетворення Фур’є),

моделювання геометричних структур, криптографія на базі ґраток, а також оптимізаційні обчислення в економіці.

Мета роботи:

Метою дипломної роботи є дослідження властивостей цілих гаусових чисел як елементів алгебраїчної структури та аналіз їх застосування в теоретичних і прикладних задачах.

Завдання дослідження:

1. Проаналізувати алгебраїчну структуру кільця $Z[i]$ та його основні властивості.
2. Вивчити поняття подільності, простоти та факторизації в кільці гаусових чисел.
3. Розглянути геометричне представлення гаусових чисел на комплексній площині.
4. Дослідити застосування гаусових чисел у теорії діофантових рівнянь, криптографії та обробці сигналів.
5. Реалізувати прикладні задачі з використанням гаусових чисел на практиці (алгоритми, обчислення, моделювання).

Об'єкт дослідження:

Цілі гаусові числа як елементи алгебраїчного кільця та їх геометричні, арифметичні та структурні властивості.

Предмет дослідження:

Властивості подільності, простоти, факторизації та алгоритмічне застосування гаусових чисел у математичному аналізі та прикладних задачах.

Методи дослідження:

- Теоретичний аналіз літературних джерел з теорії чисел і алгебри.
- Побудова математичних моделей.

- Геометрична інтерпретація числових структур.
- Реалізація прикладних алгоритмів у комп’ютерній системі.

Структура роботи:

Дипломна робота складається зі вступу, чотирьох розділів, що включають теоретичну та прикладну частини, висновків, списку використаних джерел та додатків. У першому розділі розглянуто базові поняття та алгебраїчні властивості гаусових чисел. Другий розділ присвячено їх геометричному тлумаченню. Третій розділ демонструє приклади використання в теорії чисел, криптографії та економіці. У четвертому наведено комп’ютерні моделі й алгоритми для обробки даних із залученням гаусових чисел.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЦІЛИХ ГАУСОВИХ ЧИСЕЛ

1.1 Визначення, властивості, алгебраїчна структура

Цілі гаусові числа становлять одну з найпростіших форм алгебраїчного розширення множини цілих чисел. Це комплексні числа вигляду

$z = a + bi$, де $a, b \in Z,\ i^2 = -1$, тобто такі, у яких дійсна та уявна частини — цілі числа. Множина всіх таких чисел утворює так зване кільце цілих гаусових чисел, що позначається $Z[i]$.

Поняття алгебраїчного розширення

Кільце $Z[i]$ — це найпростіше прикладне розширення звичайного кільця Z. У ньому додано елемент i, що є розв'язком рівняння $x^2 + 1 = 0$, яке не має розв'язків у Z. Таким чином, $Z[i]$ є цілим підкільцем поля комплексних чисел C, побудованим як множина всіх виразів вигляду $a + bi$, де $a, b \in Z$.

Це кільце є прикладом так званого квадратичного розширення — одновимірного алгебраїчного розширення над Z, яке породжується елементом i. У цьому контексті елементи $Z[i]$ розглядають як лінійні комбінації з цілими коефіцієнтами основи $\{1, i\}$, тобто $Z[i] = Z + iZ$ [1, с.5].

Алгебраїчна структура кільця $Z[i]$

Кільце $Z[i]$ є комутативним кільцем з одиницею, що задовольняє усі аксіоми кільця. Формально, воно має такі властивості:

- Комутативність додавання: $z_1 + z_2 = z_2 + z_1$ для всіх $z_1, z_2 \in Z[i]$;
- Асоціативність додавання і множення:

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3),$$

$$(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3);$$

- Існування нейтрального елемента:
  $0 = 0 + 0i$ — нейтральний елемент для додавання,
  $1 = 1 + 0i$ — нейтральний елемент для множення;

- Наявність оберненого до додавання: для кожного $z \in Z[i]$, існує $-z \in Z[i]$, такий що $z + (-z) = 0$;
- Розподільність:
  $z \cdot (w + v) = z \cdot w + z \cdot v$.

Завдяки цим властивостям, $Z[i]$ задовольняє всі вимоги до абстрактного кільця. Крім того, кільце $Z[i]$ не є полем, оскільки не кожен ненульовий елемент має обернений до множення, але воно має важливу властивість: у наступних підрозділах буде доведено, що це кільце є евклідовим кільцем [15, с.8].

Елементний склад кільця

Кожне гаусове число — це пара цілих чисел (a, b), які можна подати у вигляді точки на комплексній площині. Таким чином, елементи $Z[i]$ мають таку структуру:

- Якщо $b = 0$, то $z = a \in Z$, тобто $Z \subset Z[i]$;
- Якщо $a = 0$, то $z = bi$, де $b \in Z$, що відповідає уявним числам із цілим коефіцієнтом;
- Якщо $a, b \neq 0$, то $z \in Z[i] \setminus Z$, і такий елемент є істинно комплексним.

Основна одинична підгрупа

У кільці $Z[i]$ існує чотири так звані одиниці або оборотні елементи — це ті елементи, що мають обернений до множення в межах кільця. Формально,

$$u \in Z[i] \text{ — оборотний елемент } \Leftrightarrow \exists\, v \in Z[i]\colon u \cdot v = 1.$$

Такими елементами є:

$$\pm 1, \pm i.$$

Ці чотири елементи утворюють мультиплікативну групу $U(Z[i])$, яка є циклічною групою порядку 4. Наявність декількох одиниць створює основу для поняття асоційованості: два елементи $z, w \in Z[i]$ називаються асоційованими, якщо $z = u \cdot w$ для деякої одиниці u [8, с.16].

Комплексне спряження

Ще однією важливою операцією, що не порушує меж кільця $Z[i]$, є операція комплексного спряження. Для будь-якого $z = a + bi$, спряженим вважається $\bar{z} = a - bi$. Ця операція інволютивна (тобто $\bar{\bar{z}} = z$) та зберігає цілісність чисел.

Комплексне спряження не змінює належність до кільця, але змінює знак уявної частини. Це дає симетрію в алгебраїчному аналізі та дозволяє пізніше визначити норму та формулювати твердження про модуль, факторизацію та подільність [3, с.34].

Роль у теорії чисел

Кільце $Z[i]$ є основою для побудови більш загальних кілець цілих чисел у квадратичних полях. Саме це кільце було першим нетривіальним прикладом у роботах Карла Фрідріха Гауса, який використовував гаусові числа для розв'язання задач про подільність та класи залишків.

У подальших розділах буде показано, що $Z[i]$ — не просто кільце з «приємними» властивостями, а ще й структура, яка дозволяє формулювати та доводити точні твердження про факторизацію, ділення, евклідові алгоритми та геометричні уявлення.

1.2 Арифметика в кільці гаусових чисел

Арифметика в кільці цілих гаусових чисел $Z[i]$ є фундаментальною складовою теорії алгебраїчних чисел і являє собою розширення класичної арифметики цілих чисел Z. На відміну від Z, де кожне число є елементом одновимірного впорядкованого кільця, $Z[i]$ — це двовимірне комплексне кільце, в якому дійсна та уявна частини обмежені до цілих чисел. Його елементи мають вигляд $a + bi$, де $a, b \in Z$, а $i^2 = -1$. Основна відмінність

арифметики $Z[i]$ полягає в тому, що звичні властивості операцій потребують розширення і адаптації до нової структури.

У цьому підпункті розглядаються основні операції в $Z[i]$, включаючи додавання, множення, спряження, оборотні елементи, асоційованість та ділення з остачею.

Арифметичні операції

Нехай $z_1 = a + bi$ та $z_2 = c + di$, де $a, b, c, d \in Z$:

- Додавання:

$$z_1 + z_2 = (a + c) + (b + d)i$$

- Віднімання:

$$z_1 - z_2 = (a - c) + (b - d)i$$

- Множення:

$$z_1 \cdot z_2 = (ac - bd) + (ad + bc)i$$

Ці операції зберігають цілісність: сума, різниця та добуток двох елементів $Z[i]$ завжди належать до $Z[i]$. Операції є комутативними та асоціативними, множення дистрибутивне відносно додавання [4, с. 123].

