Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Варбанець Сергій Павлович

УДК 511.33, 519.2

Метод тригонометричних сум в теорії конгруентних генераторів псевдовипадкових чисел та асимптотичних задачах теорії чисел

01.01.08 — математична логіка, теорія алгоритмів і дискретна математика

Автореферат
дисертації на здобуття наукового ступеня
доктора фізико-математичних наук

Київ — 2021

Дисертацією є рукопис.

Робота виконана в Одеському національному університеті імені І.І. Мечникова Міністерства освіти і науки України.

Науковий консультант: доктор фізико-математичних наук, професор **Кореновський Анатолій Олександрович**, Одеський національний університет імені І. І. Мечникова, завідувач кафедри математичного аналізу.

Офіційні опоненти: доктор фізико-математичних наук, професор **Працьовитий Микола Вікторович**, Національний педагогічний університет імені М. П. Драгоманова, декан фізико-математичного факультету;

доктор фізико-математичних наук, старший науковий співробітник **Глазунов Микола Михайлович**, Інститут кібернетики імені В.М. Глушкова НАН України, провідний науковий співробітник;

доктор фізико-математичних наук, доцент **Бондаренко Євген Володимирович**, Київський національний університет імені Тараса Шевченка, доцент кафедри алгебри і комп'ютерної математики.

Захист відбудеться «05» травня 2021 р. о 15 годині на засіданні спеціалізованої вченої ради Д 26.001.18 Київського національного університету імені Тараса Шевченка за адресою: 03127, м. Київ, просп. Академіка Глушкова, 4е.

З дисертацією можна ознайомитись у науковій бібліотеці імені М. Максимовича Київського національного університету імені Тараса Шевченка.

Автореферат розісланий «02» квітня 2021 р.

Вчений секретар спеціалізованої вченої ради  Журавльов В.,М.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Диссертаційна робота присвячена застосуванню методу тригонометричних сум в аналітичній теорії чисел і в задачах генерування псевдовипадкових чисел. Починаючи з робіт Харді и Літлвуда, а також І.М. Виноградова, цей метод дозволив розв'язати багато задач сучасної математики. Цим методом будуються асимптотичні формули для суматорних функцій арифметичних функцій, досліджується розподіл значень дзета-функції Римана та її узагальнень, вивчаються властивості арифметичних функцій на спеціальних множинах цілих чисел, оцінюється якісність послідовностей псевдовипадкових чисел, породжених деякими конгруентними генераторами псевдовипадкових чисел, і багато інших проблем теоретичної і практичної математики.

Нехай f(x) - дійсно-значна функція на множині A, де A - скінчена підмножина k-вимірного дійсного або комплексного простору. Тоді сума

$$\sum_{x\in A} e^{2\pi i f(x)}$$

називається тригонометричною.

В більш загальному випадку, суму вигляду

$$\sum_{x\in A} g(x)e^{2\pi i f(x)}$$

будемо називати суматорною функцією для $g(x)$, зваженою тригонометричними одиницями $e^{2\pi i f(x)}$.

Такі Суми досліджуються в дисертації.

В дисертаційній роботі отримані результати по оцінкам спеціальних тригонометричних сум на відрізках натурального ряду: $A := \{X_1 \leqslant x \leqslant X_2,\ x \in \mathbb{Z}\}$, а функція f є поліном або дробово-раціональна функція. Ще К.Ф. Гаусс за допомогою суми

$$\sum_{x=0}^{q-1} e^{2\pi i \frac{ax^2}{q}}$$

побудував теорію квадратичних лишків за модулем q, продовженням якої є знаменита теорема Виноградова-Пойа для квадратичних

лишків.

Сучасна теорія тригонометричних сум будується на дослідженнях Гаусса, Клостермана, Ван дер Корпута, Виноградова, Г. Вейля, Г. Давенпорта, Л. Морделла, А. Вейля, А. Карацуби, Х. Іванця, М. Хакслі, Е. Бомб'єрі, Р. Д. Хіз-Брауна, Хуа Ло Кена, І. Катаі, А. Івича, Ж. М. ДеКонінка, М. Ютіли, С. Степанова та інших.

Дисертаційна робота присвячена побудові оцінок спеціальних тригонометричних сум (і в першу чергу суми Клостермана та її узагальнень над кільцем цілих гаусових чисел), застосуванню тригонометричних сум для оцінки якісності конгруентних генераторів псевдовипадкових чисел (за допомогою дискріпантної функції) і побудові асимптотичних формул для суматорних функцій, асоційованих з мультиплікативною функцією $\tau_k(\alpha)$, $\alpha \in \mathbb{Z}[i]$ та іншими арифметичними функціями над $\mathbb{Z}$ або $\mathbb{Z}[i]$.

К. Гаусс встановив тотожність для простого p:

$$\sum_{x=0}^{p-1} e^{2\pi i \frac{x^2}{p}} = \begin{cases} \sqrt{p}, & \text{якщо} \quad p \equiv 1 \pmod 4, \\ i\sqrt{p}, & \text{якщо} \quad p \equiv 3 \pmod 4. \end{cases}$$

А. Вейль (1948 р.) отримав більш загальну оцінку

$$\left| \sum_{x=0}^{p-1} e^{2\pi i \frac{g(x)}{p}} \right| \leqslant (d, p-1) p^{\frac{1}{2}}$$

для кожного поліному$g(x)$ степені d, $(d, p) = 1$.

Цей результат став наслідком доведеної А. Вейлем гіпотези Римана для алгебраїчних кривих над скінченим полем. У випадку, коли змінна підсумовування пробігає елементи скінченого поля $\mathbb{F}_{p^m}$ П'єр Делінь в 1973 р. отримав оцінку для суми

$$S_j(g) := \sum_{x \in \mathbb{F}_{p^j}^n} e^{2\pi i \frac{Tr_j(g(x))}{p}},$$

яка узагальнює результат А. Вейля.

Результат Деліня було узагальнено М. Кацем (1980 р.).

В дисертації ми використовуємо результати Деліня і Бомб'єрі для тригонометричних сум при побудові n-вимірних нормених сум Клостермана кільця $\mathbb{Z}[\theta]$.

Т. Кочрейн та В. Зенг вивчали "чисті"та "змішані"тригонометричні суми виду

$$S(f,p^m) := \sum_{x\in\mathbb{Z}_{p^m}} e^{2\pi i\frac{f(x)}{p^m}},$$

$$S(\chi,f,p^m) := \sum_{x\in\mathbb{Z}^*_{p^m}} \chi(x)e^{2\pi i\frac{f(x)}{p^m}},$$

де p - просте число, $m \geqslant 3$ - позитивне ціле, χ - мультиплікативний характер групи $\mathbb{Z}^*_{p^m}$, $f(x) \in \mathbb{Z}^*_{p^m}$.

