ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І. І. МЕЧНИКОВА

(повне найменування закладу вищої освіти)

Факультет математики, фізики та інформаційних технологій

(повне найменування факультету)

Кафедра алгебри, геометрії та диференціальних рівнянь

(повна назва кафедри)

Кваліфікаційна робота

на здобуття ступеня вищої освіти «бакалавр»

«Суми Клостермана на еліпсі»

(тема кваліфікаційної роботи українською мовою)

«Kloosterman sums on the ellipse»

(тема кваліфікаційної роботи англійською мовою)

Виконав: здобувач заочної форми навчання

спеціальності 111 Математика

(код, назва спеціальності)

Освітня програма Математика

(назва)

Кисельов Даниїл Олегович

(прізвище, ім'я, по-батькові здобувача)

Керівник доктор фіз.-мат. наук, доцент, Варбанець С.П.

(науковий ступінь, вчене звання, прізвище, ініціали) (підпис)

Рецензент кандидат технічних наук, доцент, Якімова Н.А.

(науковий ступінь, вчене звання, прізвище, ініціали)

Рекомендовано до захисту:
Протокол засідання кафедри

№____від ..... 20____р.

Завідувач(ка) кафедри

_____ _____
(підпис) (прізвище,ім'я)

Захищено на засіданні ЕК № _____
протокол №___від ..... 20____р.

Оцінка_____/_____/_____
(за національною шкалою/шкалою ECTS/ бали)

Голова ЕК

_____ _____
(підпис) (прізвище, ім'я)

Одеса 2025

ЗМІСТ

ВСТУП

У роботі розглядаються питання, пов’язані з узагальненням класичних сум Клостермана на кільця цілих чисел уявних квадратичних полів із введенням геометричних обмежень на змінні, зокрема у вигляді рівняння еліпса. Тому перший розділ присвячений апарату класичних сум Клостермана та сум Гауса: даються їхні визначення, основні властивості та відомі оцінки.

У другому розділі роботи розглядаються «проблеми еліпса» у геометричному та аналітичному аспектах. Зокрема, аналізуються методи пошуку рівняння еліпса за заданими фокусами й вершинами, способи обчислення довжини дуги, визначення площі, а також побудова еліпса за різними геометричними умовами.

Третій розділ об’єднує теми еліптичних інтегралів, еліптичних функцій і теоретико-числових основ еліптичних кривих. У цьому ж розділі обговорюється застосування еліптичних кривих до розв’язання діофантових рівнянь, побудови криптосистем на еліптичних кривих, а також визначення рангу кривої у гіпотезі Бірча–Свиннертона–Дайєра.

Останній, четвертий розділ, власне й присвячений узагальненню сум Клостермана на кільця цілих чисел уявних квадратичних полів за умов, що змінні відповідають точкам, розташованим на фігурі еліпса. Тут формулюються головні теореми й твердження, доводяться оцінки відповідних узагальнених сум, а також аналізуються їхні наслідки для розподілу арифметичних функцій (зокрема функції дільників $\tau(n)$ у більш загальному алгебраїчному контексті).

Таким чином, структура роботи побудована таким чином, щоб послідовно вести читача від класичних результатів з теорії експоненційних сум до нових оцінок узагальнених сум Клостермана.

РОЗДІЛ 1

Огляд сум Клостермана в розрізі тригонометричних сум

Тригонометричні суми проходять етапи від простих гаусівських випадків до загальних поліноміальних форм і часто основна задача полягає в тому, щоб побудувати якомога жорсткішу верхню оцінку для їхнього модуля. Для квадратичних сум (гаусових) це було виконано Гаусом; для довільних поліномів степеня n – Вейлем і Хуа, кожен із яких отримав оцінку, що не може бути суттєво покращена в сенсі порядку зростання при збільшенні P.

Якщо $m = p$ – просте число, то для будь-якого n, що не кратно p, в $\mathbb{Z}_p$ завжди існує n^*, обернене до n:

$n^* n \equiv 1 \; mod \; p, n^* \equiv n^{p-2} \; mod \; p$

Таким чином, раціональні суми Вейля з многочленом $P_{p-1}(n) = an^{p-1} + bn$ можна записати у вигляді

$$\sum_{a<n\leq b}{}' e^{2\pi i \frac{an^* + bn}{p}} \quad (1.1)$$

Суми такого вигляду і називаються сумами Клостермана. Загалом Клостерманові суми є скінченним кільцевим аналогом функцій Бесселя. Їх можна побачити, наприклад, у Фур'є-розкладі модульних форм.

Існують прикладні задачі, пов'язані з обчисленням середніх значень: дзета-функції Рімана, аналіз простих чисел у коротких відрізках і в арифметичних прогресіях, спектральна теорія автоморфних форм та суміжні теми.

Перепишемо вигляд сум Клостермана у більш загальному вигляді задля розгляду їх властивостей

Нехай $a, b, m \in \mathbb{N}$ Тоді

$$K(a,b;m) = \sum_{\substack{0\le x\le m-1 \\ \gcd(x,m)=1}} e^{\frac{2\pi i}{m}(ax+bx^*)} \quad (1.3)$$

Розглянемо властивості сум Клостермана:

- $K(a,b;m)$ залежить лише від класу лишків a,b. Крім того, $K(a,b;m) == K(b,a;m)$ і $K(ac,b;m) = K(a,bc;m)$ якщо $gcd(c,\ m) = 1$.
- Нехай $m = m_1 m_2$ (m_1, m_2 взаємно прості). Оберемо n_1 n_2 такі що $n_1 m_1 \equiv 1$ mod m_2 and $n_2 m_2 \equiv 1$ mod m_1. Тоді

  $K(a,b;m) = K(n_2 a, n_2 b; m_1) K(n_1 a, n_1 b; m_2)$

  Дана властивість дозволяє звести знаходження суми Клостермана до випадку $m = p^k$, де p – просте і $k \ge 1$.
- Значення $K(a,b;m)$ завжди є алгебраїчним дійсним числом.
- Тотожність Сельберга:

  $$K(a,b;m) = \sum_{d|\gcd(a,b,m)} dK\left(\frac{ab}{d^2}, 1; \frac{m}{d}\right)$$

  Дана тотожність була сформульована Сельбергом, проте вперше була доведена Кузнецовим за допомогою спектральної теорії модулярних форм. Сьогодні існують простіші доведення даної тотожності.

Наведемо оцінки для сум Клостермана. Оскільки суми Клостермана зустрічаються в розкладі Фур'є модулярних форм, оцінки для сум Клостермана також дають оцінки коефіцієнтів Фур'є модулярних форм. Найвідоміша оцінка належить Андре Вейлю і стверджує: [1,2]

$K(a,b;m) \le \tau(m)\sqrt{\gcd(a,b,m)}\sqrt{m}$, де $\tau(m)$ – кількість додатних дільників m.

Враховуючи мультиплікативні властивості сум Клостермана, достатньо розглядати випадок, коли m - просте число. Ключовий прийом Вейля дозволяє зменшити оцінку до:

$|K(a,b;p)| \le 2\sqrt{p}$, де $ab \ne 0$.

З геометричної точки зору розглядають суму, що береться по точках «гіперболи» XY=ab, трактуючи це як визначення алгебраїчної кривої над скінченним полем з p елементів. Ця крива володіє розгалуженим покриттям Артіна–Шрайєра, яке накриває криву. Вейль довів, що локальна дзета-функція C розкладається на добуток, що відповідає теорії L-функції Артіна в контексті функціональних полів. У цьому зв'язку він посилався на статтю Дж. Вайссінгера 1938 року (а наступного року в своєму збірнику статей згадує роботу Хассе 1935 року як попередню ідею). Оскільки Вейль зауважив, що спеціалісти з аналітичної теорії чисел могли самостійно вивести цей приклад, можна припустити, що такі міркування вже давно існували у певному «фольклорному» вигляді. Неполярні множники дзета-функції мають вигляд $1-Kt$, де K – це сума Клостермана; звідси оцінка виходить із фундаментальної роботи Вейля. [25]

Такий підхід дозволяє показати значно ширші речі: так, наприклад, повні експоненціальні суми, узяті вздовж алгебраїчних многовидів, задовольняють жорсткі оцінки за умови дотримання гіпотез Вейля для вимірності >1. Цей напрямок суттєво розвинули П'єр Делінь, Жерар Ломон і Ніколас Кац.[17]

РОЗДІЛ 2

Проблематика питань еліпса

Загалом такого питання як проблематика питань еліпса не існує. Під цим ми маємо на увазі розгляд основних задач/питань, що пов'язані з еліпсом. Почнемо з розгляду геометричних задач, що пов'язані з еліпсом.

1) Пошук рівняння еліпса по заданим фокусам та вершинам (вісі-орієнтований еліпс)

   Нехай маємо два фокуси $F_1 = (x_1, y_1),\ F_2 = (x_2, y_2)$

   і дві головні вершини $V_1 = (x_3, y_3),\ V_2 = (x_4, y_4)$

   Припустимо, що вісь, яка проходить через V_1, V_2 паралельно осі абсцис або осі ординат. Центр C завжди лежить на середині відрізка, що з'єднує V_1, V_2.

   $C = (h, k) = (\frac{x_3+x_4}{2}, \frac{y_3+y_4}{2})$.

   Вершини V_1, V_2 лежать на головній (великій) вісі еліпса і знаходяться на відстані a від центра C.

   $2a = \sqrt{(x_4 - x_3)^2 + (y_4 - y_3)^2}$

   $a = \frac{1}{2}\sqrt{(x_4 - x_3)^2 + (y_4 - y_3)^2}$

   Але, якщо ми розглядаємо, що головна вісь паралельна або осі абсцис, або осі ординат то маємо

   - $y_3 = y_4 = k$
   - $x_3 = x_4 = h$

   Якщо $y_3 = y_4 = k$, то вершини V_1, V_2 мають координати (h-a, k) і (h+a, k).

   Тоді $a = \frac{|x_4 - x_3|}{2}$

   За визначенням еліпса, відстань від центра C до кожного з фокусів дорівнює c. Тобто

   $c = \sqrt{(x_1 - h)^2 + (y_1 - k)^2}$

Запишемо рівняння еліпса якщо головна вісь горизонтальна (аналогічно для вертикальної вісі. В цьому випадку значення знаменників зміняться місцями)

$$\frac{(x-h)^2}{a^2}+\frac{(y-k)^2}{b^2}=1$$

2) Пошук довжини дуги еліпса

Загалом довжина дуги плоскої лінії визначається за формулою

$$l=\int_{t_1}^{t_2}\sqrt{\left(\frac{dx}{dt}\right)^2+\left(\frac{dy}{dt}\right)^2}\,dt$$

Використовуючи параметричне представлення еліпсу маємо наступне

$$l=\int_{t_1}^{t_2}\sqrt{a^2\sin^2 t+b^2\cos^2 t}\,dt=[b^2=a^2(1-e^2)]=$$

$$=a\int_{t_1}^{t_2}\sqrt{1-e^2\cos^2 t}\,dt, e<1$$

3) Визначення площі еліпсу

Площа $S_{\text{еліпсу}}$ що оточена еліпсом дорівнює:

$S_{\text{еліпсу}}=\pi ab$, де a,b - довжини великої та малої півосей відповідно.

Загалом дана формула є досить інтуїтивною: почнемо з кола радіуса b(тобто його площа πb^2) та розтягнемо його на $k=\frac{a}{b}$ для того, щоб утворився еліпс. Це масштабує площу на той самий коефіцієнт, що означає $\pi b^2\frac{a}{b}=\pi ab$. Однак, використання такого ж підходу наприклад для кола є помилковим (для того, аби це зрозуміти можна перевірити $\int f(x)dx$ та $\int\sqrt{1+f'^2(x)}\,dx$) тож використаємо більш універсальний метод доведення за допомогою інтегрування.