Оборотні елементи в $Z[i]$

Оборотними елементами в $Z[i]$ називаються ті елементи, які мають мультиплікативне обернення в цьому ж кільці. У Z оборотними елементами є лише ± 1. У $Z[i]$ це:

$$U(Z[i]) = \{\pm 1, \pm i\}.$$

Кожен із цих елементів має норму 1. Якщо u — одиниця, то для будь-якого $z \in Z[i]$ множення на u не змінює норму, факторизацію або клас залишків. Це означає, що всі інші елементи $Z[i]$ можна поділити на класи, які відрізняються лише множенням на одиницю.

Асоційовані елементи

Два гаусові числа z і w називаються асоційованими, якщо існує одиниця $u \in Z[i]$, така що $z = uw$. Це поняття надзвичайно важливе при розгляді факторизації, оскільки всі асоційовані елементи в $Z[i]$ мають однакові множники з точністю до одиниці [1, с.11]. Наприклад:

$$1 + i \sim -i(1 + i) = 1 - i.$$

Спряження

Для будь-якого $z = a + bi \in Z[i]$, спряженим елементом є $\bar{z} = a - bi$. Ця операція не лише змінює знак уявної частини, але й забезпечує основи для визначення норми, побудови ділення, симетрії та формування ряду аналітичних властивостей. У $Z[i]$ спряження є інволютивним: $\bar{z} = z$, і задовольняє:

$$\overline{z_1 + z_2} = \bar{z_1} + \bar{z_2}, \qquad \overline{z_1 \cdot z_2} = \bar{z_1} \cdot \bar{z_2}.$$

Ці властивості дозволяють зберігати алгебраїчну структуру при переході до спряжених елементів [15, с. 4].

Ділення з остачею

Незважаючи на те, що $Z[i]$ не є полем, у ньому можливе ділення з остачею, що є ознакою евклідовості кільця. Для будь-яких $\alpha, \beta \in Z[i]$, де $\beta \neq 0$, існують $q, r \in Z[i]$ такі, що:

$$\alpha = \beta q + r, \text{ де } r = 0 \text{ або } N(r) < N(\beta).$$

Цей факт буде ключовим для побудови алгоритму Евкліда, обчислення НСД та доведення унікальності факторизації в наступних підпунктах.

Особливості і важливість

Арифметика в $Z[i]$ дозволяє узагальнити звичні поняття на більш складні структури. Наприклад:

- Оборотні елементи визначають класи еквівалентності елементів;
- Асоційованість допомагає уникати дублювання в розкладах;
- Спряження забезпечує симетричність та об’єднання алгебри з геометрією;

- Ділення з остачею дозволяє формулювати ефективні алгоритми, зокрема алгоритм Евкліда.

Ці елементи створюють повноцінну арифметичну систему в $Z[i]$, яка є не лише корисною в теоретичній математиці, а й лежить в основі практичних застосувань — від криптографії до цифрової обробки сигналів [5, с.86].

1.3 Норма, простота і факторизація

Цей підпункт присвячено ґрунтовному аналізу трьох фундаментальних понять у кільці цілих гаусових чисел $Z[i]$: норми, простоти та факторизації. Разом вони формують математичну основу для визначення подільності, аналізу множників, а також реалізації алгоритмів у цьому кільці, включно з алгоритмом Евкліда та побудовою канонічного розкладу.

Норма в $Z[i]$

Означення (Норма)

Нехай $z = a + bi \in Z[i]$, де $a, b \in Z$. Нормою елемента z називається число:

$$N(z) \coloneqq z \cdot \bar{z} = (a + bi)(a - bi) = a^2 + b^2.$$

Це — відображення $N: Z[i] \to N_0$, яке надає кожному гаусовому числу невід'ємне ціле число, що відображає його "розмір" [14, с.43].

Властивості норми

- Невід'ємність:

$N(z) \geq 0$ для всіх $z \in Z[i]$.

Норма ніколи не може бути від'ємною, бо є сумою квадратів двох цілих чисел.

- Нульова норма:

$$N(z) = 0 \iff z = 0.$$

Жоден ненульовий елемент $Z[i]$ не має норми 0.

- Мультиплікативність:

$$N(z \cdot w) = N(z) \cdot N(w), \quad \forall z, w \in Z[i].$$

Доведення властивості мультиплікативності:

Нехай $z = a + bi, w = c + di$, де $a, b, c, d \in Z$.

Тоді:

$$z \cdot w = (a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

Обчислимо норму добутку:

$$N(zw) = (ac - bd)^2 + (ad + bc)^2$$

Розкриємо дужки:

$= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 = a^2(c^2 + d^2) + b^2(c^2 + d^2) = (a^2 + b^2)(c^2 + d^2) = N(z) \cdot N(w)$

Це дає змогу реалізувати ділення з остачею, алгоритм Евкліда та перевірку подільності [12, с.7].

Інваріантність до спряження:

$$N(z) = N(\bar{z}).$$

Характеристика одиниць:

$$N(z) = 1 \iff z \in \{\pm 1, \pm i\}.$$

Узгодженість із Z:

Для будь-якого $z = a \in Z \subset Z[i]$:

$$N(a) = a^2.$$

Приклади:

- $N(1 + i) = 1 + 1 = 2$
- $N(3 + 4i) = 9 + 16 = 25$
- $N(-2 - i) = 4 + 1 = 5$

Простота в $Z[i]$

Означення (Простий елемент)

Елемент $p \in Z[i]$ називається простим, якщо:

1. $p \neq 0$,
2. $p \notin \{\pm 1, \pm i\}$,
3. з $p = ab \Rightarrow$ або a, або b — одиниця.

Це аналог поняття простих чисел у Z, однак у $Z[i]$ є суттєві відмінності.

Класифікація простих з Z *у* $Z[i]$*:*

- Якщо $p \in Z$, $p \equiv 3 \; mod \; 4$, то p — просте в $Z[i]$.
- Якщо $p \in Z$, $p \equiv 1 \; mod \; 4$, то:

$\exists \, a, b \in Z$ такі, що $p = a^2 + b^2$,тобто $p = (a + bi)(a - bi)$.

- 2 — спеціальний випадок:

$$2 = (1 + i)^2 \cdot i.$$

Означення (Асоційовані елементи)

Два елементи $z1, z2 \in Z[i]$ називаються асоційованими, якщо:

$$\exists \, u \in \{\pm 1, \pm i\}: \;\; z_1 = u \cdot z_2.$$

Асоційовані елементи мають однакову норму та ту саму роль у факторизаціях.

Приклади:

- 3 — просте в $Z[i]$, бо $3 \equiv 3 \; mod \; 4$
- $5 = (2 + i)(2 - i)$ — не просте
- $13 = (3 + 2i)(3 - 2i)$
- $2 = (1 + i)^2 \cdot i$ — складене

- $2 + i \sim -i(2 + i) = 1 - 2i$ — асоційовані

Факторизація в $Z[i]$

Означення (Факторизація)

Факторизацією елемента $z \in Z[i]$ називається його подання у вигляді:

$$z = p_1 \cdot p_2 \cdots p_k,$$

де кожен p_i — простий елемент у $Z[i]$.

Властивості:

- $Z[i]$ є областю головних ідеалів (PID)
- $Z[i]$ є кільцем унікального розкладу (UFD):
  Розклад є унікальним з точністю до:
  - порядку множників
  - множення кожного множника на одиницю

Теорема (Унікальність факторизації)

Якщо елемент $z \in Z[i]$ має два розклади на прості:

$$z = p_1 \cdot \cdots \cdot p_k = q_1 \cdot \cdots \cdot q_k,$$

то існує перестановка σ та одиниці u_i, такі що:

$$p_i = u_i \cdot q_{\sigma(i)} \quad \forall i.$$

Доведення:

Розглянемо кільце $Z[i]$ — воно є евклідовим доменом із нормально визначеною нормою $N(z) = a^2 + b^2$. У кожному евклідовому кільці виконується основна теорема арифметики, а саме: існує єдиний (з точністю до асоційованості та перестановки) розклад ненульового елемента на добуток простих [9, с.30].