Для $m = 1$ такі суми були оцінені А. Вейлем.

В дисертаційній роботі також розглядаються аналоги цих сум над кільцем $\mathbb{Z}[\theta]$.

Відмінність цього випадку в тому, що для нерозкладних простих чисел p кільця $\mathbb{Z}[\theta]$ мультиплікативна група $\mathbb{Z}[\theta]_{p^m}$ не є циклічною.

Тригонометричні суми використовуються для оцінки дискріпансії послідовностей псевдовипадкових чисел, які породжуються генераторами, що розглядаються в дисертації.

В дисертаційній роботі будуються узагальнені інверсні генератори псевдовипадкових чисел. Псевдовипадкові числа являють собою важливу складову стохастичного моделювання і сучасної криптографії. Випадкові біти необхідні не тільки для генерування криптографічних ключів, але часто вони становлять головну частину криптографічних алгоритмів. Як правило, на сьогоднішній день джерелом випадковості є псевдовипадковий числовий генератор, який являє собою детермінований алгоритм, що породжує послідовність чисел з певними статистичними властивостями, і насамперед, розподіленість за даним законом та статистична незалежність (непередбачуваність). Генератори псевдовипадкових чисел є елементами кожної системи захисту інформації, вони використовуються для розв'язання багатьох задач, таких як

— моделювання реальних процемів за методом Монте-Карло;
— генерування гаміруючих послідовностей при перетворенні інформації за схемою найбільш близькою до схеми абсолютно стійкого шифру;
— хешування інформації;
— формування ключової інформації, на секретності і якості якої будується стійкість шифру;

— внесення невизначеності в роботу засобів захисту інформації і так далі.

Ми будуємо генератори псевдо-випадкових чисел за допомогою конгруенції

$$y_{n+1} \equiv ay_n^{-1} + b + F(n) \pmod{p^m},$$

де $F(n)$ є поліномом гад $\mathbb{Z}_{p^m}$ великої степені з числом ненульових коефіцієнтів в кількості $\leqslant 4$.

Цей генератор узагальнює інверсний конгруентний генератор, досліджений Ейченауером і Лехном, Нідерайтером і Шпарлінським та ін. Кріми того, розглядаються нові генератори ПВЧ, які пов'язані з розподілом елементів норменої групи E_m, яка є підгрупою кільця класів лишків по модулю p^m з нормою, конгруентною до -1 за модулем p^m, де p нерозкладне просте в кільці $\mathbb{Z}[\theta]$. Такі генератори ми називаємо циркулярними, тому що вони пов'язані з розподілом точок, які є розв'язками конгруенції $x^2 + dy^2 \equiv 1 \pmod{p^m}$, тобто з точками еліпсу над скінченим кільцем $\mathbb{Z}_{p^m}$.

Наприкінці XX століття американські вчені Н. Кобліц і В. Мілер звернули увагу на те, що секретну інформацію можна ховати в координатах точок еліптичної кривої $y^2 = x^3 + ax + b$ над скінченим полем з p^m елементів. Так були побудовані аналоги сучасних криптосистем з відкритим ключем. А незабаром виявилось, що послідовності псевдовипадкових чисел можна генерувати за допомогою координат точок еліптичних кривих над скінченим полем. В нашій роботі будуються генератори ПВЧ за допомогою еліптичних кривих над скінченим кільцем класів лишків $\mathbb{Z}_{p^m}$. Привабливість використання еліптичних кривих над скінченими полями або скінченими кільцями полягає в тому, що складність взлому відповідних криптосистем з відкритим ключем зростає, а об'єм обчислень для шифрування інформації або генерування послідовностей ПВЧ скорочується.

Також в другому розділі доведено аналог нерівності Турана-Ердьоша-Коксми для оцінки якісності послідовності комплексних ПВЧ в одиничному колі. Показано, рівномірність розподілу таких чисел в секторах одиничного кола.

Другим застосуванням методу тригонометричних сум є дослідження розподілу значень зважених функцій дільників $\tau_k(\alpha)$, $\alpha \in \mathbb{Z}[i]$, $k = 2, 3$, що можна розглядати як продовження робот М. Ютіли та О. Гунявого для зваженої функції дільників $\tau(n)$ над $\mathbb{Z}$. Тригономе-

тричні суми використовуються нами для вивчення розподілу значень функцій $\tau_k(\alpha)$ в арифметичній прогресії з розтучою по модулю різницею прогресії.

В третьому розділі роботи вивчаються арифметичні функції на спеціальних послідовностях цілих чисел уявного квадратичного розширення поля $\mathbb{Q}(\sqrt{-d})$. Зокрема побудована асимптотична формула для кількості зображень натуральних чисел нормою цілих елементів кільця $\mathbb{Z}[\theta]$ в арифметичних прогресіях і в вузьких секторах. Використовуючи аналоги результатів Ліу, Шпарлінського і Зенга, ми будуємо асимптотичну формулу про розподіл норм елементів кільця $\mathbb{Z}[\theta]$ (θ - породжуючий елемент кільця цілих чисел уявного квадратичного поля) в арифметичній прогресії по модулю степені простого раціонального числа p. Нами побудована асимптотична формула, пов'язана з зображенням натуральних чисел k-тими степенями позитивно означених квадратичних форм від двох змінних. Цю проблему можна розглядати як узагальнення теореми Варинга сумою k-тих степеней натуральних чисел.

Ще одним застосуванням методу тригонометричних сум є побудова асимптотичної формули в проблемі еліпсу в арифметичній прогресії. Такі дослідження важливі для проблеми про оцінки другого моменту Z-функції Геке на половинній прямій $\operatorname{Re} s = \frac{1}{2}$.

В останньому підрозділі третього розділу роботи вивчається перетворення Лапласа добутку двох Z-функцій Геке зі зсувом. Цей результат також можна застосовувати для побудови асимптотичної формули другого моменту Z-функції Геке з зсувом.

Таким чином, дослідження, які проведені в дисертації є новими і актуальними.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконана на кафедрі комп'ютерної алгебри та дискретної математики Одеського національного університету імені І.І. Мечникова у рамках держбюджетних тем "Дослідження асимптотичних задач комп'ютерної алгебри і аналітичної теорії чисел"(№ державної реєстрації 0107U004622) і "Застосування тригонометричних сум у криптографії"(№ державної реєстрації 0114U001489).

Мета і задачі дослідження. Основною тематикою роботи є дослідження класу конгруентних генераторів, які породжують по-

слідовності псевдовипадкових чисел, розробка математичних методів для генерування конгрентних псевдовипадкових чисел, обґрунтування псевдовипадковості згенерованих чисел, побудова нових оцінок тригонометричних сум над кільцем цілих чисел уявного квадратичного поля, а також побудова асимптотичних формул для суматорних функцій, асоційованих з мультиплікативними функціями над кільцем цілих чисел уявного квадратичного поля.