Рівняння еліпсу можна переписати у вигляді $y(x)=b\sqrt{1-\frac{x^2}{a^2}}$.

Для $x \in [-a, a]$, дана крива є верхньою половиною еліпса. Отже подвоєний інтеграл від $y(x)$ на відрізку $[-a, a]$ буде площею еліпса:

$$S_{\text{еліпсу}} = \int_{-a}^{a} 2b\sqrt{1 - \frac{x^2}{a^2}}\,dx = \frac{b}{a}\int_{-a}^{a} 2\sqrt{a^2 - x^2}\,dx$$

Другий інтеграл це площа кола з радіусом a. Отже, маємо

$$S_{\text{еліпсу}} = \frac{b}{a}a^2\pi = \pi ab$$

4) Способи побудови еліпсу

Перетин кіл

Для кожного кута θ від F_1 на промені відкладають r, а з F_2 креслять коло радіуса 2a−r. Їх перетин дає точку P з $\mathrm{PF}_1 + \mathrm{PF}_2 = 2\mathrm{a}$.

Фокус–директриса–ексцентриситет

Маючи фокус F, пряму-директрису d і e<1, шукають точки P на променях із F так, щоб $\frac{\mathrm{PF}}{\mathrm{dist(P,d)}} = \mathrm{e}$.

Оси-паралельний (за півосями)

Відомі центр C(h,k) і півосі a,b. Відкладають вершини (h±a,k) і «ко-вершини» (h,k±b). Інші точки беруть за $\frac{(\mathrm{x}-\mathrm{h})^2}{a^2} + \frac{(\mathrm{y}-\mathrm{k})^2}{b^2} = 1$.

Допоміжна окружність (проекція)

Будують коло радіуса a із центром C. Розмічають точки на ньому, «стягуючи» вертикальну координату в b/a. У випадку повороту елліпса спершу повертають коло, потім стиснення, далі повертають назад.

5) Перехід з канонічного рівняння еліпсу в параметричну форму (і навпаки)

Канонічне → параметричне

Задамо параметр t, де $t \in [0,2\pi)$. Нехай $x = \mathrm{a}\cos t\,, y = bsin\,t$.

Перевіримо нашу гіпотезу

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=\frac{a^2\cos^2 t}{a^2}+\frac{b^2\cos^2 t}{b^2}=\cos^2 t+\sin^2 t=1$$

Параметричне → канонічне

З параметричної форми маємо $\cos t=\frac{x}{a}$, $\sin t\ =\frac{y}{b}$.

Використовуючи основну тригонометричну тотожність маємо

$$\left(\frac{x}{a}\right)^2+\left(\frac{y}{b}\right)^2=1\ \rightarrow\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$$

Також під «проблемою еліпса» розуміють дослідження еліптичних рівнянь та еліптичних функцій, що приводить нас до поняття еліптичних кривих. Проте в загальному еліптичні криві та еліпси це різні об’єкти.

Незважаючи на це, наприклад, під час знаходження довжини дуги еліпсу виникає поняття еліптичного інтегралу. Інтеграл, який ми отримали в пункті 2), під час останнього переходу належить до сімейства еліптичних інтегралів, які не виражаються в елементарних функціях. Отриманий інтеграл зводиться до еліптичного інтегралу другого роду.

Як зазначено вище, даний інтеграл неможливо виразити в елементарних функціях. Тож задля обчислення такого інтегралу надзвичайно ефективно зазвичай використовують середньо арифметичне-геометричне. Суть даного методу полягає в наступному:

Нехай a_n, g_n- послідовності, де $a_0=1, g_0=\sqrt{1-k^2}=k'$ і справджуються наступні рекурентні відношення $a_{n+1}=\frac{a_n+g_n}{2}, g_{n+1}=\sqrt{a_n g_n}$.

Нехай $c_n=\sqrt{|a_n^2-g_n^2|}$

За визначенням

$$a_\infty=\lim_{n\to\infty}a_n=\lim_{n\to\infty}g_n=agm(1,\sqrt{1-k^2})$$

Також

$$\lim_{n\to\infty} c_n = 0$$

Тоді маємо

$$E(k) = \frac{\pi}{2a_\infty}(1 - \sum_{n=0}^{\infty} 2^{n-1} c_n^2)$$

На практиці, обчислення agm значно спрощуються, якщо робити це до певної межі. Дана формула сходиться квадратично для всіх $|k| \leq 1$. Для того, щоб ще більше прискорити обчислення можна використовувати відношення $c_{n+1} = \frac{c_n^2}{4a_{n+1}}$

.

Крім того, якщо $k^2 = \lambda(i\sqrt{r})$ і $r \in \mathbb{Q}^+$, де $\lambda -$ модулярна лямбда функція , тоді E(k) можна виразити в замкнутій формі як

$$K(k) = \frac{\pi}{2agm(1, \sqrt{1-k^2})}$$

Таким чином ми можемо перейти від вирішення еліптичних інтегралів до оглядового розгляду еліптичних кривих. Загалом, еліптична крива — гладка, проективна, алгебраїчна крива роду один, на якій є задана точка O. Еліптична крива визначена над полем K і описує точки в K^2, декартів добуток K на себе. Якщо характеристика поля відрізняється від 2 та 3, то криву можна описати як плоску алгебраїчну криву, яка складається з розв'язків (x, y) для:

$y^2 = x^3 + ax + b$, для деяких $a, b \in K$

Крива має бути несингулярною, що означає, що крива не має вершин або самоперетинів. (це еквівалентно умові $4a^3 + 27b^2 \neq 0$, тобто бути

безквадратною відносно x) Завжди розуміється, що крива насправді лежить у проективній площині, а точка O є єдиною точкою на нескінченності. Багато джерел визначають еліптичну криву як просто криву, задану рівнянням такого вигляду. (коли поле коефіцієнтів має характеристику 2 або 3, наведене вище рівняння недостатньо загальне, щоб включати всі несингулярні кубічні криві)

Еліптична крива є абелевим многовидом, тобто вона має груповий закон, визначений алгебраїчно, відносно якого вона є абелевою групою, а O служить одиничним елементом.

Якщо $y^2 = P(x)$, де P - будь-який многочлен третього ступеня від x без повторюваних коренів, множина розв'язків — це неособлива плоска крива роду один, еліптична крива. Якщо P має четвертий ступінь і є безквадратичною, це рівняння знову описує плоску криву роду один; однак воно не має природного вибору одиничного елемента. У більш загальному випадку, будь-яка алгебраїчна крива роду один, наприклад, перетин двох квадратичних поверхонь, вкладених у тривимірний проективний простір, називається еліптичною кривою, за умови, що вона має позначену точку, яка діє як одиниця.

Використовуючи теорію еліптичних функцій, можна показати, що еліптичні криві, визначені над комплексними числами, відповідають вкладенням тора в комплексну проективну площину. Тор також є абелевою групою, і ця відповідність також є ізоморфізмом групи.

Еліптичні криві особливо важливі в теорії чисел і складають основну галузь сучасних досліджень; наприклад, вони були використані в доведенні Ендрю Вайлзом Великої теореми Ферма. Вони також знаходять застосування в криптографії еліптичних кривих (ECC) та цілочисельній факторизації.

Еліптична крива не є еліпсом у сенсі проективної коніки, яка має рід нуль. Однак існує природне представлення дійсних еліптичних кривих з інваріантом форми $j \geq 1$ як еліпсів у гіперболічній площині $\mathcal{H}^2$. Зокрема, перетини

гіперболоїда Мінковського з квадричними поверхнями, що характеризуються певною властивістю постійного кута, утворюють еліпси Штейнера в $\mathcal{H}^2$ (породжені колінеаціями, що зберігають орієнтацію). Крім того, ортогональні траєкторії цих еліпсів складають еліптичні криві з j ≤ 1, і будь-який еліпс в $\mathcal{H}^2$, описаний як місце розташування відносно двох фокусів, однозначно є сумою еліптичних кривих двох еліпсів Штейнера, отриманих шляхом додавання пар перетинів на кожній ортогональній траєкторії. Тут вершина гіперболоїда служить одиницею на кожній кривій траєкторії. Топологічно, комплексна еліптична крива є тором, тоді як комплексний еліпс є сферою.

Хоча формальне визначення еліптичної кривої вимагає певних знань з алгебраїчної геометрії, деякі особливості еліптичних кривих над дійсними числами можна описати, використовуючи лише вступну алгебру та геометрію.

У цьому контексті еліптична крива — це плоска крива, визначена рівнянням виду

$$y^2 = x^3 + ax + b, \text{для деяких } a, b \in \mathbb{R} \quad (2.1)$$

Такий тип рівняння називається рівнянням Вейєрштрасса і, як кажуть, має форму Вейєрштрасса або нормальну форму Вейєрштрасса.

Описуючи еліптичні криві, ми торкнулись теми алгебраїчної геометрії. Проте еліптичні криві важливі не тільки в ній, а й в наприклад теорії чисел та криптографії.

Почнемо з теорії чисел: по-перше, дослідження раціональних точок на еліптичних кривих пов’язане з важливими об’єктами, як-от конгруентні числа, гіпотеза Бірча та Свіна—Дайєра. Наприклад, як вже зазначалось, множина раціональних розв’язків рівняння еліптичної кривої формує абелеву групу, що дозволяє застосовувати методи теорії груп для розв’язання діофантових рівнянь. Багато класичних задач із визначення кількості раціональних чи цілих точок

зводяться до вивчення рангу цієї групи. Окрім того, властивості модулярності еліптичних кривих стали ключем до доведення теореми Ферма в сучасному форматі (через модулярні форми).

Стосовно криптографії, варто сказати що, еліптичні криві забезпечують алгоритмічну базу для безпечної передачі даних. Завдяки складності оберненої операції до множення точки на кривій (задача дискретного логарифма на еліптичній кривій), реалізується алгоритм ECC (Elliptic Curve Cryptography). Переваги ECC над традиційними схемами (RSA, DSA) це вища криптостійкість при значно коротших ключах, що знижує навантаження на обчислювальні ресурси та пропускну здатність мережі. Сьогодні протоколи TLS/SSL, Bitcoin, SSH та багато мобільних систем безпеки ґрунтуються на еліптичних кривих.

Таким чином ми бачимо, що еліптичні криві важливі не тільки з точки зору фундаментальної математики, а й з точки зору прикладних задач безпосередньо.

Розглядаючи деякі аспекти еліптичних кривих, ми не можемо не торкнутись питань, що пов’язані з еліптичними функціями, а конкретніше їх застосувань щодо опису коливань та складних періодичних процесів. Загалом еліптичні функції відрізняються від традиційних тригонометричних тим, що мають дві фундаментальні періоди, що дозволяє їм описувати не лише прості гармонічні коливання, а й більш складні нелінійні збурення. Серед найвідоміших еліптичних функцій — функції Якобі (sn, cn, dn) та функція Вейерштрасса ($\wp$).

Спочатку розглянемо нелінійне коливання математичного маятника.

Якщо враховувати великі кути відхилення (не обмежуючись наближенням $sin\theta \approx \theta$), рівняння руху математичного маятника набуває вигляду

$\theta^{\cdot\cdot} + \frac{g}{L} sin\theta = 0$, де g прискорення вільного падіння, L довжина маятника .