Нехай елемент $z \in Z[i]$ має два різні розклади на добутки простих елементів:

$$z = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell.$$

Оскільки $Z[i]$ — евклідів домен, то і цілісний факторіальний домен, тому усі прості елементи є незвідними, а всі незвідні — прості. Отже, згідно з теоремою про унікальність факторизації в факторіальному кільці, існує перестановка σ та оборотні елементи (одиниці) u_i, такі що:

$$p_i = u_i \cdot q_{\sigma(i)} \quad \forall i.$$

Це й доводить унікальність факторизації в $Z[i]$.

Практичні аспекти:

- Оборотні елементи не змінюють структуру факторизації.
- Спряжені множники (типу $a + bi$ і $a - bi$) входять у факторизацію парно.
- Асоційовані множники — це фактично один і той самий множник у різній формі.

Приклади:

- $2 = (1 + i)^2 \cdot i$
- $5 = (2 + i)(2 - i)$
- $13 = (3 + 2i)(3 - 2i)$
- 7 — просте, бо $7 \equiv 3 \ mod \ 4$

Поняття норми, простоти і факторизації у $Z[i]$ утворюють замкнену систему, що забезпечує всі необхідні властивості для ефективного алгебраїчного аналізу [2, с.5].

- Норма визначає порядок і дає змогу реалізувати ділення.
- Прості елементи — це неподільні блоки алгебраїчної структури.
- Факторизація — це унікальне подання будь-якого елемента як добутку простих.

Ці три інструменти є наріжним каменем теорії гаусових чисел, на якому будується подальший теоретичний і прикладний аналіз.

РОЗДІЛ 2. ГЕОМЕТРИЧНЕ Й АНАЛІТИЧНЕ ПРЕДСТАВЛЕННЯ ГАУСОВИХ ЧИСЕЛ

2.1 Ґраткова структура на комплексній площині

Кільце гаусових чисел $Z[i]$ — це множина комплексних чисел вигляду $z = a + bi$, де $a, b \in Z$, а i — уявна одиниця, така що $i^2 = -1$. Геометричне представлення елементів $Z[i]$ на комплексній площині дає змогу інтерпретувати це кільце як регулярну двовимірну ґратку в евклідовому просторі R^2.

Означення ґратки

Ґратка (решітка) в R^2— це множина всіх цілих лінійних комбінацій двох лінійно незалежних векторів v_1 і $v_2 \in R^2$:

$$\lambda = Z \cdot v_1 + Z \cdot v_2.$$

У випадку $Z[i]$, базисом ґратки є вектори $(1,0)$ і $(0,1)$, які відповідають числам 1 та i. Отже, кожне гаусове число $z = a + bi$ відображається в точку з координатами $(a, b) \in Z^2$ [13, с.2]. Таким чином, $Z[i]$ ототожнюється з квадратною ґраткою на площині.

Геометричні властивості ґратки $Z[i]$

- Ґратка є регулярною, з рівновіддаленими точками по горизонталі й вертикалі.
- Відстань між сусідніми точками дорівнює 1.
- Ґратка інваріантна до паралельних зсувів на вектори $(1,0)$ та $(0,1)$.
- Базисні вектори ортонормальні: кут між ними — $90°$, довжина кожного — 1.
- Площа елементарної комірки дорівнює 1:

$$Area = |\det\big((1,0),(0,1)\big)| = 1.$$

Алгебраїчні операції як геометричні

- Додавання чисел у $Z[i]$ відповідає векторному додаванню:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \leftrightarrow (a + c, b + d).$$

- Множення реалізує обертання та масштабування на площині. Наприклад, множення на i — це поворот на $90°$ проти годинникової стрілки навколо початку координат [15, с.102].

Норма як квадрат відстані

Норма числа $z = a + bi \in Z[i]$ визначається як:

$$N(z) = a^2 + b^2.$$

Це відповідає квадрату евклідової відстані від точки (a, b) до початку координат $(0,0)$. Таким чином, множина всіх гаусових чисел з однаковою нормою лежить на колі радіуса $\sqrt{N(z)}$.

Підґратки в $Z[i]$

Добутки елемента $Z[i]$ на ціле число або на інше гаусове число формують підґратки. Наприклад:

- $\lambda = Z \cdot (1 + i)$: одновимірна ґратка.
- $\lambda = Z \cdot (1 + i) + Z \cdot (2 - i)$: повна двовимірна ґратка.

Площа елементарного паралелограма такої ґратки визначається як модуль визначника, утвореного координатами базисних векторів.

Модульна структура ґратки

Ґратка дозволяє побудову фактор-кілець виду $Z[i]/(m)$, де $m \in Z[i]$. У цьому випадку всі елементи, які лежать в однакових позиціях різних клітинок періодичної ґратки, належать до одного класу залишків за модулем m [9, с.2]. Це має важливе значення для конгруентностей, криптографії та побудови систем залишків.

Застосування ґраткової структури

- У криптографії — як базова структура для криптографії на решітках.
- У теорії чисел — при дослідженні рівнянь $a^2 + b^2 = n$.
- У геометрії чисел — для пакування куль і оцінки щільності.
- У теорії кодування — як частина двовимірних сигналів та модуляцій.
- У дослідженні фактор-кілець — для побудови $Z[i]$ −алгебр.

Ґраткова структура $Z[i]$ — це не лише геометрична візуалізація кільця гаусових чисел, а й ключ до глибокого розуміння його алгебраїчної, метричної та модульної природи.

2.2 Метричні властивості та застосування в геометрії чисел

Гаусові числа, як елементи кільця $Z[i]$, природно відображаються на комплексній площині як точки з координатами (a, b), де $z = a + bi$. Таке відображення дозволяє розглядати $Z[i]$не лише як алгебраїчну, але й як геометричну структуру, зокрема — як двовимірну евклідову ґратку. У цьому розділі розглянемо основні метричні характеристики цієї ґратки та їх застосування в геометрії чисел [6, с.17].

Відстань та евклідова метрика

Означення:

Нехай $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i \in Z[i]$. Тоді відстань між ними визначається як:

$$d(z_1, z_2) \coloneqq | z_1 - z_2 | = \sqrt{(a_1 - a_2)^2 + (b_1 - b_2)^2}.$$

Це звичайна евклідова метрика у R^2, яка дає змогу вивчати геометричні властивості кільця $Z[i]$ [4, с.22].

Норма як квадрат відстані

Норма $N(z) = z \cdot \bar{z} = a^2 + b^2$ є квадратом відстані від точки z до початку координат $(0,0)$. Отже:

$$| z |= \sqrt{N(z)}.$$

Це дозволяє застосовувати поняття кола, сферичних шарів і ізометрій для аналізу просторового розташування елементів $Z[i]$.

Кути і спрямування

Множення на комплексне число в $Z[i]$ реалізує обертання. Наприклад, множення на i обертає всю ґратку на $90°$ проти годинникової стрілки. Відношення $\frac{z_1}{z_2}$, якщо $z_2 \neq 0$, задає комплексну аргументну різницю між векторами z_1 і z_2, що дозволяє інтерпретувати кути між векторами у геометричному сенсі [14, с.8].

Щільність пакування ґратки

Ґратка $Z[i]$ є однією з найщільніших двовимірних ґраток з ортогональним базисом. Площа одиничної комірки дорівнює 1, а мінімальна відстань між сусідніми точками — також 1.

Означення:

Щільністю ґратки $\lambda \subset R^2$ називається величина:

$$\delta(\lambda) = \frac{\pi r^2}{vol(\lambda)},$$

де r — радіус вписаного круга, $vol(\lambda)$ — площа елементарної комірки.

Для ґратки $Z[i]$ маємо:

- $r = \frac{1}{2}$
- $vol = 1$

Отже:

$$\delta(Z[i]) = \frac{\pi \cdot (\frac{1}{2})^2}{1} = \frac{\pi}{4} \approx 0.785.$$

Це — максимальна щільність для квадратної упаковки у двох вимірах.

Найкоротші вектори

Найкоротшими ненульовими векторами в $Z[i]$ є елементи з нормою 1:

$$N(z) = 1 \iff z \in \{\pm 1, \pm i\}.$$

Наступний рівень — числа з нормою 2 (наприклад, $1 \pm i$) [2, с.19]. Вони формують "пояс" навколо початку координат. Такі вектори часто використовуються в задачах про найменші представники залишкових класів.