Об'єкт дослідження. Об'єктом дослідження є тригонометричні суми спеціального виду над кільцями цілих раціональних і цілих чисел уявного квадратичного поля, конгруентні генератори псевдовипадкових чисел, генератори ПВЧ на алгебраїчних кривих (в тому числі на еліптичних кривих), суматорні функції над кільцем цілих чисел уявного квадратичного поля і побудова для них асимптотичних формул, асимптотична формула для перетворення Лапласа добутку двох Z-функцій Геке.

Предмет дослідження. Предметом дослідження є тригонометричні суми над кільцем цілих чисел уявного квадратичного поля, узагальнені суми Клостермана, чисті і змішані нормені суми Клостермана, функції дільників цілих чисел уявного квадратичного поля, що зважені тригонометричними одиницями а бо сумами Клостермана, нормена підгрупа мультиплікативної групи кільця цілих чисел уявного квадратичного поля, проблема еліпсу в арифметичній прогресії та функція зображень натуральних чисел k-тими степенями квадратичної форми, Z-функції Геке з зсувом.

Методи дослідження. У дисертаційній роботі використовуються методи аналітичної теорії чисел в асимптотичних задачах, а також метод дискріпансії для доведення псевдовипадковості побудованих послідовностей, згенерованих конгруентними рекурсіями. Крім того, застосовуються методи рядів Діріхле, функціональних рівнянь для дзета-функції Римана і Z-функції Геке.

Наукова новизна одержаних результатів. Наукова новизна результатів полягає в побудові нових конгруентних генераторів псевдовипадкових чисел; отриманні нових верхніх та нижніх оцінок дискріпансії для згенерованих послідовностей псевдовипадкових чисел; дослідженні нових сум Клостермана; а також в отриманні доведених в роботі асимптотичних оцінок суматорних функцій для $\tau(\alpha)$,

$\tau_3(\alpha)$, зважених тригонометричними одиницями або сумами Клостермана. Новою є формула Лапласа для добутку двох Z-функцій Геке з зсувом. У дисертаційній роботі отримані такі нові результати:

- оцінки повних і змішених тригонометричних сум над кільцем цілих чисел уявного квадратичного поля;
- нові оцінки сум Клостермана n-го порядку над кільцем цілих чисел уявного квадратичного поля;
- оцінки узагальнених сум Клостермана над кільцем цілих чисел уявного квадратичного поля;
- нормені суми Клостермана n-го порядку над кільцем цілих чисел уявного квадратичного поля;
- нові оцінки дискріпантної функції інверсного генератора зі змінним зсувом;
- побудовані інверсні генератори другого порядку і знайдені оцінки відповідних дискріпантних функцій;
- побудовано сімейство циркулярних генераторів, доведена псевдовипадковість породжуваних ними послідовностей псевдовипадкових чисел;
- досліджено на псевдовипадковість послідовність, породжена лінійно-інверсним генератором;
- побудовано алгоритм генерації ПВЧ за допомогою еліптичних кривих над скінченим кільцем $\mathbb{Z}_{p^m}$;
- побудована асимптотична формула в проблемі еліпса на арифметичній прогресії;
- досліджена асимптотична поведінка суматорної функції для функції дільників, зваженої сумами Клостермана над $\mathbb{Z}[\theta]$;
- знайдена асимптотична формула для суматорної функції, асоційованої з кількістю зображень натуральних чисел k-тими степенями позитивно визначеної квадратичної форми;
- досліджені аналітичні властивості перетворення Лапласа для пари Z-функцій Геке з зсувом.

Практичне значення одержаних результатів. Робота має теоретичний характер, хоча її результати по генеруванню псевдовипадкових чисел мають прикладний характер. Отримані результати є внеском в теорію тригонометричних сум над кільцями цілих і цілих гаусових чисел, а також в теорії генерування послідовностей псевдовипадкових чисел. Результати роботи можуть бути використані в

задачах аналітичної теорії чисел з проблем, пов'язаних з розподілом значень мультиплікативних функцій на відрізках натурального ряду та в вузьких секторіальних областях комплексної площини.

Особистий внесок здобувача. Основні результати, що виносяться на захист, отримані автором самостійно. Визначення напрямку досліджень належить науковому консультанту професору А.О. Кореновському. У спільних статтях з проф. П.Д. Варбанцем співавтору належить обговорення загального підходу у використанні тригонометричних сум в асимптотичних задачах теорії чисел. Основні результати отримані дисертантом особисто. У наукових статтях у співавторстві з доц. О.В. Савастру, присвячених норменим сумам Клостермана співавтору належить ідея використання результатів Деліня, в статті, присвяченій зображенню чисел сумою значень позитивно визначених квадратичних форм в s-тих степенях - внесок обох авторів є рівноцинним. Основні результати статей у співавторстві з Я.А. Воробйовим здебільшого належать здобувачу. У спільних роботах з А.С. Радовою основні результати також належать здобувачу. Усі співавтори приймали участь в обговоренні основних результатів спільних статей.

Апробація результатів дисертації. Результати дисертації доповідались та обговорювалися на наукових конференциях та засіданнях наукових семинаров провідних українських та міжнародних наукових установ, а саме:

Конференції:

1. 4th Chaotic Modeling and Simulation International Conference, 31 May - 3 June 2011 Agios Nikolaos Crete Greece.
2. 8th International Algebraic Conference in Ukraine, July 5-12 (2011), Lugansk, Ukraine, 2011.
3. 5th Chaotic Modeling and Simulation International Conference, 12-15 June 2012 Athens Greece.
4. International Conference dedicated to the 120th anniversary of Stefan Banach, 2012.
5. 6th Chaotic Modeling and Simulation International Conference, 11-14 June 2013 Istanbul Turkey.
6. Numbers, Functions, Equations 2013, Dedicated to Professors

Zoltan Daroczy and Imre Katai on the occasion of their 75th birthday, Visegrad, Hungary June 28–30, 2013.