Розв’язок цього рівняння через інтегрування дає еліптичний інтеграл першого роду, а сам рух можна виразити через функції Якобі. Наприклад, перебуваючи при стартовому куті θ, кутова координата θ(t) задається через

$\theta(t) = 2arcsin(\kappa\, sn(\omega t,\, k))$, де sn— функція Якобі з модулем $k = sin(\frac{\theta_0}{2})$, а $\omega = \sqrt{gL}$. Завдяки цьому опису можна точно визначити період коливань залежно від початкового відхилення (тобто від k), без апроксимації малого кута.

Проте існують й складніші періодичні процеси. У фізиці й інженерії нерідко виникають осцилятори з нелінійними характеристиками (наприклад, пружини із залежною від деформації жорсткістю) або підвищеною диссипацією. У таких системах рух часто описується рівняннями, що зводяться до форми еліптичного інтеграла. Тоді загальні рішення можна подати через еліптичні функції Якобі або Вейерштрасса. Наприклад, рух у потенціалі виду $V(x) = \frac{1}{4}x^4 - 12x^2$ (двунівельний потенціал) приводить до рівняння

$\ddot{x} + x - x^3 = 0$, яке розв’язується через функцію Вейерштрасса $\wp(t; g_2, g_3)$, де параметри g_2, g_3 залежать від енергії початкового стану. Аналогічно, у задачах з магнітними феромагнетиками чи консервацією енергії в нелінійних середовищах виникають еліптичні рівняння Ляпунова–Остроградського, що розв’язуються через функції Якобі.

Проте існує ще одна група маятників, а саме маятники з додатковими силами. Наприклад, маятник у полі тяжіння під дією зовнішніх гармонічних збурень (вимушений маятник) може приводити до рівнянь, що містять як лінійні, так і кубічні члени. Загальні рішення таких диференціальних рівнянь записуються через еліптичні функції, що дозволяє аналізувати резонансні явища, біфуркації та перехід до хаотичного режиму.

Тож, завдяки своїй здатності відтворювати подвійний період і плавно описувати перехід від малих коливань до великих нерегулярних траєкторій, еліптичні

функції стають незамінними у прикладних задачах механіки, фізики конденсованого стану, а також у теоретичних дослідженнях складних динамічних систем.

Розглядачи загальну проблематику еліпсу може виникнути уявлення, що «проблематика питань еліпсу» я декотрою річчю в собі із деякими виключеннями у вигляді криптографії. Проте, це зовсім не так. В кінці цього розділу, ми хочемо розглянути найбільш прикладні розділи в яких використовується проблематика еліпсу, а саме астрофізика, оптика та машинне навчання.

Почнемо з астрофізики. Відповідно до законів Кеплера, траєкторії руху планет навколо Сонця (або супутників навколо планети) описуються еліпсами, причому один із фокусів еліпса знаходиться точно в центрі тяжіння (наприклад, у Сонця для планет). Основні моменти:

- Геометрична форма орбіти. Рівняння еліпса в полярних координатах із центром у фокусі: $r(\theta) = a\,\frac{1-e^2}{1+e\cos\theta}$, де a — велика піввісь (середня відстань від планети до Сонця), а e — ексцентриситет (міра «витягнутості»). При e=0 орбіта перетворюється на коло.
- Другий закон Кеплера (закон площ). Радіус-вектор планети (пряма від Сонця до планети) описує рівні площі за рівні інтервали часу. Це випливає з умов збереження моменту імпульсу в центральному полі тяжіння. За фізичною інтерпретацією: коли планета розташована ближче до Сонця (в перигелії), вона рухається швидше; коли далі (в афелії) — повільніше.
- Третій закон Кеплера (гармонічний зв’язок)**.** Квадрат періоду обертання T пропорційний кубу великої півосі a:

  $T^2 \propto a^3$,

що випливає з рівняння руху в центральному гравітаційному потенціалі

$$F = G\,\frac{Mm}{r^2}.$$

- Застосування. Такий еліптичний опис дає змогу точно розраховувати позиції планет, астероїдів та комет (особливо для тіл із високим ексцентриситетом). Сучасна астродинаміка враховує також непружні впливи (приливи, вплив інших планет), але еліптична апроксимація є базовою для розрахунку траєкторій у міжпланетних місіях і прогнозування сонячних затемнень.

Перейдемо до оптики, а саме до відбивальних властивостей еліпса. У геометричній оптиці еліптичне дзеркало (або еліптична поверхня обертання) має унікальне відображальне правило:

- Геометричний факт: промінь, що виходить із одного фокуса еліпса, після відбиття від бічної поверхні завжди пройде через другий фокус. І навпаки: промені, які спрямовані в один фокус, після відбиття збираються в інший.
- Математична основа: оскільки еліпс є множиною точок, для яких сума відстаней до двох фокусів F_1 і F_2 стала, на будь-якій дотичній до еліпса кути падіння і відбиття рівні, але завдяки геометричній будові це гарантує «фокусування» променів.

До прикладів застосування тут можемо віднести:

- Олександрівські телескопи та рефлектори з еліптичними дзеркалами. Якщо джерело світла розташоване у одному фокусі, то після відбиття від еліптичного дзеркала промінь стає майже паралельним, або, навпаки, промені паралельного пучка збираються в другому фокусі.
- Акустичні застосування. В «еліптичних кімнатах» звук, що починається в одному фокусі (наприклад, голос оратора), концентрується в другому

фокусі, тому людина, яка стоїть у другому фокусі, добре чує навіть шепіт із протилежного кінця залу.

- Освітлювальні прилади. Зоряні проектори та прожектори іноді використовують еліптичні відбивачі для рівномірного фокусування світла із лампи (яка розміщується в одному фокусі) у проекційний отвір, що знаходиться в другому фокусі.

Перейдемо до розгляду машинного навчання.

У контексті байєсівського аналізу та машинного навчання часто зустрічаються класи розподілів, які називають «еліптичними» (англ. elliptically contoured distributions). Їхня назва походить від того, що рівень однакової щільності (ізоденсити) у багатовимірному просторі утворює еліпсоїдні контури. Основні властивості:

- Загальна форма щільності. Для випадкового вектора $X \in \mathbb{R}^n$ еліптичний розподіл можна задати через щільність

  $p_X(x) \ \propto \ g((x-\mu)^T \Sigma^{-1}(x-\mu))$,

  де μ - вектор середніх (центр «еліпсу»), Σ - позитивно визначена матриця коваріацій (визначає «форми» еліпсоїда), а функція $g:[0,\infty)\to[0,\infty)$ задає профіль розподілу.

- Клас розподілів (багатовимірний нормальний розподіл, багатовимірний розподіл Стьюдента з певною кількістю ступенів свободи, багатовимірний розподіл Коші).

Проте основним питанням, яке нас цікавить є застосування в байєсівських моделях, а саме:

- Апріорні розподіли: при побудові багатовимірних апріорів дослідник може вибирати еліптичний апріор для параметрів моделі. Наприклад, якщо

є припущення, що декілька вхідних змінних мають кореляцію, використовують апріор виду Multivariate Normal або Multivariate ttt, щоб урахувати відхилення від нормальності (густіші «хвости»).

- Моделювання невизначеності: еліптичні апріори легко комбінувати із лінійними моделями (як у лінійній регресії чи багатовимірній регресії), тому що умова «еліптичності» зберігається при лінійних перетвореннях. Це спрощує аналітичні виведення постеріорного розподілу.
- Розрізненість вибірок: якщо дані мають кореляційну структуру, еліптично контуровані моделі (особливо нормальні) дають інтерпретацію коваріаційних зв'язків через «еліпс-інтервали» (аналог інтервалів довіри, але в багатовимірному сенсі).

Виділимо переваги та особливості застосування.

- Всі еліптичні розподіли мають властивість: лінійна комбінація компонентів $X = (X_1, \dots, X_n)$ (напр., проекція на будь-який напрямок $w^T X$) є одномірним еліптичним (а отже, симетричним) розподілом.
- Для багатовимірного нормального випадку еліптичні контури - справжні еліпсоїди, а для інших — розмиті або згладжені еліпсоїдні поверхні.
- У байєсівській параметричній оцінці, якщо апріор імовірності є еліптичним розподілом, а ймовірність вибірки за умовою параметрів має логліківську, квадратично залежну від параметрів форму (як у звичайній гаусівській помилці), то постеріорний розподіл також залишиться еліптичним (що дає простоту розрахунків, зокрема для знаходження MAP-оцінок та довірчих областей).

Таким чином, еліптичні розподіли в байєсовій статистиці дозволяють гнучко й коректно моделювати кореляційні структури у високовимірних даних, забезпечуючи як аналітичну зручність (лінійність у коваріації), так і достатню гнучкість для даних зі «гострими» або «тяжкими» хвостами.

РОЗДІЛ 3

Теоретико-числові основи еліптичних кривих

В розділі 2 ми навели оглядові теоретичні та прикладні відомості про еліптичні криві. Даний розділ буде направлений на поглиблення вже наведеної інформації.

І почнемо ми з задачі пошуку раціональних точок на еліптичній кривій. Еліптична крива над полем раціональних чисел $\mathbb{Q}$ зазвичай задається у вигляді, вже відомого нам, проєкційного рівняння Вейерштрасса

$$E\colon\ y^2 = x^3 + ax + b, a, b \in \mathbb{Q}, 4a^3 + 27b^2 \neq 0. \quad (3.1)$$

Раціональними точками називають ті пари (x,y), де $x, y \in \mathbb{Q}$, які задовольняють наведене рівняння. Щоб знайти хоча б одну нетривіальну раціональну точку, починають із пошуку невеликих раціональних розв'язків (перебір «невеликих» x-координат, приблизно $x = \frac{p}{q}$ з невеликими

чисельниками і знаменниками). Якщо знайдено (x_0, y_0), далі застосовують групову операцію, яку ми опишемо згодом, щоб згенерувати інші точки.

Іноді еліптичну криву породжують як характеристика певного діофантового рівняння (наприклад, $y^2 = x^3 - D^2x$ або $y^2 + y = x^3 - x$), і тоді можна застосувати методи спадання (як у класичних задачах Ферма) для побудови нескінченної послідовності раціональних розв'язків або доведення її скінченності.

Наведемо приклад: для кривої $E\colon y^2 = x^3 - x$ відомо, що (0,0), (1,0), (−1,0) і (2,±2) — раціональні точки. Далі, наприклад, за допомогою групового закону додаючи (2,2) до себе самій (подвоєння точки) можна отримати нові координати (x_1, y_1) із досить складними виразами, але раціональними. Якщо таких «генераторів» достатньо, вони породжують нескінченну множину раціональних точок.

Одне з найважливіших відкриттів у вивченні еліптичних кривих це те, що множина $E(\mathbb{Q})$ раціональних точок утворює абелеву групу з нульовим елементом у вигляді спеціальної точки нескінченності O. Груповий закон визначається наступним чином:

- Означення нульового елементу. Точка O (яку можна вважати вершиною у проєкціях) є нейтральним елементом.
- Орієнтація для додавання. Нехай $P = (x_1, y_1)$ і $Q = (x_2, y_2)$ - дві раціональні точки на кривій. Щоб знайти суму R=P+Q, проводимо пряму через P і Q (якщо P=Q, то пряма — це дотична до кривої в точці); ця пряма перетинає криву ще в одній точці $R' = (x_3, y_3)$. Тоді R визначаємо як відбиття R′ відносно осі x: тобто $R = (x_3, -y_3)$.
- Особливі випадки. Якщо пряма вертикальна (тобто $x_1 = x_2$ та $y_1 = -y_2$), то P+Q=O. При подвоєнні точки P, замість звичайної прямої береться дотична до кривої в P.