Застосування в геометрії чисел

Метричні властивості ґратки $Z[i]$ знаходять широке застосування у класичних і сучасних задачах:

- Розв’язування рівнянь у цілих числах, таких як $x^2 + y^2 = n$. Кожен розв’язок відповідає точці ґратки на колі радіуса $\sqrt{n}$.
- Теорема Гаусса–Ферма**:** якщо просте число $p \equiv 1 \ mod \ 4$, то воно представляється як сума двох квадратів. Геометрично це — точка на колі радіуса $\sqrt{p}$, яка належить ґратці $Z[i]$.
- Оцінка кількості точок у крузі: задача про число елементів $Z[i]$ з нормою, меншою за задане R^2, зводиться до підрахунку точок у крузі радіуса R з центром у нулі.
- Лінійні обмеження на ґратці: задачі виду $a_1 x + a_2 y = c$, де $x, y \in Z$, можуть бути геометрично зображені як прямі, що проходять через ґратку.

Приклад:

Знайдемо кількість гаусових чисел $z = a + bi$, для яких $N(z) \leq 5$.

Шукаємо всі пари $(a, b) \in Z^2$, для яких $a^2 + b^2 \leq 5$. Отримаємо:

- Норма 0: $(0,0)$
- Норма 1: $(\pm 1,0), (0, \pm 1)$
- Норма 2: $(\pm 1, \pm 1)$
- Норма 4: $(\pm 2,0), (0, \pm 2)$
- Норма 5: $(\pm 2, \pm 1), (\pm 1, \pm 2)$

Загалом: 1 (нуль) $+ 4 + 4 + 4 + 8 = 21$ елемент.

Метричні властивості $Z[i]$ дозволяють вивчати це кільце не лише як алгебраїчну, а і як геометричну структуру з евклідовою метрикою. Відстані, кути, норми, щільність та підрахунок точок дають потужний інструментарій для розв'язання задач теорії чисел, теорії решіток, а також для практичних застосувань — у криптографії, цифрових обчисленнях та аналізі сигналів.

2.3 Гаусові числа у теорії форм і квадратів

Кільце гаусових чисел $Z[i]$, як підмножина комплексних чисел, тісно пов'язане з класичною теорією представлення цілих чисел у вигляді суми двох квадратів [12, с.52]. Алгебраїчна структура $Z[i]$ дозволяє здійснювати ефективний аналіз таких подань за допомогою факторизації та норм.

Представлення чисел як суми квадратів

Означення:

Ціле число $n \in N$ представляється у вигляді суми двох квадратів, якщо існують такі $a, b \in Z$, що:

$$n = a^2 + b^2.$$

Теорема Ферма:

Просте число $p \in Z$ можна представити у вигляді $a^2 + b^2$ тоді і лише тоді, коли $p = 2$ або $p \equiv 1 \; mod \; 4$.

Доведення:

Нехай p — просте число у Z. Ми розглянемо кільце гаусових чисел $Z[i]$, в якому визначено норму:

$$N(a+bi) = a^2 + b^2.$$

Необхідність:

Якщо $p = a^2 + b^2$, то у $Z[i]$ маємо:

$$p = (a+bi)(a-bi),$$

тобто p розкладається у $Z[i]$ на два (необов'язково прості) множники, кожен з нормою p.

Але у Z просте p не розкладається. Отже, p не є простим у $Z[i]$. З теорії факторизації в $Z[i]$ відомо, що таке відбувається лише тоді, коли $p = 2$ або $p \equiv 1 \, mod \, 4$. Тобто:

- Якщо $p \equiv 3 \, mod \, 4$, то p залишається простим у $Z[i]$, і не може бути представлений як сума двох квадратів.

Достатність:

Нехай $p \equiv 1 \, mod \, 4$. Тоді за теоремою про розклад простого в $Z[i]$ маємо:

$$p = \pi \cdot \bar{\pi},$$

де $\pi = a + bi \in Z[i]$, $\bar{\pi} = a - bi$, і π — непростий у $Z[i]$.
Отже:

$$p = (a+bi)(a-bi) = a^2 + b^2.$$

Таким чином, p подається як сума двох квадратів.

Норма і факторизація в $Z[i]$

У кільці $Z[i]$, для будь-якого $z = a + bi$, визначена норма:

$$N(z) = z \cdot \bar{z} = a^2 + b^2.$$

Таким чином, задача представлення $n \in N$ як суми двох квадратів еквівалентна задачі знаходження $z \in Z[i]$, для якого $N(z) = n$ [3, с.64].

Представлення простих чисел

Теорема:

Нехай $p \in Z$ — просте число. Тоді:

- Якщо $p \equiv 3\ mod\ 4$, то p — просте також у $Z[i]$ і не представимо як сума двох квадратів.
- Якщо $p \equiv 1\ mod\ 4$, то існує $z \in Z[i]$, таке що $N(z) = p$, тобто:

$$p = a^2 + b^2.$$

Приклади:

- $5 = (2 + i)(2 - i) = 4 + 1$
- $13 = (3 + 2i)(3 - 2i) = 9 + 4$

Бінарні квадратичні форми

Означення:

Бінарною квадратичною формою називається функція вигляду:

$f(x, y) = ax^2 + bxy + cy^2$, де $a, b, c \in Z$.

Форма $f(x, y) = x^2 + y^2$ — одна з найпростіших, пов'язаних із гаусовими числами, оскільки:

$$f(a, b) = N(a + bi).$$

Це дозволяє інтерпретувати подання чисел як значення цієї квадратичної форми в цілих точках.

Дискримінант і відповідне поле

Форма $x^2 + y^2$ має дискримінант:

$$D = b^2 - 4ac = 0^2 - 4 \cdot 1 \cdot 1 = -4.$$

Цей дискримінант збігається з дискримінантом поля $Q(i)$, що додатково підтверджує зв'язок квадратичної форми $x^2 + y^2$ з кільцем $Z[i]$ [13, с.29].

Унікальність представлень

Унікальність представлення числа n як суми двох квадратів у $Z[i]$ тісно пов'язана з властивістю унікального розкладу на прості. Зокрема, для:

$$n = a^2 + b^2 = (a + bi)(a - bi),$$

розклад у $Z[i]$ є унікальним з точністю до:

- порядку множників;
- множення на оборотні елементи $\{\pm 1, \pm i\}$.

Кількість представлень

Кількість пар цілих чисел (a, b), таких що $a^2 + b^2 = n$, дорівнює кількості елементів $z \in Z[i]$ з нормою n, з урахуванням спряження та асоційованості.

Для простого $p \equiv 1 \, mod \, 4$, таких представлень завжди 8:
$\pm(a \pm bi)$, $\pm(b \pm ai)$, що відповідає дії групи автоморфізмів $Z[i]$.

Кільце $Z[i]$ є природним середовищем для дослідження задач подання цілих чисел у вигляді суми квадратів. Його норма відображає значення квадратичної форми $x^2 + y^2$, а структура факторизації дає змогу ефективно вирішувати питання існування й кількості таких подань [1, с.48]. Таким чином, теорія гаусових чисел повністю узгоджується з класичною теорією квадратичних форм і розширює її засобами алгебраїчної теорії чисел.

РОЗДІЛ 3. ЗАСТОСУВАННЯ В ТЕОРІЇ ЧИСЕЛ, КРИПТОГРАФІЇ ТА ЕКОНОМІЦІ

3.1 Розв'язування діофантових рівнянь

Діофантові рівняння — це рівняння з цілими коефіцієнтами, для яких шукаються цілі або раціональні розв'язки. Вони є центральним об'єктом дослідження в теорії чисел і відіграють важливу роль у математиці від античності до сьогодення.

Застосування гаусових чисел $Z[i]$ (множини чисел вигляду $a + bi$, де $a, b \in Z$ дає потужний інструмент для розв'язання широкого класу діофантових рівнянь, зокрема таких, що пов'язані з квадратами, модулями та геометрією чисел.

Загальне означення

Означення 1.1.

Діофантовим називається рівняння виду:

$$f(x_1, x_2, \dots, x_n) = 0, \qquad f \in Z[x_1, \dots, xn],$$

для якого шукаються розв'язки $x_1, \dots, x_n \in Z$ або Q.