7. 9th International Algebraic Conference in Ukraine, July 8-13, 2013.
8. The Fifth International Conference on Analytic Number Theory and Spatial Tessellations, Kyiv, Ukraine, September 16-20, 2013.
9. 7th Chaotic Modeling and Simulation International Conference, 7-10 June 2014 Lisbon Portugal.
10. 11th Vilnius Confgerence on Probababilistic Theory, 2014.
11. The International Algebraic Conference dedicated to the 100th anniversary of L.A. Kaluzhnin, Jyly 7-12, 2014.
12. 8th Chaotic Modeling and Simulation International Conference, 26-29 May 2015 Paris, France.
13. X International Algebraic Conference in Ukraine dedicated to 70th anniversary of Yu. A. Drozd, 2015.
14. 9th Chaotic Modeling and Simulation International Conference, 23-26 May 2016 London, UK.
15. XII Белорусская математическая конференция, 5–10 сентября 2016 года, Минск, Беларусь.
16. International Conference Groups and Actions: Geometry and Dynamics December 19-22, Kyiv, Ukraine.
17. 2nd International Conference on Computer Algebra and Information Technologies, August 21 – 26, 2016, Odessa, Ukraine.
18. 10th Chaotic Modeling and Simulation International Conference, 30 May-2 June 2017 Barcelona, Spain.
19. XI International Algebraic Conference in Ukraine dedicated to 75th anniversary of V. V. Kirichenko, 2017 11th Chaotic Modeling and Simulation International Conference, 5-8 June 2018 Rome, Italy
20. International Conference Computer Algebra and Information Technologies, Odessa (Ukraine), August 20 – August 25, 2018.
21. The Sixth International Conference on Analytic Number Theory and Spatial Tessellations, Kyiv, Ukraine September 24-28, 2018.
22. Numbers, Functions, Equations 2018, Hajduszoboszlo (Hungary), August 26 – September 1, 2018.
23. 13th Chaotic Modeling and Simulation International Conference, 9-12 2020 June.

24. Chaotic Modeling and Simulation Web Conference 22-24 October 2020.

Наукові семінари:

1. Одеський міський семінар по теорії графів (2014, 2015, 2016, 2017).
2. Семінари по аналітичній теорії чисел Одеського національного університету імені І. І. Мечникова.
3. Розширене засідання «Під кінець року» Алгебраїчного семінару Київського національного університету імені Тараса Шевченка, Київ 29 грудня 2020.

Публікації. Основні результати роботи викладено у 34 ([135]-[166]) наукових статтях, які опубліковано у виданнях, що внесені до переліку наукових фахових видань України та іноземних періодичних фахових виданнях, причому дві з цих статтей [137] та [165] є науковими публікаціями у виданнях, віднесених до третього квартиля (Q3). Згідно з наказом Міністерства освіти і науки України №1220 від 23 вересня 2019 року "Про опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук"наукова публікація у виданні, віднесеному до першого та другого квартилів (Q1, Q2) відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports, прирівнюється до трьох публікацій, наукова публікація у виданні, віднесеному до третього квартиля (Q3) відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports, прирівнюється до двох публікацій. Матеріали дисертації також додатково відображено у 21 матеріалах конференцій [167]-[187]. 18 публікацій ([135]-[136], [139], [143]-[147], [150]-[152], [154]-[156], [159], [161], [162], [165]) надруковано у наукових періодичних виданнях, що включені до міжнародних наукометричних баз даних.

Структура та обсяг дисертації. Дисертація складається зі вступу, анотації, трьох розділів, розбитих на підрозділи, висновків, списку використаних джерел із 192 найменувань та додатку, що містить список публікацій здобувача за темою дисертації та відомості про апробацію результатів. Повний обсяг дисертації становить 285 сторінок, основний текст займає 231 сторінки.

Подяка. Автор вдячний своєму науковому консультанту Кореновському Анатолію Олександровичу за підтримку і надання кваліфікаційних роз'яснень по деяким питанням, пов'язаним з третім розділом дисертації та за доцільні зауваження.
Автор висловлює щиру вдячність член-кореспонденту НАН Україна Дрозду Юрію Анатолійовичу (Київ, Україна), академіку Академії Наук Угорщини Імре Катаі(Будапешт, Угорщина) та професору Вільнюського університету Антанасу Лауринчикасу за увагу до роботи, підтримку, корисні поради та роз'яснення окремих питань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

Метод тригонометричних сум у перше проявив свою силу в доведенні класичних проблем Варинга і Гольдбаха, які були розв'язані І.М. Виноградовим в 30-х роках минулого століття. Багато задач асимптотичної та статистичної теорії чисел мають асимптотичні формули з нетривіальним залишком завдяки використанню тригонометричних сум над кільцем цілих раціональних або над кільцями цілих алгебраїчних чисел скінчених розширень поля раціональних чисел. В роботі метод тригонометричних сум використовується для оцінки "якісності"послідовностей, які генеруються конгруентними генераторами, а також для побудови нетривіальних асимптотичних формул розподілу арифметичних функцій над кільцями $\mathbb{Z}$ і $\mathbb{Z}[\theta]$.

У вступі дисертації обґрунтовано актуальність теми, вказано зв'язок роботи з науковими програмами, планами, темами, визначено мету і завдання, об'єкт, предмет та методи дослідження, вказано наукову новизну та практичне значення отриманих результатів, охарактеризовано особистий внесок здобувача, апробацію отриманих результатів. Наведено також список семінарів та конференцій, на яких дисертаційна робота пройшла апробацію. Вступ дисертації містить огляд літератури за тематикою дослідження.

В першому розділі розглядаються тригонометиричні суми над кільцями $\mathbb{Z}$ і $\mathbb{Z}[\theta]$, які використовуються в розділах 2 і 3, а саме вивчаються повні тригонометричні суми з многочленом в показнику над кільцем цілих елементів уявного квадратичного розширення

поля раціональних чисел $\mathbb{Q}$. Тригонометрична сума виду

$$\sum_{x\in G_{\mathfrak{p}^m}} \chi(x)\exp\left(\frac{Spf(x)}{p^m}\right)$$

називається повною тригонометричною сумою з характером (або твістовою сумою), де χ мультиплікативний характер групи $G^*_{p^m}$. Для полінома $f(x)\in G[x]$, $f(x)=a_0+a_1x+\cdots+a_dx^d$ введемо наступні позначення:

$$\begin{aligned} t=t(f) &:= \operatorname*{ord}_p(f'(X)) = \min_{1\leqslant i\leqslant d}(\nu_p((ia_i))),\\ t_1=t_1(f) &:= \operatorname*{ord}_p(rXf'(X)+C_1),\\ t_2=t_2(f) &:= \operatorname*{ord}_p(rXf'(X)+C_2). \end{aligned}$$

Позначимо через A_i, $i=1,2$ множину критичних точок, асоційованих з сумою $S(\chi,f,p^m)$. Покладемо

$$S_\alpha(f,p^m)=S_\alpha := \sum_{\substack{x\in G_{p^m}\\ x\equiv\alpha \pmod p}} e_{p^m}(f(x)).$$

ТЕОРЕМА. *Нехай $\mathfrak{p}$ - непарне просте число кільця $\mathbb{Z}[\theta]$, m - позитивне ціле число і $f(x)$ - многочлен степені $\geqslant 1$ над $G_\mathfrak{p}$, $t=\operatorname{ord}_\mathfrak{p}(f(x))$. Тоді для $m\geqslant t-2$ маємо*

(i) $S_\alpha(f,\mathfrak{p}^m)=0$, *якщо* $\alpha\notin A$

(ii) $|S_\alpha(f,\mathfrak{p}^m)|\leqslant \nu N(\mathfrak{p})^{\frac{1}{\nu+1}}N(\mathfrak{p}^m)^{1-\frac{1}{\nu+1}}$, *якщо* $\alpha\in A$.