Цей закон забезпечує замкненість, асоціативність (хоч доведення асоціативності виходить за межі елементарного), існування нейтрального елемента (O) та оберненого елемента (для $P = (x, y)$ це $P^{-1} = (x, -y)$). Завдяки цій груповій структурі можна говорити про ранг групи та її торсіонну підгрупу. Раціональні точки, які мають скінечний порядок (тобто nP=O для деякого n>0), утворюють торсіонну частину $E(\mathbb{Q})_{tors}$; точки без обмежень у групі формують безторсіонну підгрупу, яка ізоморфна $\mathbb{Z}^r$, де r - ранг кривої.

Як вже було зазначено, еліптичні криві розглядаються не лише над полями раціональних або дійсних чисел, а й над довільними числовими полями. Основним результатом, який цього стосується є теорема Морделла–Вейля.

Теорема Морделла-Вейля стверджує, що для будь-якого числа K (наприклад $\mathbb{Q}$ або більшого розширення $\mathbb{Q}(\sqrt{D})$ чи навіть довільного алгебричного поля чисел) множина точок E(K) на еліптичній кривій E, визначеній коефіцієнтами у K, є скінченно породженою за точками

нескінченності й, головне, є скінченно породженою абелевою групою. Формально це означає:

$E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r$, де $E(K)_{tors}$ — торсіонна підгрупа, а r — ранг.

Інтуїтивно ранг це кількість незалежних безторсіонних точок-генераторів. Якщо r=0, то всі раціональні точки є торсіонними (обмеженої кількості). Якщо r>0, існує нескінченна множина раціональних точок.

Нам варто розглянути поняття торсіонної підгруппи та безторсіонної частини.

Якщо ми розглядаємо $K = \mathbb{Q}$, то отримаємо відому теорему Мозер, що описує можливі групи $E(\mathbb{Q})_{tors}$. Список із 15 можливих структурувань (наприклад, циклічні групи Z/nZ з 1≤n≤101 або n=12, а також двочлені групи Z/2Z×Z/2mZ для 1≤m≤4.

Після знаходження торсіонних точок зазвичай застосовують процедури вузького спуску (наприклад, 2- чи p-спуск) та обчислення локальних глобальних інваріантів (наприклад, інваріант Шафаревича–Тейта Ш(E/K)) для наближеного визначення рангу. У загальному випадку доведення скінченності порядку групи базується на комбінації технік з арифметичної геометрії (лінеаризація групи, застосування мінімальних моделей тощо).

Розглянемо наслідки для різних полів. Якщо K — розширення ступеня d, ранг може зростати порівняно з рангом над ℚ. Загальна задача вивчення E(K) для довільного алгебричного поля чисел пов’язана з питаннями спуску і торсіонних розширень полів. Наприклад, якщо K містить координати коренів певного многочлена, криву над ℚ можна розкласти на більш «просту» форму над K, що іноді дозволяє збільшити число відомих точок.

Тепер можемо розглянути гіпотезу Бірча–Свіннертона–Дайєра. (дана задача з однією так званих «Задач тисячоліття») Розглянемо передумови виникнення даної гіпотези. Морделл у 1922 році довів теорему Морделла: група раціональних точок на еліптичній кривій має скінченний базис. Це означає, що

для будь-якої еліптичної кривої існує скінченна підмножина раціональних точок на кривій, з якої можна генерувати всі подальші раціональні точки. Якщо кількість раціональних точок на кривій нескінченна, то деяка точка в скінченному базисі повинна мати нескінченний порядок. Кількість незалежних базисних точок з нескінченним порядком називається рангом кривої та є важливою інваріантною властивістю еліптичної кривої.

Якщо ранг еліптичної кривої дорівнює 0, то крива має лише скінченну кількість раціональних точок. З іншого боку, якщо ранг кривої більший за 0, то крива має нескінченну кількість раціональних точок. Хоча теорема Морделла показує, що ранг еліптичної кривої завжди скінченний, вона не дає ефективного методу для обчислення рангу кожної кривої. Ранг певних еліптичних кривих можна обчислити за допомогою числових методів, але (на сучасному рівні знань) невідомо, чи ці методи охоплюють усі криві.

L-функцію L(E, s) можна визначити для еліптичної кривої E, побудувавши добуток Ейлера з кількості точок на кривій за модулем кожного простого числа p. Ця L-функція аналогічна дзета-функції Рімана та L-ряду Діріхле, який визначено для бінарної квадратичної форми. Це окремий випадок L-функції Хассе-Вейля.

Природне визначення L(E, s) збігається лише для значень s на комплексній площині з Re(s) > 3/2. Хассе висунув гіпотезу, що L(E, s) можна продовжити аналітичним продовженням на всю комплексну площину. Цю гіпотезу вперше довів Дойрінг для еліптичних кривих з комплексним множенням. Згодом було показано, що вона справджується для всіх еліптичних кривих над Q, як наслідок теореми про модулярність у 2001 році.

Загалом находження раціональних точок на загальній еліптичній кривій є складною задачею. Знаходження точок на еліптичній кривій за модулем заданого простого числа p є концептуально простим, оскільки існує лише скінченна

кількість можливостей для перевірки. Однак для великих простих чисел це вимагає обчислювальних ресурсів.

Загалом формулювання гіпотези передбачає, що ранг r еліптичної кривої E над полем K дорівнює порядку нуля дзета-функції Хассе — Вейля в точці s=1. Точніше, гіпотеза стверджує, що існує ненульова границя

$$B_E = \lim_{s \to 1} \frac{L(E, s)}{(s-1)^r},$$

де значення B_E залежить від тонких арифметичних інваріантів кривих.

На початку 1960-х років Пітер Свіннертон-Дайер використав комп'ютер EDSAC-2 у комп'ютерній лабораторії Кембриджського університету для обчислення кількості точок за модулем p (позначено N_p) для великої кількості простих чисел p на еліптичних кривих, ранг яких був відомий. З цих числових результатів Бірч та Свіннертон-Дайер (1965) висунули гіпотезу, що N_p для кривої E з рангом r підпорядковується асимптотичному закону:

$$\prod_{p \leq x} \frac{N_p}{p} \approx C \ln(x)^r \text{ при } x \to \infty \quad (3.2)$$

Спочатку це базувалося на дещо нечітких тенденціях у графіках; це викликало певний скептицизм у Касселса (наукового керівника Берча). З часом числові докази накопичувалися.

Це, у свою чергу, призвело до загальної гіпотези про поведінку L-функції кривої L(E, s) при s = 1, а саме, що в цій точці вона матиме нуль порядку r. Це була далекоглядна гіпотеза на той час, враховуючи, що аналітичне продовження L(E, s) було встановлено лише для кривих з комплексним множенням, які також були основним джерелом числових прикладів. (обернена величина L-функції з деяких точок зору є більш природним об'єктом дослідження; іноді це означає, що слід розглядати полюси, а не нулі)

Дана гіпотеза цікава для нас тим, що гіпотеза є єдиним відносно простим загальним способом обчислення рангу еліптичних кривих.

Еліптичні криві часто використовуються в питаннях розв'язання діофантових рівнянь. Багато класичних діофантових задач (тобто рівнянь у невідомих цілих чи раціональних) можна звести до вивчення еліптичних кривих. Ідея зводиться до того, що певне рівняння високого ступеня приводиться до форми $y^2 = x^3 + ax + b$, а далі досліджується множина раціональних рішень. Наведемо приклади подібних задач.

Рівняння Пелля. Рівняння виду $x^2 - Dy^2 = 1$ (де D — невід'ємне ціле число, що не є квадратом) спочатку зводилось саме до кривої першого порядку (циліндричної форми). Однак за певних обмежень (наприклад, обмеження x непарне, у парне) можна провести перетворення, що дає еліптичну криву. У таких випадках пошук нескінченної кількості рішень здійснюють через групову структуру.

Конгруентні числа. Класична задача: для якого натурального n існує трикутник зі стороною n, котрий має раціональні бічні сторони та висоту ? Це достатньо громіздке геометричне формулювання зводиться до того, щоб знайти раціональні розв'язки рівняння

$y^2 = x^3 - n^2x.$

Якщо множина раціональних точок на цій кривій (так званій «конгруентній кривій») не пуста і має ранг ≥ 1, тоді n - конгруентне число. Завдяки методам 2-спуску та Лагранжевим множникам можна довести, що певні класи n (наприклад, n=p, де p - просте вигляду 4k+1) обов'язково конгруентні.

Проте часто розглядаються задачі більш високого степіня. Наприклад, діофантове рівняння $x^3 + y^3 = z^3 + w^3$ (дві кубічні суми) іноді зводиться до рішення рівнянь четвертого степеня, що, у свою чергу, перетворюється на певні криві другого степеня у багатовимірному просторі. В окремих підходах

знаходять раціональні параметричні вирази, а групова структура кривої допомагає довести існування нескінченного сімейства розв'язків.

Тож розглянувши більш детальні аспекти еліптичних кривих, ми можемо більш детально розглянути прикладні моменти, що стосуються побудові криптосистем на основі еліптичних кривих, а також протоколи шифрування і цифрові підписи. Загалом це стає можливо завдяки важкості обчислення дискретного логарифма на еліптичній кривій поверхні скінченого поля F_p чи F_{2^m}. Тож еліптичні криві сьогодні є опорою більшості сучасних криптографічних протоколів.

Як ми зазначили, зазвичай використовуються скінченні поля. Це робиться наступним чином: обирають криву E у формі Вейерштрасса (або оптимізовану сумісно з апаратними вимогами, наприклад, крива Монтгомері) над F_p. Фіксують базову (генеруючу) точку $G \in E(F_p)$ з великим простим порядком n.

Наступним етапом є побудова ключів:

- Приватний ключ d - випадкове ціле число в інтервалі [1, n−1].
- Публічний ключ Q=d G - результат множення точки G на скаляр d за груповим законом (це швидко виконується за алгоритмом подвійного множення й додавання точки).

Далі необхідно розробити певні правила щодо обміну ключами. Дані правила носять назву протоколів. Розглянемо протокол ECDH (обмін ключем)**.** Два учасники, Аліса та Боб, мають публічні ключі $Q_A = d_A G, Q_B = d_B G$. Аліса рахує $S = d_A Q_B$, Боб рахує $S' = d_B Q_A$. Оскільки $d_A Q_B = d_A(d_B G) == d_B(d_A G) = d_B Q_A$, обидва дістають однакову точку S, аби з неї умовно сформувати спільний таємний ключ.

Наступним етапом нашого розгляду є цифровий підпис (ECDSA) з точку зору еліптичних кривих. Для підписування повідомлення m генерується випадкове $k \in [1, n-1]$, обчислюють $R = k\,G = (x_R, y_R)$, із якого беруть $r = x_R \; mod n$. Далі обчислюють $s = k^{-1}(h(m) + d_A \cdot r) \; mod n$. Підпис це пара (r,s).

Перевіряють через $u_1 = h(m)\, s^{-1}\ mod\, n, u_2 = rs^{-1}\ mod\, n$, а потім точку $P = u_1 G + u_2 Q_A = (x_P, y_P)$. Якщо $r \equiv x_P\ mod n$, підпис вважається дійсним.

До переваг використання еліптичних кривих в криптографії відноситься те, що при еквівалентному рівні криптостійкості еліптичні криві потребують значно менших розмірів ключів, ніж RSA чи DSA: наприклад, 256-бітовий ключ ECC дає безпеку, порівнянну з 3072-бітовим RSA. Це знижує навантаження на мережу та процесорний час. Проте не будь-яку криву можна використовувати в питаннях криптографії. Існують сталі криві від NIST (наприклад, P-256, P-384), від SECG (secp256k1 — у Bitcoin) тощо. Обрані криві піддаються ретельному аналізу, щоб запобігти вразливостям.