Класифікація діофантових рівнянь

- Лінійні: $ax + by = c$
- Квадратичні: $x^2 + y^2 = n,\ x^2 - dy^2 = 1$
- Вищого степеня: $x^3 + y^3 = z^3$ тощо
- Системи діофантових рівнянь
- Параметричні задачі з обмеженнями

Особливо цікаві — квадратичні рівняння, бо саме до них застосування гаусових чисел є максимально природним і ефективним [4, с.36].

Гаусові числа в контексті рівняння $x^2 + y^2 = n$

Рівняння $x^2 + y^2 = n$ є центральним у класичній арифметиці. Його геометричне тлумачення — це опис точок решітки Z^2, що лежать на колі радіуса $\sqrt{n}$.

Теорема Ферма:

Просте число $p \in Z$ представляється у вигляді $a^2 + b^2$ тоді й лише тоді, коли:

$$p = 2 \text{ або } p \equiv 1 \, mod \, 4.$$

Доведення:

Якщо $p \equiv 1 \, mod \, 4$, то p не є простим у $Z[i]$, бо:

$$p = (a + bi)(a - bi), N(a + bi) = p.$$

Таким чином, існує $z \in Z[i]$, таке що $N(z) = p \Rightarrow p = a^2 + b^2$.

Загальний підхід через $Z[i]$

Нехай потрібно знайти цілі x, y, що задовольняють:

$$x^2 + y^2 = n.$$

Кроки:

1. Розкласти n у $Z[i]$:

$$n = z \cdot \bar{z}$$

2. Обчислити $z = a + bi$ — один із множників.
3. Знайти $a, b \in Z$:

$$n = N(z) = a^2 + b^2.$$

Приклади:

Приклад 1.

Знайдемо представлення 13 у вигляді $x^2 + y^2$.

Оскільки $13 \equiv 1 \, mod \, 4$, розкладається у $Z[i]$:

$$13 = (3 + 2i)(3 - 2i), \qquad \Rightarrow x = 3, y = 2.$$

Приклад 2.

Число $29 = 5^2 + 2^2 = 25 + 4$

Отже, $z = 5 + 2i, N(z) = 29 \Rightarrow$ розв'язок існує.

Суміжні рівняння

Піфагорові трійки:

Знаходимо цілі x, y, z такі, що:

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

Відомо, що всі примітивні рішення мають вигляд:

$$x = m^2 - n^2, \qquad y = 2mn, \qquad z = m^2 + n^2,$$

де $m > n,\ m, n \in Z$, одного з них — парне, і $gcd(m, n) = 1$. Цей параметричний опис тісно пов'язаний із гаусовими числами:

$$(m + ni)^2 = m^2 - n^2 + 2mni.$$

Лінійні діофантові рівняння і $Z[i]$

Рівняння $ax + by = c$ в Z можна вирішити стандартними методами. У $Z[i]$ аналогічно:

$$z_1 x + z_2 y = z_3, \text{ де } z_i \in Z[i].$$

Існує розв'язок $(x, y) \in Z[i]^2$ тоді й лише тоді, коли $gcd(z_1, z_2) \mid z_3$ [11, с.18]. Це дозволяє застосовувати алгоритм Евкліда в $Z[i]$ і знаходити розв'язки у вигляді:

$$x = x_0 + \frac{z_2}{d}t, \qquad y = y_0 - \frac{z_1}{d}t,\ t \in Z[i].$$

Системи діофантових рівнянь

Системи рівнянь виду:

$$\begin{cases} x^2 + y^2 = n \\ x = y = k \end{cases}$$

можуть бути зведені до однієї змінної і далі — до задачі у $Z[i]$, використовуючи властивості спряження та симетрії.

Алгоритмічні аспекти

Розв'язування діофантових рівнянь через $Z[i]$ має переваги:

- Можна використовувати алгоритм Евкліда для знаходження НСД.
- Можна застосовувати розклади на прості з урахуванням норм.
- Є можливість перевірки існування розв'язку за нормою.
- Дає природну геометричну інтерпретацію.

Розв'язування діофантових рівнянь є класичною задачею, яка завдяки гаусовим числам отримує нове алгебраїчно-геометричне тлумачення [4, с.7]. Кільце $Z[i]$, зі своєю структурою факторизації, нормою, спряженням та евклідовістю, дозволяє не лише формулювати розв'язки у компактному вигляді, але й доводити факти, які у Z виглядають складно.

Цей підхід є потужним інструментом у сучасній теорії чисел і природним способом опису багатьох класичних задач через призму алгебраїчних чисел.

3.2 Факторизація цілих чисел за допомогою гаусових чисел

У класичній арифметиці поняття розкладу на прості числа лежить в основі всього будівництва цілих чисел. У цьому підпункті розглянемо, як ціле число можна факторизувати не лише у кільці Z, а й у його розширенні — кільці гаусових чисел $Z[i]$. Такий підхід не тільки збагачує інструментарій теорії чисел, а й відкриває нові структури і закономірності, які не видно в класичному контексті Z.

Ідеологія факторизації в розширенні

У Z факторизація є унікальною: кожне ненульове ціле число розкладається у добуток простих, і цей розклад єдине з точністю до порядку та знаку [6, с.20].

Проте у $Z[i]$ поняття простоти набуває нового вигляду. Деякі числа, що в Z є простими, у $Z[i]$ — вже не є неподільними, бо там існує ширше коло можливих дільників. Саме це робить факторизацію в $Z[i]$ не лише продовженням, а й уточненням класичної.

Аксіоматична база: простота та неподільність

Простим в $Z[i]$ елементом називають такий $\pi \in Z[i]$, що:

- $\pi \neq 0$,
- $\pi \notin U(Z[i])$,
- і з $\pi = ab$ випливає, що або a, або b — одиниця в $Z[i]$ [7, с.47].

Але при цьому просте число в Z може перестати бути простим у $Z[i]$, якщо у новому середовищі воно розкладається на нетривіальні множники. Це фундаментальний факт, що прямо стосується процедури факторизації.

Критерії подільності та перевизначення розкладу

У $Z[i]$ число $n \in Z$ можна подати у вигляді добутку елементів, що не є простими в Z, але прості в $Z[i]$. Наприклад:

- Число 65 в $Z\ -\ 5 \cdot 13$, але в $Z[i]$:

$$65 = (2+i)(2-i)(3+2i)(3-2i)\,,$$

оскільки $5 = (2+i)(2-i)$, $13 = (3+2i)(3-2i)$, бо $5{,}13 \equiv 1\ mod\ 4$. Таким чином, факторизація "вглиблюється": ми розкладаємо складники Z-факторизації далі в $Z[i]$.

Це дозволяє виявляти внутрішню симетрію цілих чисел, яку Z приховує.

Факторизація як декомпозиція через норму

На відміну від Z, у $Z[i]$ факторизація тісно пов’язана з нормою:

$$N(a+bi) = a^2 + b^2.$$

Це дає змогу перевірити дійсність розкладу: якщо

$$n = z_1 z_2 \cdots z_k,$$

то має виконуватись:

$$n^2 = N(z_1) \cdot N(z_2) \cdots N(z_k).$$

Таким чином, норма служить контролером правильності розкладу, аналогічно до модуля у векторних просторах [12, с.74].

Побудова факторизації

Алгоритм:

1. Провести класичну факторизацію $n \in Z$.
2. Для кожного простого множника p:
   - Якщо $p \equiv 3\ mod\ 4$, залишити як є.
   - Якщо $p \equiv 1 mod\ 4$, знайти $p = a^2 + b^2$.
3. Записати $p = (a + bi)(a - bi)$ і замінити на ці множники.
4. Зібрати все разом — з урахуванням кратності.

Приклад:

Нехай $n = 325$.

У Z:

$$325 = 5^2 \cdot 13.$$

Але 5 і $13 - \equiv 1\ mod\ 4$, тож:

- $5 = (2 + i)(2 - i)$,
- $13 = (3 + 2i)(3 - 2i)$,

отже:

$$325 = (2 + i)^2(2 - i)^2(3 + 2i)(3 - 2i).$$

Це — факторизація з повним урахуванням гаусової структури. І вона єдина з точністю до асоційованості та порядку.