де ν - кратність точки $\alpha\in A$, A - множина критичних точок для суми $S_\alpha(f,\mathfrak{p}^m)$.

ТЕОРЕМА. *Нехай p нерозкладне просте число кільця $\mathbb{Z}[\theta]$, $f(x)\in G_{p^m}$, причому $m\geqslant t+2$. Тоді для кожного $\alpha\in G_{p^m}$*

(i) *Якщо $\alpha\notin A$, тоді $S_\alpha(f,p^m)=0$.*

(ii) *Якщо α - критична точка кратності ν, тоді*

$$|S_\alpha(f,p^m)|\leqslant \nu p^{\frac{2}{\nu+1}}p^{2m\left(1-\frac{1}{\nu+1}\right)}.$$

(iii) *Якщо α - критична точка кратності 1, тоді*

$$S_\alpha(f,p^m)=\begin{cases} e_{p^m}(f(\alpha^*))p^{\frac{m+t}{2}}, \text{ якщо } m-t \text{ - парне},\\ \chi_2(A_\alpha)e_{p^m}(f(\alpha^*))\cdot G(p)p^{\frac{m+t-1}{2}}, \text{ інакше},\end{cases}$$

де α^* - єдиний розв'язок конгруенції $p^{-t}f'(x)\equiv 0 \pmod{p^{\frac{m-t+1}{2}}}$, що лежить над α, і $A_\alpha = 2p^{-t}f''(\alpha^*) \pmod p$; $G(p)$ - сума Гауса над кільцем $\mathbb{Z}[\theta]$ за модулем p.

Нехай p - просте раціональне число, яке нерозкладне в кільці $\mathbb{Z}[\theta]$, χ - мультиплікативний характер $\pmod{p^m}$ над $\mathbb{Z}[\theta]$:

ТЕОРЕМА. *Нехай $\mathfrak{p}$ - просте непарне число із $\mathbb{Z}[\theta]$, $f\in\mathbb{Z}[\theta]$, а числа t_1, t_2 визначені вище. Тоді для кожного $\alpha\in A$, $(\alpha,\mathfrak{p})=1$:*

(i) *$S_\alpha(\chi,f,\mathfrak{p}^m)=0$, якщо $\alpha\notin A$;*

(ii) *для $\alpha\in A$*

$$S_\alpha(\chi,f,\mathfrak{p}^m)=\begin{cases} \chi(\alpha^*)\exp\left(Sp\frac{f(\alpha^*)}{\mathfrak{p}^m}\right)N(\mathfrak{p})^{\frac{m+t}{2}},\\ \text{якщо } m-t\text{-парне}\\ \chi(\alpha^*)\exp\left(Sp\frac{f(\alpha^*)}{\mathfrak{p}^m}\right)\left(\frac{a(\alpha)}{N(\mathfrak{p}^m)}\right)S(\mathfrak{p})N(\mathfrak{p})^{\frac{m+t-1}{2}},\\ \text{якщо } m-t\text{-непарне}\end{cases}$$

де α^* - розв'язок конгруенції $\mathfrak{p}^{-t}(Rxf'(x)+c)\equiv 0 \pmod{p^{\frac{m-t+1}{2}}}$, $S(\mathfrak{p})$ - сума Гауса над полем $G_\mathfrak{p}$, а параметри R і c визначаються характером χ.

В підрозділі 1.2 розглядаються узагальнення сум Клостермана над кільцями цілих елементів уявного квадратичного розширення поля раціональних чисел по модулю $\mathfrak{p}^m$. Для цілих α, β, γ з $\mathbb{G}$ ми визначаємо суму Клостермана, як

$$K(\alpha,\beta;\gamma)=\sum_{x\in\mathbb{G}^*_\gamma}\exp\left(\pi i Sp\frac{\alpha x+\beta x'}{\gamma}\right).$$

Нехай $k_1,k_2>1$ - натуральне число. Розглядаємо узагальнену суму Клостермана над $\mathbb{Z}[\theta]$

$$K(\alpha,\beta;k_1,k_2;\gamma,\chi)=\sum_{x\in G^*_\gamma}\chi(x)\exp\left(\pi i Sp\frac{\alpha x^{k_1}+\beta x'^{k_2}}{\gamma}\right),$$

де α, β, $\gamma \in \mathbb{Z}[\theta]$, χ - мультиплікативний характер за модулем γ. Ми називаємо $K(\alpha, \beta; k; \gamma, \chi)$ узагальненою степеневою сумою Клостермана.

ТЕОРЕМА. *Нехай k_1 і k_2 - позитивні цілі числа, причому $k_1 \Big| k_2$ і нехай $\gamma = \prod\limits_{\substack{i=1 \\ \mathfrak{p}_i \text{ - розкладне}}}^{s} \mathfrak{p}_i^{n_i} \prod\limits_{\substack{j=1 \\ p_j \text{ - нерозкладне}}}^{t} p_j^{n_j}$. Тоді*

$$|K(\alpha, \beta; k_1, k_2; \gamma)| \leqslant 2D\sqrt{N((\alpha, \beta, \gamma))}N(\gamma)^{\frac{1}{2}},$$

де $D = k_1 \prod\limits_{i=1}^{s} (k_2, p_j - 1) \prod\limits_{j=1}^{t} (k_2, p_j^2 - 1)$.

В цьому ж підрозділі також досліджуються суми Клостермана на еліпсі:

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

ТЕОРЕМА. *Нехай $(h, p) = 1$. Тоді*

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

з абсолютною константою в символі "$\ll$".