РОЗДІЛ 4

Суми Клостермана на еліпсі

Нагадаємо формулювання суми Клостермана над зведеною системою лишків за модулем q:[18]

$$K(a,b;q) := \sum_{\substack{x=1 \\ (x,q)=1}}^{q} e^{2\pi i \frac{ax+bx'}{q}}, a,b \in \mathbb{Z}, q > 1 \in \mathbb{N}, \tag{4.1}$$

де x'- мультиплікативно обернений до x за $mod\ q$. $(xx' \equiv 1\ mod\ q)$

Загалом суми Клостермана знайшли своє застосування в асимптотичних задачах теорії чисел і, перш за все, в задачах розподілу значень функцій дільника $\tau(n)$ на арифметичних прогресіях.

Як вже зазначалось в розділі 2, найбільшу складність у побудові оцінок сум Клостермана представляє випадок, коли q=p, де p - просте число. У 1948 році А. Вейль довів гіпотезу Рімана [25] на алгебраїчних кривих, що призводить до побудови найкращої можливої оцінки:

$$K(a,b;q) \ll p^{\frac{1}{2}}. \tag{4.2}$$

Суми Клостермана відіграють суттєву роль у спектральній теорії дзета-функції Рімана, розробленій Ю. Мотохаші. [21]

Новий поштовх вирішенню складних проблем асимптотичної теорії чисел дали роботи Кузнецова та Бруггемана,[9,19] присвячені оцінкам суми сум Клостермана. Пізніше з'явилися узагальнення класичних сум Клостермана. Наприклад, У. Жанбирбаєва [28] досліджувала суми Клостермана над кільцем гауссових цілих чисел $\mathbb{Z}[\theta]$ та вирішила задачу розподілу функції дільника гауссових цілих чисел в арифметичній прогресії.

У роботі знову ж таки Бруггемана [9] досліджувалися суми Клостермана над цілковито дійсними числовими полями. У 2003 році Бруггеман та Мотохаші

[10] отримали аналог формули Кузнецова для сум Клостермана над кільцем гауссових цілих чисел. Геометрія гауссових цілих чисел багатша за геометрію цілих раціональних чисел. У роботі розглядалася нормована сума Клостермана над кільцем $\mathbb{Z}[\theta]$, яка не має аналогічного раціонального випадку.

Нехай $\alpha, \beta \in \mathbb{Z}[\theta], h \in \mathbb{Z}, q \in \mathbb{N}, q > 1, (h, q) = 1$. Припустимо

$$\widetilde{K}(\alpha, \beta; h, q) := \sum_{\substack{x,y(\mathrm{mod}q) \\ N(xy) \equiv h(\mathrm{mod}q)}} e_q\left(\frac{1}{2} Sp(\alpha x + \beta y)\right) \tag{4.3}$$

де $e_q(x) := e^{2\pi i \frac{x}{q}}, \mathrm{Sp}(\alpha) = 2\mathrm{Re}\alpha$.

Дану суму ми будемо називати сумою Клостермана над еліпсом $u^2 + dv^2 \equiv\equiv 1(\mathrm{mod}p^m)$.

Для $q = q_1 q_2, (q_1, q_2) = 1$ маємо

$$\widetilde{K}(\alpha, \beta; h, q) = \widetilde{K}(\alpha, \beta; hq_2', q_1) \cdot \widetilde{K}(\alpha, \beta; hq_1', q_2) =$$
$$= \widetilde{K}(\alpha q_2, \beta q_2; h, q_1) \cdot \widetilde{K}(\alpha q_1, \beta q_1; h, q_2)$$

де q_2' обернений до q_2 за модулем q_1 і q_1' обернений до q_1 за модулем q_2.

В даній роботі ми розглядаємо лише випадок $q = p^n$, де p – просте число,

$n \in \mathbb{N}$.

Позначимо $m_\alpha = \max\limits_{\alpha \equiv 0(\mathrm{mod}p^m)} \{m: m \leqslant \nu_p(q)\}$ (тобто m_α є максимальним показником p, який не більше ніж $\nu_p(q)$ і таке що, $\alpha \equiv 0(\mathrm{mod}p^m)$).

Теорема 1. *Нехай* $(h, p) = 1$. *Тоді*

$$\widetilde{K}(\alpha, \beta; h, p^n) \ll (p^{m_\alpha}, p^{m_\beta}, p^n)^{\frac{1}{2}} \cdot p^{\frac{3n}{2}},$$

де $\ll$ - символ Виноградова (означає теж саме що і О-велике)

Доведення: Перш за все припустимо, що $n = 1$. Випадок $m_\alpha = m_\beta = 1$ є очевидним, тому ми будемо розглядати $m_\alpha = 0$ або $m_\beta = 0$. Далі припустимо, що $\alpha = a_1 + ia_2, \beta = b_1 + ib_2$ і тоді $(a_1, a_2, b_1, b_2) = 1$.

Для факторизованого р маємо

$$\widetilde{K}(\alpha, \beta; h, p) = \sum_{(U)} e_p(a_1x_1 - \varepsilon_0 a_2x_2 + b_1y_1 - \varepsilon_0 b_2y_2) \qquad (4.4)$$

де

$$U = \begin{Bmatrix} x_1, x_2, y_1, y_2 \in \{0,1, \dots, p-1\} \\ (x_1^2 + d \cdot x_2^2)(y_1^2 + d \cdot y_2^2) \equiv h \ (\mathrm{mod} p) \end{Bmatrix}$$
$$\varepsilon_0^2 \equiv -d \ (\mathrm{mod}\ p^m)$$

Припустимо $(d, p) = 1$.

Суму $\widetilde{K}(\alpha, \beta; h, p)$ ми називаємо нормованою сумою Клостермана над кільцем $\mathbb{Z}[\theta]$.

Нехай ε_0 розв'язок конгруенції $x^2 \equiv -d(\mathrm{mod}\ p)$. Дана конгруенція має розв'язок бо $-d$ є квадратичним лишком за модулем р.

Далі припустимо

$u_1 = x_1 + \varepsilon_0 x_2, u_2 = x_1 - \varepsilon_0 x_2, v_1 = y_1 + \varepsilon_0 y_2, v_2 = y_1 - \varepsilon_0 y_2.$

З (4.4) ми отримуємо

$$\widetilde{K}(\alpha, \beta; h, p) = \sum_{(U)} e_p(A_1u_1 + A_2u_2 + B_1v_1 + B_2v_2),$$

де $U = \{u_1, u_2, v_1, v_2 \in \{0,1, \dots, p-1\}, u_1u_2v_1v_2 \equiv h(\mathrm{mod} p)\}$.

Бомб'єрі довів, що останню суму можна оцінити як $\ll p^{\frac{3}{2}}$.

Якщо р незвідне, то така ж оцінка справедлива для суми (4) (доведення аналогічне).

Тепер нехай $n \geqslant 2$. Нам достатньо розглянути лише випадок $(p^{m_\alpha}, p^{m_\beta}, p^n) = 1$. У такому випадку, хоча б одне з чисел a_1, a_2, b_1 не ділиться на р. ($\alpha = a_1 + \theta a_2, \beta = b_1 + \theta b_2$)

Тоді можемо зробити висновок

$$\widetilde{K}(\alpha, \beta; h, p^n) =$$

$$= \sum_{x,y \in G_{p^n}} \frac{1}{p^n} \sum_{k=0}^{p^n-1} e_{p^n}(k(N(x)N(y) - h) + \Re(\alpha x) + \Re(\beta y)) =$$

$$= \frac{1}{p^n} \sum_{S(C)} e_{p^n}(k(d \cdot (x_1^2 + x_2^2)(y_1^2 + y_2^2) - h) + \qquad (4.5)$$

$$+ a_1 x_1 - a_2 x_2 + d b_1 y_1 - d b_2 y_2),$$

де

$$C := \{k (\mathrm{mod} p^n); x_1, x_2 (\mathrm{mod} p^n); y_1, y_2 (\mathrm{mod} p^n); x_1, x_2, y_1, y_2 \in \mathbb{Z}_{p^n}\}$$

Зауважимо, що одна з сум по x_1, x_2, y_1, y_2 дорівнює 0, якщо $(k, p) = p$. (за раціональним аналогом повної експоненціальної суми лінійної функції)

Отже, припускаючи що $(a_1, a_2, p) = 1$ маємо

$$\widetilde{K}(\alpha, \beta; h, p^n) =$$

$$= \frac{1}{p^n} \sum_{S(C)} e_p^n(-kh) e_{p^n}(kdN(x)(y_1^2 + y_2^2) + \Re(\alpha x) + d b_1 y_1 - d b_2 y_2) =$$

$$= \frac{1}{p^n} \sum_{k \in \mathbb{Z}_{p^n}^*} e_{p^n}(-kh) \left(\sum_{\substack{x \in \mathbb{G}_{p^n} \\ (N(x), p) = 1}} + \sum_{\substack{x \in \mathbb{G}_{p^n} \\ x (\mathrm{mod} p^n) \\ N(x) \equiv 0 \ (\mathrm{mod} p)}} \right) = \sum_1 + \sum_2 \qquad (4.6)$$

де $C := \{k \in \mathbb{Z}_{p^n}^*, x \in \mathbb{G}_{p^n}, y_1, y_2 \in \mathbb{Z}_{p^n}\}$

Нехай $N(x)'$ і k' розв'язки конгруенцій $N(x)u \equiv 1(\mathrm{mod}\, p^n), ku \equiv 1(\mathrm{mod}\, p^n)$, відповідно.

Тоді

$$\left|\sum_1\right| = \left| \sum_{k\in\mathbb{Z}_{p^n}^*} e_{p^n}(-kh) \times \right. \tag{4.7}$$
$$\left. \times \sum_{x\in\mathbb{G}_{p^n}} e_{p^n}(4'N(x)'k'(b_1^2+b_2^2)+a_1x_1-a_2x_2) \right|$$

Припустимо

$$x_1 = x_1^0 + p^m z_1, x_2 = x_2^0 + p^m z_2$$
$$0 \leqslant x_1^0, x_2^0 \leqslant p^m - 1, 0 \leqslant z_1, z_2 \leqslant p^{n-m} - 1, m = \left[\frac{n+1}{2}\right]$$

Зрозуміло що,

$$N(x)' = \left(x_1^{0^2} + d \cdot x_2^{0^2}\right)' \left(1 - 2p^m \left(x_1^{0^2} + d \cdot x_2^{0^2}\right)' (x_1^0 z_2 + x_2^0 z_1)\right)$$

Тоді маємо

$$\left|\sum_1\right| = \left| \sum_{k\in\mathbb{Z}_{p^n}^*} e_{p^n}(-kh) \times \right.$$
$$\times \sum_{\substack{x_1^0, x_2^0 (\mathrm{mod} p^n) \\ (x_1^{02}+x_2^{02}, p)=1}} e_{p^n}\left(4'k'\left(x_1^{0^2}+x_2^{0^2}\right)' \cdot (b_1^2+b_2^2) + a_1x_1^0 - a_2x_2^0\right) \times$$
$$\left. \times \sum_{z_1, z_2 (\mathrm{mod} p^{n-m})} e_{p^{n-m}}\left((A_1+a_1)z_1 + (A_2+a_2)z_2\right) \right|$$

де $A_1 = 2\left(\left(x_1^{0^2} + x_2^{0^2}\right)'\right)^2 x_2^0, A_2 = 2\left(\left(x_1^{0^2} + x_2^{0^2}\right)'\right)^2 x_1^0.$

Сума по z_1, z_2 дорівнює 0 якщо конгруенція

$A_1 + a_1 \equiv 0(\mathrm{mod}\, p^{n-m}), A_2 - a_2 \equiv 0(\mathrm{mod}\, p^{n-m})$

або еквівалентна їй конгруенція

$a_2x_1^0 + a_1x_2^0 \equiv 0(\mathrm{mod}p^{n-m}), 2x_2^0 \equiv -a_1\left(x_1^{0^2} + x_2^{0^2}\right)^2(\mathrm{mod}p^{n-m})$

порушуються.