Теорія множників і симетрії

Кільце $Z[i]$ має 4 одиниці: $\pm 1, \pm i$. Тому кожне просте має 4 асоційовані форми:

- π,
- $-\pi$,
- $i\pi$,
- $-i\pi$.

Приклади: $1+i, -1-i, i(1+i), -i(1+i)$ — усі однакові з точки зору структури розкладу.

Це створює орбіти множників, і ми обираємо одну представницьку форму при записі факторизації.

Відношення до геометрії: факторизація як складання векторів

Факторизацію в $Z[i]$ можна бачити як:

- розклад довжини (через норму);
- розклад спрямування (через аргумент);
- побудову конструктивної симетрії на площині.

Візуально: добуток двох чисел у $Z[i]$ — це поворот і масштабування одного вектора відносно іншого [6, с.25]. Тобто, кожен множник несе не лише модульну, а і кутову інформацію.

Факторизація цілих чисел у $Z[i]$ — це не просто розклад на добуток, а виявлення внутрішньої структури числа. Така факторизація уточнює класичну, показуючи, де Z "зливає" складні симетрії в одне ціле [6, с.25]. Залучення гаусових чисел дозволяє:

- розділити прості Z на ті, що залишаються неподільними, і ті, що розпадаються;

- побачити геометрію і обертання множників;
- побудувати багатокомпонентну картину арифметики.

Це перетворює арифметичну операцію на структуру із глибокими геометричними й алгебраїчними зв'язками.

3.3 Криптографічні схеми з використанням гаусових решіток

Сучасна криптографія базується на складних математичних задачах, які складно (або неможливо) розв'язати ефективними алгоритмами. У цьому контексті решіткова криптографія (lattice-based cryptography) є одним із найперспективніших напрямів, зокрема через свою стійкість до квантових атак [10, с.6]. Центральне місце в цій галузі займають решітки, породжені на основі гаусових чисел $Z[i]$, що поєднують алгебраїчну структуру з геометричним змістом.

Поняття гаусової решітки

Означення:

Нехай $\alpha_1, \alpha_2 \in Z[i]$, лінійно незалежні над R. Тоді решітка виду:

$$\lambda = \{a\alpha_1 + b\alpha_2 \mid a, b \in Z\}$$

називається гаусовою решіткою у $C \cong R^2$.

Ці решітки є підгрупами C, що дискретні і замкнуті під додаванням, і можуть бути представлені як матриці з комплексними або дійсними коефіцієнтами [8, с.14]. У випадку, коли базисні вектори лежать у $Z[i]$, ґратка відображає арифметичну симетрію гаусових чисел.

Решіткові задачі в криптографії

У центрі криптографії на решітках лежать задачі, що важко обчислюються. Найвідоміші з них:

- SVP (Shortest Vector Problem):
  знайти найкоротший ненульовий вектор у заданій решітці.
- CVP (Closest Vector Problem):
  знайти вектор решітки, найближчий до довільної точки простору.
- LWE (Learning With Errors):
  задається система рівнянь з шумом; знайти секрет вважається складною задачею.

Ці задачі залишаються складними навіть для квантових комп'ютерів, що робить їх привабливими для постквантової криптографії.

Зв'язок з $Z[i]$ і нормами

У $Z[i]$ норма $N(z) = a^2 + b^2$ відіграє роль евклідової метрики. Якщо вектори ґратки — це елементи $Z[i]$, то їхня довжина обчислюється через норму. Таким чином, пошук найкоротшого вектора в гаусовій решітці — це пошук елемента з мінімальною нормою [5, с.17].

Це дозволяє використовувати властивості $Z[i]$ для генерації решіток зі строго контрольованою структурою, де факторизація, спряження, симетрія та обертання мають ключове значення.

Криптографічні схеми на базі решіток

Схема Рейж-Шпільмана (Regev scheme)

- Базується на задачі LWE.
- Генерується матриця $A \in Z_q^{n \times m}$ та вектор з невеликим шумом.
- Зашифроване повідомлення не дозволяє точно відновити розв'язок без секретного ключа.

Гаусові решітки можуть бути використані для побудови таких схем із використанням чисел з $Z[i]$ як базису [10, с.43].

Схеми гомоморфного шифрування

- Працюють із алгебраїчними структурами $Z[i]$, що допускають операції додавання і множення у зашифрованому вигляді.
- Решітки на основі $Z[i]$ забезпечують високий ступінь симетрії та щільність, що полегшує реалізацію.

Переваги гаусових решіток

- Компактність: базис з $Z[i]$ дозволяє зберігати коротші ключі.
- Симетричність: сприяє побудові стабільних решіткових структур.
- Метричні властивості: дозволяють використовувати норму як простий критерій для обчислень.
- Уніфікація з геометрією чисел: поєднання алгебри й геометрії робить моделі стійкішими.

Побудова решітки на $Z[i]$

Розглянемо базис:

$$\alpha_1 = 1 + i, \qquad \alpha_2 = 2 - i.$$

Тоді ґратка:

$$\lambda = \{a(1 + i) + b(2 - i) \mid a, b \in Z\}$$

є прикладом комплексної двовимірної решітки з високою щільністю. Норма кожного елемента визначає його відстань до початку координат, що безпосередньо впливає на обчислювальну складність криптографічних задач.

Гаусові решітки поєднують сильні сторони двох світів: алгебраїчну структуру $Z[i]$ та геометричні властивості евклідової площини [7, с.38]. У криптографії це дає змогу:

- формалізувати задачі як решіткові;
- спиратися на важкі задачі (LWE, SVP) для безпеки;
- створювати надійні, компактні та квантостійкі схеми.

3.4 Застосування гаусових чисел в економічних розрахунках

Хоча гаусові числа традиційно належать до області чистої математики, зокрема теорії чисел, їх структура та властивості дозволяють розглядати і потенційне застосування в економічних розрахунках. Враховуючи, що сучасна економіка дедалі активніше залучає математичні моделі високого рівня абстракції, використання гаусових чисел в аналізі, моделюванні та оптимізації цілком обґрунтоване.

Комплексні змінні в економіці

У багатьох фінансових або логістичних задачах моделювання включає дві взаємопов'язані змінні, наприклад:

- реальні та очікувані значення;
- прибуток та ризик;
- обсяг інвестиції та термін її реалізації.

Модель на основі гаусових чисел дозволяє трактувати таку пару величин як єдиний комплексний об'єкт $z = a + bi$, де a — реальна економічна змінна (наприклад, фактична вартість), а b — пов'язана оцінка (наприклад, ризик, відхилення або прогноз) [5, с.10].

Алгебраїчні операції та економічна інтерпретація

- Додавання гаусових чисел — це сумарний результат об'єднання двох пар економічних величин.
- Множення — моделює вплив взаємозалежних факторів: ефект збільшення обсягу при зростанні прибутковості.
- Норма $N(z) = a^2 + b^2$ — може інтерпретуватись як інтегральна оцінка показника ефективності, яка враховує одночасно основний результат та супутній фактор (наприклад, прибуток + ризик).

Векторизація і геометричне подання даних

Гаусові числа можна інтерпретувати як точки в R^2, що відкриває можливості:

- кластерного аналізу;
- побудови економічних графіків;
- оцінки «відстаней» між рішеннями (наприклад, між оптимальною і реальною інвестиційною стратегією).

Відстань між елементами $Z[i]$ = різниця між альтернативами.
Кут між векторами = відношення структур: наприклад, стратегія з однаковою нормою, але іншим розподілом прибутку і ризику.

Оптимізаційні задачі з цілими змінними

У задачах лінійного або цілочисельного програмування, коли змінні повинні набувати дискретних парних значень (наприклад, кількість одиниць продукції та її категорія), зручно використовувати модель на основі $Z[i]$. Вона забезпечує:

- ціле значення координат;
- компактне подання змінної у вигляді одного виразу;
- збереження симетрій та геометричних властивостей.

Балансові моделі

Балансові моделі описуються системами лінійних рівнянь [1, с.40]. Якщо взаємодія двох галузей потребує одночасної оцінки прямого та побічного ефекту, гаусове число може унаочнити цю парність:

- a — основне виробництво,
- b — вторинний вплив (енергоспоживання, викиди тощо).