Для натурального $k > 1$ покладемо

$$\widetilde{K}(\alpha, \beta; h, q; k_1, k_2) := \sum_{\substack{x,y (mod\, q) \\ N(xy) \equiv h (mod\, q)}} e_q\left(\frac{1}{2} Sp\left(\alpha x^{k_1} + \beta y^{k_2}\right)\right).$$

ТЕОРЕМА. *Нехай p нерозкладне, $h \in \mathbb{Z}$, $(h, p) = 1$, $k_1, k_2 \in \mathbb{N}$, $k_1 | k_2$, $t = (k_1, p-1)$. Тоді для будь-яких цілих чисел α, β, $(\alpha, \beta, p) = 1$ кільця $\mathbb{Z}[\theta]$ справедлива оцінка*

$$\left|\widetilde{K}(\alpha, \beta; h, p; k_1, k_2)\right| \ll \begin{cases} t^2 p^{\frac{3}{2}}, & \text{якщо} \quad t - 1 \leqslant \sqrt[4]{p}, \\ dp^2, & \text{якщо} \quad t \geqslant \sqrt[4]{p} + 1. \end{cases}$$

ТЕОРЕМА. *Нехай p - просте нерозкладне число, $h \in \mathbb{Z}$, $(h,p) = 1$, $k_1, k_2 > 1$ натуральні, $k_1 | k_2$, a, b - цілі числа в $\mathbb{Z}[\theta]$, $(a,p) = (b,p) = 1$. Тоді для $n \geqslant 2$*

$$\left|\widetilde{K}(a,b;h,p^n;k_1,k_2)\right| \leqslant 2p^{\frac{3}{2}n+m}\log p^n,$$

де $m = \nu_p(k_1)$.

В цьому ж підрозділі далі ми вивчаємо n-мірні суми Клостермана над $\mathbb{Z}[\theta]$. Для $\alpha_0, \alpha_1, \ldots, \alpha_n \in \mathbb{Z}[\theta]$ ми визначаємо

$$K_n(\alpha_0, \alpha_1, \ldots, \alpha_n\,;\gamma) = \sum_{S(C)} e^{\pi i Sp\left(\frac{\alpha_0 x_0 + \ldots + \alpha_n x_n}{\gamma}\right)}.$$

де

$$S(C) : \{x_i \in \mathbf{G}^*(\gamma),\ i = 0,1,\ldots,n;\ x_0 x_1 \ldots x_n \equiv 1 \pmod{\gamma} | G = \mathbb{Z}[\theta]\}.$$

Ми вивчаємо тільки суми $K_n(\alpha_0, \ldots, \alpha_n\,;\mathfrak{p}^m)$, де $\mathfrak{p}$ – просте в $\mathbb{Z}[\theta]$, $m \geqslant 1$ – натуральне.

ТЕОРЕМА. *Нехай $m = 1$. Тоді справедливі співвідношення*

a) $K_n(\alpha_0, \ldots, \alpha_n\,;\mathfrak{p}) = (N(\mathfrak{p})-1)^n$, *якщо* $(\alpha_0, \alpha_1, \ldots, \alpha_n, \mathfrak{p}) = \mathfrak{p}$;

b) $K_n(\alpha_0, \ldots, \alpha_n\,;\mathfrak{p}) = (-1)^l (N(\mathfrak{p})-1)^{n-l}$, *якщо* $(\alpha_0, \alpha_1, \ldots, \alpha_n, \mathfrak{p}) = 1$ *і серед* α_i *є точно* l, $1 \leqslant l < n$, *взаємно простих з* $\mathfrak{p}$;

c) $|K_n(\alpha_0, \ldots, \alpha_n\,;\mathfrak{p})| \leqslant (n+1)(N(\mathfrak{p})^{\frac{n}{2}}$, *якщо* $(\alpha_i, \mathfrak{p}) = 1,\ i = 0,1,\ldots,n$.

ТЕОРЕМА. *Нехай* $(\alpha_0, \alpha_1, \ldots, \alpha_n, \mathfrak{p}^m) = 1,\ m \geqslant 2$. *Тоді*

$$|K_n(\alpha_0, \ldots, \alpha_n; \mathfrak{p}^m)| \leqslant \begin{cases} 0, & \text{якщо } \alpha_0\alpha_1\ldots\alpha_n \equiv 0 \pmod{\mathfrak{p}}; \\ nN(\mathfrak{p}^m), & \text{якщо } (\alpha_0, \ldots, \alpha_n, \mathfrak{p}) = 1 \\ & i\ \mathfrak{p} \neq 1+i, 3; \\ 2^{m+1}n, & \text{якщо } (\alpha_0, \ldots, \alpha_n, \mathfrak{p}) = 1\ i\ \mathfrak{p} = 1+i; \\ 3^{2m+1}n, & \text{якщо } (\alpha_0, \ldots, \alpha_n, \mathfrak{p}) = 1\ i\ \mathfrak{p} = 3. \end{cases}$$

Для цілих гаусових $\alpha_0, \alpha_1, \ldots, \alpha_N$ позначимо N-мірну нормену суму Клостермана для $(h,q) = 1$ як:

$$\widetilde{K}_N(\alpha_0, \alpha_1, \ldots, \alpha_N\,;q,h) := \sum_{S(C)} e_q\left(\mathrm{Re}(\alpha_0 x_0 + \ldots + \alpha_N x_N)\right),$$

где

$$S(C) : \{x_i \in \mathbb{Z}_q,\ i = 0, 1, \ldots, N;\ N(x_0 x_1 \ldots x_N) \equiv h \pmod q\}.$$

Аналогічним чином визначається нормена сума Клостермана над кільцем $\mathbb{Z}[\theta]$ цілих елементів уявного квадратичного розширення поля $\mathbb{Q}$.

ТЕОРЕМА. *Нехай h - залишкова норма по модулю p. Тоді*

$$\widetilde{K}_N(\alpha_0, \alpha_1, \ldots, \alpha_N; p^m, h) \leqslant 2(4N-1)p^{2N(m-n)} I(\alpha_1, \ldots, \alpha_N; p^m),$$

де $I(\alpha_1, \ldots, \alpha_N; p^m)$ - число розв'язків системи конгруенцій

$$\begin{cases} a_j - 2D^2 N(\eta_j)' x_j \equiv 0 \pmod{p^{m-n}}, \\ b_j + 2D^2 N(\eta_j)' y_j \equiv 0 \pmod{p^{m-n}}, \end{cases}$$

окрім того $I(\alpha_1, \ldots, \alpha_N; p^m) \leqslant (4N-1)p^{N(2n-m)}$, якщо $m_{\alpha_1} = \ldots = m_{\alpha_N} = 0$. (Тут $n = \left[\frac{m+1}{2}\right]$, $[x]$ позначає найбільше ціле $\leqslant x$).

В **третьому підрозділі** першого розділу вивчаються тригонометричні суми Клостерманівського типу на підгрупах групи G_{p^m}. Нехай p - просте раціональне число, яке нерозкладне в $\mathbb{Z}[\theta]$. Позначимо через E_m і U_m наступні підгрупи в G_{p^m}:

$$E_m := \{x \in G_{p^m} |\ N(x) \equiv \pm 1 \pmod{p^m}\},$$

$$U_m := \{x \in G_{p^m} |\ x \equiv 1 \pmod p\}.$$

Підгрупи E_m і U_m будемо називати нормеою групою в G_{p^m} і групою головних одиниць, відповідно.