Дана система конгруенцій має щонайбільше три розв'язки за модулем p^{n-m}, і, тоді, щонайбільше $3p^{m-(n-m)}$ за модулем p^m.

Тоді

$$\left|\sum_1\right| = \left|p^{2(n-m)}\sum_{S(C)} e_{p^n}(a_1x_1^0 - a_2x_1^0)\sum_{k\in\mathbb{G}_{p^n}^*}(kh + k'B)\right| \leqslant 8p^{\frac{3}{2}n}, \qquad (4.8)$$

де

$$C = \left\{x_1^0, x_2^0(\mathrm{mod}p^m) \quad \begin{matrix} a_2x_1^0 \equiv -a_1x_2^0(\mathrm{mod}p^{n-m}), \\ 2x_1^0 \equiv -a_1\left(x_1^{0^2} + x_2^{0^2}\right)^2(\mathrm{mod}p^{n-m})\end{matrix}\right\}.$$

Нарешті, якщо $N(x) \equiv 0(\mathrm{mod}p)$, то $\sum_2 = 0$ за раціональним аналогом повної еспоненціальної суми лінійної функції. ■

Для натурального $k > 1$ ми припускаємо

$$\widetilde{K}(\alpha, \beta; h, q; k) := \sum_{\substack{x,y\in\mathfrak{G}_q \\ N(xy)\equiv h(\mathrm{mod}q)}} e_q\left(\frac{1}{2}Sp(\alpha x^k + \beta y^k)\right). \qquad (4.9)$$

Зрозуміло, що $\widetilde{K}(\alpha, \beta; h, q; 1) = \widetilde{K}(\alpha, \beta; h, q)$.

Метод дослідження суми $\widetilde{K}(\alpha, \beta; h, q; k)$ показує, що достатньо розглядати випадок $q = p^n$, p – просте. Перш за все, ми припустимо, що p незвідне.

Теорема 2. *Нехай p – незвідне, $h \in \mathbb{Z}, (h, p) = 1, k \in \mathbb{N}, t = (k, p-1)$. Тоді $\forall\alpha, \beta \in \mathbb{Z}, (\alpha, \beta, p) = 1$ над кільцем $\mathbb{Z}[\theta]$ справджується наступна оцінка*

$$|\widetilde{K}(\alpha, \beta; h, p; k)| \ll \begin{cases} t^2p^{\frac{3}{2}}, \text{якщо } t - 1 \leqslant \sqrt[4]{p} \\ dp^2, \text{якщо } t \geqslant \sqrt[4]{p} + 1 \end{cases}$$

Доведення: Нехай $k = dk_1, \left(k_1, \frac{p-1}{t}\right) = 1$. Маємо

$$\sum_{\substack{x,y\in\mathfrak{G}_p \\ N(xy)\equiv h(\mathrm{mod}p)}} e_p\left(\frac{1}{2}Sp(\alpha(x^{k_1})^t + \beta(y^{k_1})^t)\right) =$$

$$= \sum_{\substack{x,y\in\mathfrak{G}_p \\ N\left(x^{k_1}y^{k_1}\right)\equiv h^{k_1}(\mathrm{mod}p)}} e_p\left(\frac{1}{2}Sp(\alpha(x^{k_1})^t + \beta(y^{k_1})^t)\right) =$$

$$= \sum_{\substack{x,y\in\mathfrak{G}_p \\ N(xy)\equiv h^{k_1}(\mathrm{mod}p)}} e_p\left(\frac{1}{2}Sp(\alpha x^t + \beta y^t)\right) = \widetilde{K}(\alpha,\beta;h^{k_1},p;t)$$

В силу того факту, що для будь-якого мультиплікативного характеру χ над полем $\mathbb{F}_{p^2}$ маємо

$$\sum_{h\in\mathbb{F}_p^*} \chi(h)\widetilde{K}(\alpha,\beta;h,p;t) =$$

$$= \sum_{x,y\in\mathbb{F}_{p^2}^*} \chi(N(x)N(y))e_p\left(\frac{1}{2}Sp(\alpha x^t)\right)e_p\left(\frac{1}{2}Sp(\beta y^t)\right) = \quad (4.10)$$

$$= \left(\sum_{x\in\mathbb{F}_{p^2}^*} \chi\left(N(x)e_p\left(\frac{1}{2}Sp(\alpha x^t)\right)\right)\right)\left(\sum_{y\in\mathbb{F}_{p^2}^*} \chi(N(y))e_p\left(\frac{1}{2}Sp(\beta y^t)\right)\right)$$

Суму у правій частині (4.10) можна оцінити як $(t-1)N(p)^{\frac{1}{2}}$. (узагальнена гаусова сума)

Отже маємо

$$\left|\sum_{h\in\mathbb{F}_{p^2}^*} \chi(h)\widetilde{K}(\alpha,\beta;h,p;t)\right| \leqslant (t-1)^2p^2$$

Застосування теореми Планшереля дає

$$\sum_{h\in\mathbb{F}_{p^2}^*} |K(\alpha,\beta;h,p;t)|^2 \leqslant (t-1)^4 p^4$$

Тепер, подібно до роботи Бомб'єрі, ми робимо висновок, що вага характеристичних коренів, що асоціюються з $\widetilde{K}(\alpha,\beta;h,p;t)$ не повинна перевищувати 3, якщо $(t-1)^4 < p$. Тоді, використовуючи результати Бомб'єрі та Деліня, знаходимо

$\widetilde{K}(\alpha,\beta;h,p;t) \ll (t-1)^2 p^2 \ll t^2 p^2$ якщо $t-1 < \sqrt[4]{p}$

Далі, для $x = x_1 + \theta x_2, x_1, x_2 \in \mathbb{Z}$, маємо $x_1 - i\theta x_2 \equiv (x_1 + \theta x_2)^p (\mathrm{mod}\, p)$ і тоді $N(x) \equiv x^{p+1} (\mathrm{mod} p)$.

Тоді

$$\sum_{\substack{x,y\in\mathbb{G}_p \\ N(xy)\equiv h(\mathrm{mod}p)}} e_p\left(\frac{1}{2} Sp(\alpha x^t + \beta y^t)\right) =$$

$$= \sum_{\substack{x,y\in\mathbb{G}_p \\ (xy)^{p+1}\equiv h(\mathrm{mod}p)}} e_p\left(\frac{1}{2} Sp(\alpha x^t + \beta y^t)\right) = \quad (4.11)$$

$$= \sum_{\substack{\varepsilon\in\mathbb{G}_p \\ \varepsilon^{p+1}\equiv h(\mathrm{mod}p)}} \sum_{x(\mathrm{mod}p)} e_p\left(\frac{1}{2} Sp(\alpha x^t + \beta y^t)\right)$$

Конгруенція $z^{p+1} \equiv h(\mathrm{mod}\, p)$ має рівно два розв’язки за модулем p якщо h – квадратичний лишок. Внутрішня сума в правій частині (11) оцінюється як

$\leqslant 2dp$. Це завершує доведення теореми. ■

Тепер нехай $q = p^n$, p – незвідне, $n \geqslant 2$. Ми будемо використовувати опис елементів з нормою 1 зведеної системи лишків $\mathrm{mod}\, p^n$. Вони утворюють групу, яку ми описуємо через E_m.

В подальшому нам знадобиться наступне твердження.

Твердження 1. *Нехай* $n, k \in \mathbb{N}, p \geqslant 3$ *– просте,* $u \in \mathbb{Z}, (p, u) = 1$. *Тоді* $\forall t \in \mathbb{N}$ *маємо*

$$(1 + p^k u)^t \equiv 1 + p^k a_1 t + p^{2k} a_2 t^2 + p^{\lambda_3} a_3 t^3 + \cdots + p^{\lambda_n} a_n t^n (mod\ p^n),$$

крім того, $(a_i, p) = 1, i = 1, \dots, n; \lambda_j > 2k, j = 3, \dots, n$

Доведення: З відношення

$$\binom{t}{m} = \frac{1}{m!}\left(t^m - \frac{m(m-1)}{2} t^{m-1} + \cdots + (-1)^{m-1}(m-1)! \cdot t\right)$$

та верхню межу показника степеня з тим, що число p потрапляє в m!, отримуємо

$$(1 + p^k u)^t \equiv 1 + p^k a_1 t + p^{2k} a_2 t^2 + p^{\lambda_3} a_3 t^3 + \cdots + p^{\lambda_n} a_n t^n (\mathrm{mod}\ p^n),$$

де $(a_i, p) = 1, i = 1, \dots, n; \lambda_j > \left(k - \frac{1}{p-1}\right) \cdot j > 2k$ для $j = 3,4, \dots$. ■

Отже, породжуючий елемент $u + \sqrt{-d}v$ групи E_1 можна взяти, оскільки він буде породжуючим елементом групи E_ℓ для будь-якого фіксованого $\ell > 2$.

Нехай $\ell = \max(5, n)$. Маємо

$$N((u + \sqrt{-d}v))^2 \equiv 1\left(\mathrm{mod} p^\ell\right)$$

$$(u + \sqrt{-d}v)^{2(p+1)} = 1 + p\left(x_0 + \sqrt{-d}y_0\right), \left(x_0 + \sqrt{-d}y_0, p\right) = 1.$$

Тоді

$$N\left(1 + px_0 + \sqrt{-d}py_0\right) \equiv 1 + 2px_0 + p^2 x_0^2 + p^2 d y_0^2 \equiv 1\left(\mathrm{mod} p^\ell\right)$$

Звідси, $2px_0 \equiv 0(\mathrm{mod} p^2), x_0 = px_0', (y_0, p) = 1.$

Маємо

$$(u + \sqrt{-d}v)^{2(p+1)} \equiv 1 + p^2 x_0 + \sqrt{-d}py_0, (x_0, p) = (y_0, p) = 1$$

Тоді з твердження 1 випливає

$$\Re\left((u + \sqrt{-d}v)^{2(p+1)t}\right) \equiv A_0 + A_1 t + A_2 t^2 + \cdots + A_{n-1} t^{n-1} (\mathrm{mod} p^n)$$

$$\Im\left((u+\sqrt{-d}v)^{2(p+1)t}\right) \equiv B_0 + B_1 t + B_2 t^2 + \cdots + B_{n-1}t^{n-1}(\mathrm{mod}p^n) \quad (4.12)$$

де

$A_0 \equiv 1(\mathrm{mod}p), B_0 \equiv 0(\mathrm{mod}p)$
$A_1 \equiv p^2 x_0 + 2' d y_0^2 p^2(\mathrm{mod}p^3)$, тобто $A_1 \equiv 0(\mathrm{mod}p^3)$
$A_2 \equiv -2' y_0^2 p^2(\mathrm{mod}p^3)$, тобто $A_2 = p^2 A_2', (A_2', p) = 1$
$B_1 \equiv p y_0(\mathrm{mod}p^3)$, тобто $B_1 = pB_1', (B_1', p) = 1$
$B_2 \equiv A_3 \equiv B_3 \equiv \cdots \equiv A_{n-1} \equiv B_{n-1} \equiv 0(\mathrm{mod}p^3)$

Нехай

$$\beta = 2(p+1)t + z, 0 \leqslant t \leqslant p^{n-1} - 1, 0 \leqslant z \leqslant 2p+1$$

і визначимо

$$(u+\sqrt{-d}v)^{\beta} = (u+\sqrt{-d}v)^{2(p+1)t} \cdot (u(z) + \sqrt{-d}v(z)).$$

Тоді маємо

$$\Re\left\{(u+\sqrt{-d}v)^{2(p+1)t+z}\right\} \equiv\equiv A_0(z) + A_1(z)t + \cdots + A_{n-1}(z)t^{n-1}(\mathrm{mod}p^n), (4.13)$$

де $A_i(z) = A_i u(z) - B_i v(z)$

Тепер визначимо, для яких значень z справджується конгруенція

$$v(z) \equiv 0(\mathrm{mod}\, p).$$

Нехай $v(z) = pv_0(z), v_0(z) \equiv 0(\mathrm{mod}p^k), k \geqslant 0.$

Тоді

$(u+\sqrt{-d}v)^z = u(z) + \sqrt{-d}pv_0(z)$
$(u+\sqrt{-d}v)^{z(p-1)p^{n-k}} \equiv (u(z))^{(p-1)p^{n-k}}(\mathrm{mod}p^n).$

Послідовності $\left\{(u+\sqrt{-d}v)^{2\beta}\right\}$ і $\{g^{\alpha}\}$ можуть мати 2 спільні елементи за модулем p. (1 та -1) Тоді

$$(u(z))^{(p-1)p^{n-k}} \equiv \pm 1(\mathrm{mod}p^n).$$

Конгруенція $(u(z))^{(p-1)p^{n-k}} \equiv -1(\mathrm{mod}\, p^n)$ неможлива, оскільки інакше б мали $(-1)^{p^{k-1}} \equiv (u(z))^{(p+1)p^{n-1}} \equiv 1(\mathrm{mod}\, p^n)$, тобто $-1 \equiv 1(\mathrm{mod}\, p)$.