Таким чином, система рівнянь набуває структури, що може бути лінійною в $Z[i]$, де фактори взаємодіють через додавання, масштабування та спряження.

Приклад (умовна модель):

Нехай підприємство має дві одиниці впливу:
дохід a та ризик b.
Модель результативності можна оцінити через:

$z = a + bi$, ефективність: $N(z) = a^2 + b^2$.

Розглянемо два варіанти інвестування:

- $z_1 = 3 + 4i \Rightarrow N(z_1) = 25$
- $z_2 = 5 + 0i \Rightarrow N(z_2) = 25$

Формально — однакова ефективність, але в z_1 більша частка ризику, що важливо для стратегії.

Гаусові числа як матричні індикатори

У великих облікових або логістичних таблицях, де відстежуються два параметри на кожну подію, запис у вигляді одного комплексного числа з $Z[i]$ дає змогу:

- зменшити кількість колонок;
- застосувати обчислення над комплексними матрицями;
- скористатись готовими алгоритмами для аналізу симетрій.

Хоча гаусові числа не є стандартним інструментом економіста, їх структура надзвичайно зручна для подання, аналізу та моделювання парних економічних величин, особливо тоді, коли взаємозв'язки мають як кількісний, так і структурний характер [4, с.62]. Завдяки поєднанню арифметики та геометрії, $Z[i]$ забезпечує унікальну платформу для розробки нових методів оптимізації, візуалізації та прийняття рішень в економічному контексті.

РОЗДІЛ 4. ПРАКТИЧНЕ ЗАСТОСУВАННЯ :КОМП'ЮТЕРНІ МОДЕЛІ ТА АЛГОРИТМИ

4.1 Використання гаусових чисел у FFT та обробці сигналів

Гаусові числа $Z[i]$, що утворюють кільце всіх комплексних чисел виду $a + bi$, де $a, b \in Z$, мають широке застосування в цифровій обробці сигналів. Зокрема, вони є ефективним засобом для реалізації дискретного перетворення Фур'є (DFT) у вигляді FFT (Fast Fourier Transform), особливо в контексті дискретних, цілих і симетричних даних.

Обґрунтування застосування $Z[i]$ у обробці сигналів

У цифрових обчисленнях використовуються кінцеві розрядності, тому застосування наближених дійсних чисел може призводити до накопичення похибок [12, с.55]. Натомість, гаусові числа дають змогу:

- точно подати пари цілих змінних у вигляді одного об'єкта;
- здійснювати обчислення у дискретному середовищі;
- уникати похибок округлення при реалізації алгоритмів FFT.

Таким чином, $Z[i]$ дозволяє побудувати дискретні аналогії для обробки спектрів, що особливо корисно у вбудованих системах або криптографічних алгоритмах.

Основи FFT у комплексній площині

Дискретне перетворення Фур'є для вектора довжини N визначається як:

$$X_k = \sum_{n=0}^{N-1} x_n \cdot e^{-\frac{2\pi i k n}{N}}, \quad k = 0,1, \dots, N-1.$$

Коли вхідні дані $x_n \in Z[i]$, це перетворення можна реалізувати повністю в $Z[i]$ або над кільцем залишків $Z[i]/(p)$ [14, с.21].

Розв'язання прикладу

Розглянемо приклад для $N = 4$, де:

$$x = [x_0, x_1, x_2, x_3] = [1 + i,\ 2 - i,\ 0,\ -1 + i] \in Z[i]^4.$$

Обчислимо DFT цього вектора за допомогою стандартного алгоритму FFT.

Крок 1: Визначення кореня

$$\omega = e^{-2\pi i/4} = -i,$$

тобто $\omega^0 = 1, \omega^1 = -i, \omega^2 = -1, \omega^3 = i.$

Крок 2: Обчислення перетворення

$$X_k = \sum_{n=0}^{3} x_n \cdot \omega^{kn}$$

X_0:

$$X_0 = (1 + i) + (2 - i) + 0 + (-1 + i) = 2 + i$$

X_1:

$$X_1 = (1 + i) \cdot 1 + (2 - i) \cdot (-i) + 0 + (-1 + i) \cdot i$$
$$= (1 + i) + (-1 - 2i) + (-1 - i) = -2 - 2i$$

X_2:

$$X_2 = (1 + i) - (2 - i) + 0 - (-1 + i) = (1 - 2 + 1) + (i + i - i) = 0 + i$$

X_3:

$$X_3 = (1 + i) + (2 - i)i + (-1 + i)(-i) = (1 + i) + (1 + 2i) + (1 + i) = 3 + 4i$$

Підсумок:

$$X = [2 + i,\ -2 - 2i,\ i,\ 3 + 4i] \in Z[i]^4$$

Інтерпретація результату

Кожне значення X_k — комплексна частотна складова, яка зберігає дискретну, цілу структуру, оскільки всі операції виконувались у $Z[i]$. Це означає:

- результати можна зберігати без втрат у точності;
- є можливість відновлення зворотного сигналу з точністю до одиниці;
- обчислення є ідеально придатними для реалізації в обмежених апаратних ресурсах.

Геометричне представлення

Елементи $Z[i]$ лежать на регулярній ґратці у R^2. FFT перетворює один набір точок (часовий домен) у новий набір (частотний домен), де:

- відстані відповідають інтенсивності складових;
- кути — фазовим зсувам;
- симетрія сприяє оптимізації обчислень.

Застосування гаусових чисел у FFT не лише дозволяє формалізувати алгоритми обробки сигналів у дискретному вигляді, але й розкриває геометричну та алгебраїчну структуру даних. Завдяки цьому можлива реалізація ефективних, цілочисельних та точних алгоритмів перетворення Фур'є, які критично важливі в комп'ютерній інженерії, обробці зображень, криптографії та телекомунікаціях.

4.2 Реалізація алгоритмів у Python

Мова програмування Python є одним із найпопулярніших інструментів для реалізації математичних алгоритмів завдяки своїй простоті, великій кількості бібліотек та активній спільноті розробників. У контексті гаусових чисел Python дозволяє ефективно створювати об'єкти, що відповідають структурі $Z[i]$, виконувати арифметичні дії над ними, а також будувати прикладні алгоритми для обробки даних.

Створення класу GaussianInteger

Python не має вбудованої підтримки кільця $Z[i]$, проте можна легко реалізувати гаусові числа за допомогою користувацького класу, це зображено на рисунку 1.

```python
class GaussianInteger:
    def __init__(self, a, b):
        self.a = a  # дійсна частина
        self.b = b  # уявна частина

    def __add__(self, other):
        return GaussianInteger(self.a + other.a, self.b + other.b)

    def __sub__(self, other):
        return GaussianInteger(self.a - other.a, self.b - other.b)

    def __mul__(self, other):
        a, b = self.a, self.b
        c, d = other.a, other.b
        return GaussianInteger(a*c - b*d, a*d + b*c)

    def conjugate(self):
        return GaussianInteger(self.a, -self.b)

    def norm(self):
        return self.a**2 + self.b**2

    def __str__(self):
        return f"{self.a} + {self.b}i"
```

Рисунок 1

Приклади використання

На рисунку 2 показано приклад використання.

```
z1 = GaussianInteger(3, 2)
z2 = GaussianInteger(1, -1)

print("z1 + z2 =", z1 + z2)
print("z1 * z2 =", z1 * z2)
print("Norm of z1:", z1.norm())
print("Conjugate of z2:", z2.conjugate())
```

Рисунок 2

Цей код дозволяє здійснювати базові обчислення у кільці $Z[i]$ та аналізувати властивості гаусових чисел, такі як спряження та норма.

Алгоритм факторизації у $Z[i]$

Реалізація функції для перевірки, чи можна просте число $p \in Z$ подати як суму квадратів двох цілих чисел, показано на рисунку 3:

```
def is_sum_of_squares(p):
    for a in range(1, int(p**0.5) + 1):
        b2 = p - a**2
        b = int(b2**0.5)
        if b * b == b2:
            return a, b
    return None
```

Рисунок 3

Наприклад, для числа 13 функція поверне $(3, 2)$, адже $3^2 + 2^2 = 13$.