ТЕОРЕМА. *Нехай $f(x) \in G_{p^m}[x]$ і нехай k - степінь $f(x)$, $(k, p) = 1$. Припустимо, що $f'(x)$ має єдиний корінь в G_p^* і $f'(1) + f''(1) \not\equiv 0 \pmod p$. Тоді справедлива наступна оцінка*

$$\left| \sum_{x \in E_m} e^{2\pi i \frac{\operatorname{Re} f(x)}{p^m}} \right| \leqslant (k+1)p^{\frac{m}{2}}.$$

Розглянемо тригонометричну суму

$$K_{E_m}(1, \alpha) := \sum_{\substack{x, y \in E_m \\ xy \equiv 1 \pmod{p^m}}} e^{2\pi i \operatorname{Re}\left(\frac{x + \alpha y}{p^m}\right)}.$$

Сума K_{E_m} зветься сумою Клостермана, асоційованою з норменою групою E_m.

ТЕОРЕМА. *Нехай $\alpha = a + b\sqrt{-d} \in G$, і нехай p - нерозкладне ціле. Тоді*

$$|K_{E_m}(1,\alpha)| \leqslant \begin{cases} 2p^{\frac{m}{2}}, & \nu_p(НСД(1+a,b)) = 0, \\ 0, & \nu_p(НСД(1+a,b)) = 1, \\ 2p^{\frac{m+1}{2}}, & \nu_p(НСД(1+a,b)) > 1. \end{cases}$$

Розглянемо твістову тригонометричну суму над групою головних одиниць U_m

$$S(\chi, f) = \sum_{x \in U_m} \chi(x) e^{2\pi i \operatorname{Re}\left(\frac{f(x)}{p^m}\right)}.$$

ТЕОРЕМА. *Нехай χ_Λ - нетривіальний характер по модулю p^m над G і $F(x) \in G[x]$, де $F'(1) \not\equiv -2F''(1) \pmod p$. Тоді ми маємо*

$$\left| \sum_{x \in U_m} \chi_\Lambda(x) e^{2\pi i \operatorname{Re}\left(\frac{F(x)}{p^m}\right)} \right| \leqslant \begin{cases} N(p)^{\frac{m}{2}}, & \text{якщо } F'(1) + \Lambda \equiv 0 \pmod p, \\ 0 & \text{інакше.} \end{cases}$$

(тут Λ - параметер, що визначається характером χ_Λ).

Перший підрозділ **другого розділу** дисертації присвячений дослідженню псевдовипадкових чисел, які породжені конгруентними генераторами виду:

$$y_{n+1} \equiv f(y_n, \ldots, y_{n-s}) \pmod{p^n},$$

де $y_0, y_1, \ldots, y_s$ - ініціальні значення конгруентної рекурсії, а f - раціональна функція від s змінних з коефіцієнтами із $\mathbb{Z}_{p^m}$. Ми досліджуємо лише випадки $s = 1$ і $s = 2$.

ОЗНАЧЕННЯ. *Послідовність дійсних чисел, породжена конгруентною рекурсією*

$$y_{n+1} \equiv f(y_n) \pmod M, \ 0 \leqslant y_i \leqslant M, \ i = 0, 1, \ldots,$$

називається псевдовипадковою, якщо послідовність $\left\{\frac{y_n}{M}\right\}$

(i) *рівномірно розподілена на $[0, 1)$;*

(ii) *"статистично незалежна";*

(iii) *має великий період;*

(iv) *допускає просту апаратну реалізацію.*

Ейченауер і Лехн з одного боку і Нідерайтер з другого вивчали рекурентний генератор виду:

$$y_{n+1} \equiv ay_n^{-1} + b \pmod{p^m}$$

який називається інверсним конгруентним генератором, де y_n^{-1} є мультиплікативним оберненим до y_n. Ми узагальнили інверсний генератор і в дисертації вивчаємо інверсний генератор зі змінним зсувом:

$$b(n) = b + c \cdot \Phi(n),$$

де $\Phi(n) = n$ або $\Phi(n) = n + F(n)$, де $F(n)$ - поліном з цілими коефіцієнтами високої степені і кількістю ненульових членів 3 або 4. Наше дослідження узагальненого інверсного генератору полягає в тому, що елементи послідовності y_n можна представити у вигляді поліномів від номеру елемента.

Ще одне узагальнення інверсного генератора має вигляд:

$$y_{n+1} \equiv ay_n^{-1} + b + cy_n (mod\ p^m),$$

крім того, $(a, p) = (y_0, p) = 1$, $b \equiv c \equiv 0 (mod\ p)$. Це так званий лінійно-інверсний конгруентний генератор. Нами для непарного p було знайдено зображення для $k \geqslant 2m + 1$:

$$y_{2k} = kb + kacy_0^{-1} + (1 - k(k-1)a^{-1}b^2)y_0 + (-ka^{-1}b)y_0^2 + \\ + (-ka^{-1}c + k^2a^{-2}b^2)y_0^3 + p^\alpha F_0(k, y_0, y_0^{-1}),$$

$$y_{2k+1} = (k+1)b + (a - k(k+1)b^2)y_0^{-1} + (-kab)y_0^{-2} + \\ + (-ka^2c + k^2ab^2)y_0^{-3} + (k+1)cy_0 + p^\alpha G_0(k, y_0, y_0^{-1}),$$

де $\alpha := \min(\nu_p(b^3), \nu_p(bc))$;

$F_0(u, v, w)$, $G_0(u, v, w) \in \mathbb{Z}[u, v, w]$, $F_0(0, v, w) = G_0(0, v, w) = 0$.

В роботі також досліджується інверсний конгруентний генератор другого порядку, визначений рекурсією

$$y_{n+1} \equiv a(y_{n-1}y_n)^{-1} + b \pmod{p^m},$$

де $(a, p) = 1$, $b \equiv 0 \pmod{p}$, $(y_0, p) = (y_1, p) = 1$. Були знайдені зображення елементів відповідної послідовності.