Тоді

$$(u(z))^{(p-1)p^{n-k}} \equiv 1(\mathrm{mod} p^n)$$
$$z(p-1)p^{n-k} \equiv 0(m_0 d 2(p+1)p^{n-1})$$

Так як $(p-1, p+1) = 2$ то $z \equiv 0(\mathrm{mod}(p+1)p^{k-1})$. Отже, отримуємо що з $p \| v(z)$ слідує $z = p+1$, і з $p^2 \mid v(z)$ слідує $z = 0$. Отже, маємо

$$p \| A_1(z), A_i(z) \equiv 0(\mathrm{mod} p^2), \quad i = 2, \dots, n-1 \text{ if } z \neq 0, z \neq p+1;$$
$$A_1(0) = A_1(p+1) \equiv 0(\mathrm{mod} p^2), \quad p^2 \| A_2(0) p^2 \| A_2(p+1),$$
$$A_j(0) \equiv A_j(p+1) \equiv 0(\mathrm{mod} p^3), \quad j = 3,4, \dots, n-1.$$

Наведемо твердження, яке будемо використовувати

Твердження 2.(узагальнена сума Гауса) *Нехай* $\mathfrak{p}$ *– просте число з уявного квадратичного поля,* $m \geqslant 1$ *– натуральне,* $\alpha_1, \alpha_2, \dots, \alpha_n \in G$, $(\alpha_2, \mathfrak{p}) = 1$.

Тоді для $\forall\, k \geqslant 2$ *маємо*

$$\sum_{\omega \in G_{\mathfrak{p}} m} exp\left(\pi i Sp\left(\frac{\alpha_1 \omega + \mathfrak{p}\alpha_2 \omega^2 + \mathfrak{p}^3 \alpha_3 \omega^3 + \cdots + \mathfrak{p}^k \alpha_k \omega^k}{\mathfrak{p}^m}\right)\right)\Bigg| =$$
$$= \begin{cases} 0, & \text{якщо } (\alpha_1, \mathfrak{p}) = 1\ (mod\ \mathfrak{p}), \\ (N(\mathfrak{p}))^{\frac{m+1}{2}}, & \text{якщо } \alpha_1 \equiv 0\ (mod\ \mathfrak{p}). \end{cases}$$

Тепер можемо довести наступну теорему

Теорема 3. *Нехай* p *– просте незведне число,* $h \in \mathbb{Z}, (h,p) = 1$, $k > 1$ *– натуральне,* a,b *– цілі числа в* $\mathbb{Z}[\theta]$,

$(a,p) = (b,p) = 1$. *Тоді для* $n \geqslant 2$

$$\left|\widetilde{K}(a,b;h,p^n;k)\right| \leqslant 2p^{\frac{3}{2}n+m} ln\ p^n$$

де m: $p^m \| k$

Доведення: Використовуючи твердження 1, ми можемо записати a, b у формі

$a = g^{\alpha_0'}(u+\theta v)^{\beta_0'}, b = g^{\alpha_0''}(u+\theta v)^{\beta_0''}$

де g – первісний корінь за модулем p^n в $\mathbb{Z}, u+\theta v$ – породжувальний елемент групи E_n.

Тоді отримуємо

$\widetilde{K}(a,b;h,p^n;k) =$ (4.14)

$$= \sum_{\substack{x,y\in\mathbb{G}_{p^n} \\ N(x)N(y)\equiv h(\mathrm{mod}p^n)}} e_{p^n}\left(g^{\alpha_0'}\Re\left((u+\theta v)^{\beta_0'}x^k\right) + g^{\alpha_0''}\Re\left((u+\theta v)^{\beta_0''}y^k\right)\right)$$

Нехай $h \equiv g^{\alpha}(\mathrm{mod}\, p^n)$. Тоді $h \equiv \pm g^{2\alpha_0}(\mathrm{mod}\, p^n)$, де

$$2\alpha_0 = \begin{cases} \alpha_0 & \text{якщо} \quad \alpha \text{ - парне} \\ \alpha + \dfrac{p-1}{2}p^{n-1} & \text{якщо} \quad \alpha \text{ - непарне} \end{cases}$$

Сума по $x \in \mathbb{G}_{p^n}$ в (4.14) ми розіб'ємо на 2 частини, $\sum = \sum_1 + \sum_2$. В сумі $\sum_1$ покладемо $x \in \mathbb{G}_{p^n}$ для яких

$N(x) \equiv g^{2\alpha_1}(\mathrm{mod}p^n)$

і в сумі $\sum_2$ випадуть такі $x \in \mathbb{G}_{p^n}$, такі що

$N(x) \equiv -g^{2\alpha_1}(\mathrm{mod}\, p^n)$.

Для обох випадків маємо, що α_1 пробігає всі значення $0,1,\dots,\frac{p-1}{2}p^{n-1}-1$.

Тоді

$$\widetilde{K}(a,b;h,p^n;k) = \sum_1 + \sum_2 \qquad (4.15)$$

Для $x \in \sum_1$ маємо

$$x \equiv g^{\alpha_1}(u+\theta v)^{2\beta_1}(\mathrm{mod}p^n),$$

$\alpha_1 = 0,1,\dots,\frac{1}{2}(p-1)p^{n-1}-1;\ \beta_1 = 0,1,\dots,(p+1)p^{n-1}-1.$

Це означає що

$$\Re\left((u+\theta v)^{\beta_0'}x^k\right) \equiv g^{k\alpha_1}\Re\left((u+\theta v)^{2k\beta_1+\beta_0'}\right)(\mathrm{mod}p^n).$$

З умови $N(x)N(y) \equiv h(\mathrm{mod}p^n)$ маємо

$$N(y) \equiv \pm g^{2\alpha_2}(\mathrm{mod}p^n)$$

де $\alpha_2 = \alpha_0 + ((p-1)p^{n-1}-1)\alpha_1$.

Тоді маємо

$$\sum_1 = \sum_{(\alpha_1)}\sum_{(\beta_1)}\sum_{(\beta_2)} e_{p^n}(\mathfrak{U}), \tag{4.16}$$

де

$$(\mathfrak{U}) = \left(g^{\alpha_0'+\alpha_1 k}\Re\left((u+\theta v)^{2k\beta_1+\beta_0'}\right) + g^{\alpha_0''+\alpha_2 k}\Re\left((u+\theta v)^{2k\beta_2+\beta_0''+\delta k}\right)\right)$$

Тут (α_1) означає, що α_1 пробігає всі значення $0,1,\dots,\frac{1}{2}(p-1)p^{n-1}-1$; (β_i) пробігає всі значення $0,1,\dots,(p+1)p^{n-1}-1, (i=1,2)$; $\delta = 0$ якщо

$h \equiv g^{2\alpha_0}(\mathrm{mod}p^n)$ і $\delta = 1$ якщо $h \equiv -g^{2\alpha_0}(\mathrm{mod}p^n)$.

Аналогічно,

$$\sum_2 = \sum_{(\alpha_1)}\sum_{(\beta_1)}\sum_{(\beta_2)} e_{p^n}(\mathfrak{V}) \tag{4.17}$$

де

$$(\mathfrak{V}) = \left(g^{\alpha_0'+\alpha_1 k}\Re\left((u+iv)^{2k\beta_1+\beta_0'+1}\right) + g^{\alpha_0''+\alpha_2 k}\Re\left((u+\theta v)^{2k\beta_2+\beta_0''+\delta k}\right)\right).$$

Нехай знову

$$\beta_i = (p+1)t_i + z_i, t_i(\mathrm{mod}p^{n-1}), z_i = 0,1,\dots,p, (i=1,2)$$

Тоді

$$k\beta_i = 2(p+1)kt_i + kz_i, (i=1,2)$$

Тоді з (4.13)-(4.14) і твердження 1 випливає що суми по t_i дорівнюють нулю якщо порушуються наступні конгруенції

$\beta_0' + 2kz_1 \equiv 0(\mathrm{mod}(p+1))$

$\beta_0'' + 2kz_2 + k\delta \equiv 0\big(\mathrm{mod}(p+1)\big)$, для суми $\sum_1$

(4.18)

$\beta_0' + 2kz_1 + 1 \equiv 0(\mathrm{mod}(p+1))$

$\beta_0'' + 2kz_2 + k\delta \equiv 0\big(\mathrm{mod}(p+1)\big)$, для суми $\sum_2$

Звідси, одна з сум $\sum_1$ або $\sum_2$ обов'язково дорівнює 0.

Відношення (4.18) справджуються лише для $(k, p+1)^2$ пар значень (z_1, z_2).

Нехай $\mathfrak{B}$ множина таких значень (z_1, z_2).

З (4.13)-(4.14) ми маємо

$$\widetilde{K}(a,b;h,p^n;k) = \sum_{(\alpha_1)} e_{p^n}(N_0 g^{\alpha_1} + M_0 g^{\alpha_2}) \times$$
$$\times \sum_{(z_1,z_2)\in\mathfrak{B}} \sum_{t_1,t_2(\mathrm{mod}p^{n-1})} e_{p^{n-2}}(F_1(kt_1)g^{\alpha_1} + F_2(kt_2)g^{\alpha_2}),$$

де $F_i(t) = c_1^{(i)}t + c_2^{(i)}t^2 + p^{\lambda_3}c_3^{(i)}t^3 + \cdots + p^{\lambda_\ell}c_\ell^{(i)}t^\ell, \left(c_2^{(i)}, p\right) = \left(c_3^{(i)}, p\right) = \cdots = = 1, \lambda_j > 0$ для $j \geqslant 3, (N_0, p) = (M_0, p) = 1$.

Суми по t_1, t_2 розраховуються аналогічно. Нехай розіб'ємо суму по t_i на блоки довжини p^{n-2-2m} (якщо $2m < n-2$). Тоді використовуючи твердження 2, маємо

$$\widetilde{K}(a,b;h,p^n;k) = p^{n+2m} \sum_{(\alpha_1)} e_{p^n}(N_1 g^{\alpha_1} + N_2 g^{\alpha_2}), \qquad (4.19)$$

де $(N_1, p) = (N_2, p) = 1$.