Побудова FFT із використанням комплексних чисел

Можна реалізувати дискретне перетворення Фур'є для вектора з гаусових чисел, так як продемонстровано на рисунку 4:

```python
import cmath

def fft_gaussian(x):
    N = len(x)
    return [sum(x[n] * cmath.exp(-2j * cmath.pi * k * n / N) for n in range(N)) for k in range(N)]
```

Рисунок 4

Для повної роботи з гаусовими числами можна реалізувати округлення результатів до найближчих цілих значень у дійсній та уявній частинах.

Візуалізація рішень

Python дозволяє легко візуалізувати розташування гаусових чисел на комплексній площині, рисунок 5:

```python
import matplotlib.pyplot as plt

points = [GaussianInteger(a, b) for a in range(-5, 6) for b in range(-5, 6)]
x_vals = [z.a for z in points]
y_vals = [z.b for z in points]

plt.scatter(x_vals, y_vals)
plt.title("Gaussian Integers in the Complex Plane")
plt.xlabel("Real part")
plt.ylabel("Imaginary part")
plt.grid(True)
plt.axis("equal")
plt.show()
```

Рисунок 5

Мова Python є гнучким середовищем для моделювання та аналізу алгебраїчних структур. Створення користувацьких класів для гаусових чисел, реалізація алгоритмів факторизації, норм, перетворень та візуалізації дає змогу поєднувати теоретичні знання з практичними розрахунками. Це особливо цінно для наукових досліджень, освітніх задач та прототипування прикладних моделей.

4.3 Приклади розв’язання задач (економіка, кодування, оптимізація)

Розглянемо практичне застосування гаусових чисел для розв’язання задач, які виникають у таких сферах, як економічне моделювання, оптимізація процесів та кодування інформації. Властивості гаусових чисел дозволяють ефективно працювати з парними величинами (наприклад, дохід і ризик), маніпулювати комплексними представленнями даних та реалізовувати швидкі обчислення [7, с.13].

Приклад 1: Економічне моделювання — аналіз прибутку та ризику

Нехай маємо два проекти, кожен з яких представлено як гаусове число:

- Проект A: $z_1 = 10 + 3i$ — де 10 — очікуваний прибуток, 3 — ризик
- Проект B: $z_2 = 8 + 4i$

Порівняймо "ефективність" проєктів за нормою: $N(z) = a^2 + b^2$

$$N(z_1) = 10^2 + 3^2 = 109, \quad N(z_2) = 8^2 + 4^2 = 80.$$

Висновок: Проект A має більшу норму, отже, в загальному має більшу сумарну потужність (враховуючи прибуток та ризик). Якщо пріоритетом є прибуток при помірному ризику, вибираємо A.

Приклад 2: Оптимізація маршрутів (геометрична модель)

Уявимо, що переміщення в місті представлено як рух по комплексній сітці:

- Один крок на схід $= +1$
- Один крок на північ $= +i$

Маршрут A: $3 + 4i$ — 3 кроки схід, 4 північ

Маршрут B: $5 + i$ — 5 схід, 1 північ

Який маршрут коротший?

Висновок: Маршрут A коротший (менша норма). Це корисно при проектуванні логістики, де кожен крок має сталу вартість.

Приклад 3: Кодування інформації через парні компоненти

Нехай дані для передавання мають дві характеристики: сила сигналу та відхилення в шумі. Це зручно кодувати гаусовими числами:

- Сигнал: $s = 7 + 2i$
- Помилка: $e = -1 + 3i$

Прийнятий сигнал: $r = s + e = (7 - 10) + (2 + 3)i = 6 + 5i$

На приймачі можемо легко відновити оригінал: $s = r - e = 6 + 5i - (-1 + 3i) = 7 + 2i$.

Використання гаусових чисел дозволяє кодувати і обробляти багатовимірні дані у зручній формі. Як показали наведені приклади, гаусові числа мають широке практичне застосування у завданнях, де потрібно працювати з парними величинами, векторами або комплексними змінними. Їх використання спрощує обчислення, покращує візуалізацію задач і дозволяє будувати алгоритми на основі математично чітких структур.

ВИСНОВКИ

У результаті виконаної дипломної роботи було досліджено ключові властивості цілих гаусових чисел як елементів алгебраїчного кільця, а також вивчено можливості їх практичного застосування. Зокрема:

- побудовано повне уявлення про структуру кільця $Z[i]$, включно з означеннями, властивостями подільності, простоти та факторизації;
- обґрунтовано геометричну інтерпретацію гаусових чисел як точок на площині та введено поняття норми як засобу оцінки "розміру" числа;
- доведено важливі властивості норми, зокрема мультиплікативність, що має суттєве значення для факторизації;
- розглянуто унікальність розкладу гаусових чисел на прості множники, підтверджену аналогом основної теореми арифметики в $Z[i]$;
- застосовано апарат гаусових чисел для розв’язування діофантових рівнянь, зокрема на основі теореми Ферма про подання простого числа у вигляді суми квадратів;
- проаналізовано застосування гаусових чисел у сучасних криптографічних схемах, пов’язаних із решітками, та в обробці цифрових сигналів (через алгоритм БПФ);
- змодельовано прикладні задачі економіки, логістики та кодування, де гаусові числа дозволяють компактно кодувати інформацію та оптимізувати обчислення.

Таким чином, підтверджено, що цілі гаусові числа — це не лише важливий теоретичний об'єкт, але й практичний інструмент, який знаходить застосування у багатьох прикладних сферах — від теорії чисел до комп’ютерних наук.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gauss, C. F. Theoria Residuorum Biquadraticorum, Commentatio Secunda. Werke, Band II. Göttingen: Königlichen Gesellschaft der Wissenschaften, 1876. [Електронний ресурс]. – Режим доступу: https://archive.org/details/117771763002/page/n103/mode/2up

2. Zinotes Notes (Expanded). [Електронний ресурс]. – Режим доступу: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/

3. Wikipedia. Gaussian Integer. [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Gaussian_integer

4. Victor Shoup. A Computational Introduction to Number Theory and Algebra. Cambridge University Press. [Електронний ресурс]. – Режим доступу: https://shoup.net/ntb/

5. Odlyzko, A. M. Discrete logarithms in finite fields and their cryptographic significance. Advances in Cryptology, 1985.

6. Nguyen, P. Q., & Vallée, B. The LLL Algorithm: Survey and Applications. Springer, 2010.

7. Nielsen, M. A., & Chuang, I. L. Quantum Computation and Quantum Information. Cambridge University Press, 2010.

8. Conrad, K. The Gaussian Integers. [Електронний ресурс]. – Режим доступу: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf

9. Luthchenko, A. V. Точкові ґратки та їх застосування. 2019. [Електронний ресурс]. – Режим доступу: https://epub.chnpu.edu.ua/jspui/handle/123456789/9735

10. Avramenko, Kh. M. Комп'ютерна система захисту інформації з використанням гіперкомплексних числових систем: дис. – Київ, 2024. [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/items/05682cbe-b643-42c8-b2f2-0c3e995f4d0f

11. Матійко, А. А. Метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем. Київ, 2023. [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/items/77703ad6-ef14-4878-8b69-065b9839d807

12. Thierry, V. Handbook of Mathematics. BoD – Books on Demand, 2015.

13. Вікіпедія. Ґратка (порядок). [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Ґратка_(порядок)

14. ICDG2012. Gaussian Lattices. Stefka M. 2012.

15. Gaussian Integers Final Notes. Unpublished PDF.

ДОДАТКИ

Додаток А

Код реалізації алгоритму швидкого перетворення Фур'є (БПФ) для гаусових чисел

```
def fft(a):
    n = len(a)
    if n == 1:
        return a
    a_even = fft(a[0::2])
    a_odd = fft(a[1::2])
    factor = [cmath.exp(-2j * cmath.pi * k / n) for k in range(n // 2)]
    return [a_even[k] + factor[k] * a_odd[k] for k in range(n // 2)] +
[a_even[k] - factor[k] * a_odd[k] for k in range(n // 2)]
```

Додаток Б

Код перевірки простоти гаусового числа у Python

```
def norm(z):
    return z.real**2 + z.imag**2

def is_gaussian_prime(z):
    n = norm(z)
    if z.real == 0 or z.imag == 0:
        return is_prime(int(n))
    return is_prime(int(n)) and n % 4 == 1
```