З визначення α_2 маємо $g^{\alpha_2} \equiv g^{\alpha_0}(g')^{\alpha_1}(\mathrm{mod} p^n)$.

Сума в правій частині (19) це неповна сума Клостермана. З підбором первісного кореня g маємо

$g^{p-1} = 1 + pu, (u, p) = 1$

Тоді $g'^{p-1} = 1 - pu_1, (u_1, p) = 1, u \equiv u_1 (\mathrm{mod}\, p)$.

Тепер покладемо

$$\alpha_1 = (p-1)t + z$$
$$t = 0,1, \dots, \frac{1}{2}(p^{n-1} - 1), z = 0,1, \dots, p-2$$

Тоді

$$g^{\alpha_1} = g^z\left(1 + a_1 pt + a_2 p^2 t^2 + a_3 p^{\lambda_3} t^3 + \cdots\right)(\mathrm{mod}\, p^n),$$
$$a_1 \equiv -u_1, a_2 \equiv -2'u^2 (\mathrm{mod}\, p), \lambda_j \geqslant 3.$$

Аналогічно, ми маємо

$$g^{\lambda_2} \equiv g^{\alpha_0} g'^{\alpha_1} \equiv g^{\alpha_0} g'^z (1 + b_1 pt + b_2 p^2 t^2 + b_3 p^{\mu_3} t^3 + \cdots)(\mathrm{mod}\, p^n)$$
$$b_1 \equiv -u_1, b_2 \equiv -2'u^2 (\mathrm{mod}\, p), \mu_j \geqslant 3$$

Звідси,

$$N_1 g^{\alpha_1} + N_2 g^{\alpha_2} \equiv c_0 + c_1 pt + c_2 p^2 t^2 + c_3 p^{\nu_3} t^3 + \cdots (\mathrm{mod} p^n),$$

де $c_i = g^z a_i N_1 + g^{\alpha_0} g'^z b_i N_2, (i = 1,2)$.

З $(N_1, p) = (N_2, p) = 1$ ми маємо, що конгруенції

$$c_1 \equiv 0 (\mathrm{mod}\, p), c_2 \equiv 0 (\mathrm{mod}\, p)$$

не можуть справджуватись одночасно.

Але з $c_1 \equiv 0 (\mathrm{mod}\, p)$ випливає, що $g^{2z} \equiv g^{\alpha_0} N_2 N_1' (\mathrm{mod}\, p)$. Це можливо лише для єдиного значення z. Назвемо це значення z_0.

Тоді з (19) маємо:

$\widetilde{K}(a, b; h, p^n; k) = p^{n+2m} \times$

$$\times\left(\sum_{\substack{z=0\\z\neq z_0}}^{p-2}\sum_{t=0}^{\frac{1}{2}(p^{n-1}-1)} e^{2\pi i\frac{c_0}{p^n}}\cdot e_p^{n-1}(c_1t+c_2pt^2+c_3p^{\nu_3-1}t^3+\cdots)+ \quad (4.20)\right.$$

$$\left.+\sum_{t=0}^{\frac{1}{2}(p^{n-1}-1)} e^{2\pi i\frac{c_0'}{p^n}}\cdot e_{p^{n-2}}(c_1't+c_2't^2+c_3'p^{\nu_3-2}t^3+\cdots)\right)$$

де $(c_1,p)=(c_2',p)=1$.

Суми по t це неповні раціональні суми, оцінки яких ми отримуємо за допомогою оцінок повних експоненціальних сум.

Для довільного полінома $\Phi(t)\in\mathbb{Z}[t]$ маємо

$$\left|\sum_{t=0}^{T} e^{2\pi i\frac{\Phi(t)}{q}}-\frac{T}{q}\sum_{t=0}^{q-1} e^{2\pi i\frac{\Phi(t)}{q}}\right|\leqslant \quad (4.21)$$

$$\leqslant\sum_{r=1}^{q}\frac{1}{\min(r,q-r+1)}\left|\sum_{t=0}^{q-1} e^{2\pi i\frac{\Phi(t)-t}{q}}\right|.$$

Тепер якщо $\Phi(t)=c_1t+c_2pt^2+c_3p^{\nu_3-1}t^3+\cdots,(c_1,p)=1,q=p^{n-1}$ то повні суми в (4.21) дорівнюють нулю для всіх r окрім випадку $r\equiv c_1(\mathrm{mod}p)$. В цьому окремому випадку маємо

$$\Psi(t)=c_1't+c_2't^2+c_3'p^{\nu_3-1}t^3+\cdots,(c_2',p)=1,q=p^{n-2}$$

і тоді повна сума оцінюється через $2p^{\frac{n-2}{2}}$.

Звідси

$$\left|\widetilde{K}(a,b;h,p^n;k)\right|\leqslant p^{n+m}\left[\sum_{\substack{z=0\\z\neq z_0}}^{p-2}\frac{1}{|c_1(z)|}+\sum_{r=1}^{p^n}\frac{1}{kp}\cdot p^{\frac{n-2}{2}}+p\cdot p^{\frac{n-2}{2}}\right]$$

Нарешті, враховуючи, що для різних z ми маємо різні значення для $c_1(z) (\mathrm{mod}\ p)$. Тоді ми маємо

$$\left|\widetilde{K}(a,b;h,p^n;k)\right| \leqslant p^{\frac{3}{2}n+m}\left(\log\ p + \frac{\log\ p^n}{p}\right) \blacksquare$$

Таким чином, в даному розділі, ми довели 2 основні теореми що стосуються оцінок сум Клостермана, враховуючи умови, пов’язані з еліпсом.

ВИСНОВКИ

У виконаній роботі було проведено всебічний аналіз сум Клостермана і отримано оцінки для даних сум, враховуючи еліптичні обмеження.

Отримані оцінки узагальнених сум підтверджують, що введення еліптичного обмеження не лише зберігає властивості тонких оцінок, відомі для класичних сум, але й відкриває нові можливості для вивчення розподілу арифметичних функцій у розширеному алгебраїчному контексті. Зокрема, застосування таких оцінок дозволяє поширити класичні результати про розподіл функції дільників на випадок еліптичних обмежень.

Дослідження еліптичних інтегралів і еліптичних функцій сприяло глибшому розумінню аналітичних властивостей еліпса, а вивчення теоретико-числових основ еліптичних кривих відкрило перспективи для подальшого розвитку теми.

Практичне значення отриманих результатів полягає в тому, що вони можуть бути застосовані як в аналітичній теорії чисел для уточнення оцінок кореляційних сум і нелінійних послідовностей, так і в алгебраїчній теорії чисел для розв’язання діофантових задач у ширшому контексті. Крім того, можливості використання еліптичних кривих у криптографії вимагають подальшого дослідження зв’язку між оцінками узагальнених сум і стійкістю криптографічних протоколів.

Отже, було з’єднано класичні методи суми Клостермана з геометричними та алгебраїчними підходами, що дозволило отримати нові оцінки й відкрити перспективи для подальших досліджень у аналітичній теорії чисел та прикладній криптографії. У подальших дослідженнях доцільно розглядати узагальнення для інших форм обмежень (наприклад, гіпереліпсів) та аналізувати вплив цих оцінок на конкретні криптографічні задачі.

СПИСОК ЛІТЕРАТУРИ

1. Корольов М. А. Методи оцінок коротких сум Клостермана // Чебишевський збірник. – 2016. – Т. 17, вип. 4. – С. 79-109.
2. Корольов М. А. Про короткі суми Клостермана за простим модулем // Математичні замітки. – 2016. – Т. 100, вип. 6. – С. 838-846.
3. Abramowitz M., Stegun I. A. Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. – New York: Dover, 1972.
4. Birch B. J., Swinnerton-Dyer H. P. F. Notes on Elliptic Curves I // J. reine angew. Math. – 1963. – Vol. 212. – P. 7-25.
5. Birch B. J., Swinnerton-Dyer H. P. F. Notes on Elliptic Curves II // Proc. London Math. Soc. – 1964. – Ser. 3. – Vol. 14. – P. 78-81.
6. Boyd P. F., Friedman M. D. Handbook of Elliptic Integrals for Engineers and Physicists. – 2nd ed. – Berlin: Springer, 1971.
7. Bombieri E. On exponential sums in finite fields // Invent. Math. – 1978. – Vol. 47, №1. – P. 29-39.
8. Bruggeman R. Fourier Coefficients of Automorphic Forms // Lecture Notes in Mathematics. – Berlin: Springer-Verlag, 1981. – Vol. 865.
9. Bruggeman R. W. Fourier coefficients of cusp forms // Invent. Math. – 1978. – Vol. 445. – P. 1-18.
10. Bruggeman R., Motohashi Y. Sum formula for Kloosterman sums and fourth moment of the Dedekind zeta-function over the Gaussian number field // Functiones et Approximatio. – 2003. – Vol. 31. – P. 23-92.
11. Cui J., Wang L. The generalized Kloosterman’s sums and its fourth power mean // AIMS Mathematics. – 2023. – Vol. 8, №11. – P. 26590-26599.
12. Deligne P. La conjecture de Weil. I, II // Publ. Math. IHES. – 1974. – Vol. 43. – P. 273-307; 1980. – Vol. 52. – P. 137-252.
13. Gauss C.F. Theoria combinationum observationum erroribus minimis obnoxiarum / C. F. Gauss. – Hamburg: F. Perthes, 1823. – 172 p.
14. Ireland K., Rosen M. A Classical Introduction to Modern Number Theory. – New York: Springer-Verlag, 1982.
15. Iwaniec H. Topics in Classical Automorphic Forms. – Providence: American Mathematical Society, 1997.
16. Katz N. M., Sarnak P. Random Matrices, Frobenius Eigenvalues, and Monodromy. – Providence: American Mathematical Society, 1999.
17. Koblitz N. Introduction to Elliptic Curves and Modular Forms. – 2nd ed. – New York: Springer-Verlag, 1993.
18. Kloosterman H. D. On the representation of numbers in the form ax^2 + by^2 + cz^2 + dt^2 // Acta Math. – 1926. – Vol. 49. – P. 407-464.
19. Kuznetsov N. V. Peterson hypothesis for the form with weight zero and Linnik hypothesis // Mat. Sb. – 1980. – Vol. 111, no. 3. – P. 334–383.

20. Lang S. Elliptic Curves: Diophantine Analysis. – New York: Springer-Verlag, 1978.
21. Motohashi Y. Spectral Theory of the Riemann zeta-function. – Cambridge: Cambridge Univ. Press, 1997.
22. Radova A., Varbanets S. On exponential sums involving the divisor function over Z[i] // Ann. Univ. Sci. Budapest, Sect. Comp. – 2017. – Vol. 46. – P. 235-246.
23. Savastru O., Varbanets S. Norm Kloosterman sums over Z[i] // Algebra Discrete Math. – 2011. – Vol. 11, №2. – P. 82-91.
24. Washington L. C. Elliptic Curves : Number Theory and Cryptography. – 2nd ed. – Boca Raton: CRC Press, 2008.
25. Weil A. On some exponential sums // Proc. Natl. Acad. Sci. USA. – 1948. – Vol. 34. – P. 204-207.
26. Ye Y. The lifting of Kloosterman sums // J. Number Theory. – 1995. – Vol. 51. – P. 275-287.
27. Ye Y. The lifting of an exponential sum to a cyclic algebraic number field of prime degree // Trans. Amer. Math. Soc. – 1998. – Vol. 350. – P. 5003-5015.
28. Zanbyrbaeva U. Asympotic problems of number theory in sector region // Dissertation, Odessa, 1993.