ПРОПОЗИЦІЯ. *Нехай послідовність* $\{y_n\}$ *породжена попередньою рекурсією з* $(a,p) = (y_0,p) = (y_1,p) = 1$, $\nu_p(b) = \nu_0 > 0$. *Існують поліноми* $F_{-1}(x), F_0(x), F_1(x) \in \mathbb{Z}[x]$ *з коефіцієнтами, залежними від* y_0, y_1, *такі, що*

$$\begin{aligned} y_{3k-1} = {} & y_0^{-1}y_1^{-1}((a + b(-6a^{-1}y_0y_1) + b^2B_0(y_0,y_1))+ \\ & + kb(1 - 2ay_1^{-1} + bB_1(y_0,y_1))+ \\ & + k^2b^2(y_0 - \frac{7}{2}ay_1^{-1} + bB_2(y_0,y_1))) + p^{3\nu_0}F_{-1}(k) \end{aligned}$$

$$\begin{aligned} y_{3k} = {} & (2y_0 + b^2C_0(y_0,y_1)) + kb(1 + bC_1(y_0,y_1))+ \\ & + k^2b^2(-\frac{1}{2}a^{-1}y_0y_1 - 2a^{-1}y_0^2) + p^{3\nu_0}F_0(k) \end{aligned}$$

$$\begin{aligned} y_{3k+1} = {} & 2^{-1}y_0^{-1}(a + 2by_0 + 3b^2y_0(1 - ba^{-1}y_1)) + kb(y_0y_1 - 2^{-1}ay_0^{-1})+ \\ & + k^2b^2(y_0 + 2^{-1}ay_0^{-2} - (2^{-1})^2y_0^{-1} - 2^{-1}y_1^{-1}) + p^{3\nu_0}F_1(k). \end{aligned}$$

Після опису введених узагальнених інверсних конгруентних генераторів, який надається в першому підрозділі другого розділу, в цьому ж підрозділі ми розглядаємо тригонометричні суми на псевдовипадкових числах, породжених введеними інверсними генераторами. Для послідовностей, породжених змінним поліноміальним зсувом з періодом τ, маємо:

ТЕОРЕМА. *Справедливі наступні оцінки*

$$|\sigma_{k,\ell}|(h_1,h_2) \leqslant \begin{cases} 2^{\left[\frac{m+1}{2}\right]}p^{\frac{m}{2}}, & \text{якщо } k \not\equiv \ell \,(mod\ 2) \\ 2p^{\frac{m+s}{2}}, & \text{якщо } k \equiv \ell \,(mod\ 2), \\ & НСД(h_1+h_2, h_1k_1 + h_2\ell_1, p^m) = p^s, \\ & s < m, \\ \varphi(m), & \text{якщо } k \equiv \ell \,(mod\ 2), \\ & НСД(h_1+h_2, h_1k_1 + h_2\ell_1, p^m) = p^s, \\ & s \geqslant m, \end{cases}$$

де $k = 2k_1$, $\ell = 2\ell_1$ *або* $k = 2k_1 + 1$, $\ell = 2\ell_1 + 1$.

Для послідовностей, породжених лінійно-інверсним генератором по модулю p^m, $p \geqslant 3$, мають місце твердження:

ТЕОРЕМА. *Нехай лінійно-інверсна конгруентна послідовність, породжена попередньою рекурсією, має період τ, і нехай $\nu_p(b) = \nu$, $\nu_p(a - y_0^2) = \nu_0$, $2\nu \leqslant m$. Тоді справедливі наступні оцінки*

$$|S_\tau(h, y_0)| \leqslant \begin{cases} O(m), & \text{якщо } p > 2 \text{ і } \nu_0 < \nu,\ \nu_p(h) < m - \nu - \nu_0 \\ & \text{або } p = 2,\ \nu_0 < \nu,\ \nu_2(h) < m - 2\nu; \\ 4 \cdot p^{\frac{m+\nu_p(h)}{2}}, & \text{якщо } \nu_0 \geqslant \nu,\ \nu_p(h) < m - 2\nu; \\ \tau & \text{інакше.} \end{cases}$$

Для середнього значення $S_N(h, y_0)$ по всім $y_0 \in \mathbb{Z}_{p^m}^*$ маємо:

ТЕОРЕМА. *Нехай a, b, c - параметри лінійно-інверсного конгруентного генератора і нехай $(a, p) = 1$, $0 < \nu = \nu_p(b) < \nu_p(c)$, $1 \leqslant N \leqslant 2p^{m-1}$, $\nu_p(h) = p^s$, $s < m$. Тоді середнє значення $S_N(h, y_0)$ над $y_0 \in \mathbb{Z}_{p^m}^*$ задовольняє*

$$\overline{S}_N(h) := \frac{1}{\varphi(p^m)} \sum_{y_0 \in \mathbb{Z}_{p^m}^*} |S_N(h, y_0)| \leqslant N^{\frac{1}{2}} p^{-\frac{m}{4}} \left(2(\varepsilon_p(a))^{\frac{m}{4}} + \sqrt{10} p^{\frac{\nu+s}{4}} \right),$$

де $s = \nu_p((h, p^m))$, $h = h_0 p^s$,

$$\varepsilon_p(a) = \begin{cases} 1, & \text{якщо} \quad p = 2 \\ 1 + \left(\frac{-a}{p}\right), & \text{якщо} \quad p > 2,\ \left(\frac{-a}{p}\right) \text{ - символ Лежандра.} \end{cases}$$

Для лінійно-інверсного генератора по модулю 2^m:

ТЕОРЕМА. *Нехай $(h_1, h_2, 2) = 1$, $\nu_2(h_1 + h_2) = \beta$, $\nu_2(h_1 k + h_2 \ell) = \gamma$. Справедливі наступні оцінки*

$$|\sigma_{k,\ell}(h_1, h_2; M)| \leqslant \begin{cases} 2^{\frac{m+2}{2}}, & \text{якщо} \quad k \not\equiv \ell (mod\ 2); \\ 0, & \text{якщо} \quad k \equiv \ell (mod\ 2) \\ & \text{і} \quad \beta < \gamma + \nu,\ m - \beta - \nu > 0; \\ 2^{m-1}, & \text{якщо} \quad k \equiv \ell (mod\ 2) \\ & \text{і} \quad \beta \geqslant \gamma + \nu,\ m - \nu - \gamma \leqslant 0; \\ 2^{\frac{m+\nu+\gamma+2}{2}}, & \text{якщо} \quad k \equiv \ell (mod\ 2) \\ & \text{і} \quad \beta \geqslant \gamma + \nu,\ m - \nu - \gamma > 0. \end{cases}$$

Аналогічним чином розглядаються тригонометричні суми $\sigma_{k,\ell}$ і $S_N(y_0, y_1)$ на випадок послідовності ПВЧ, породженої інверсним генератором другого порядку.

Отримані оцінки тригонометричних сум на послідовностях, згенерованих дослідженими нами інверсними генераторами, за допомогою нерівності Турана-Ердьоша-Коксми дозволяють оцінити дескріпансії породжених послідовностей, а отже оцінити якісність на рівномірність і непередбачуваність цих послідовностей.

Із послідовності одномірних точок $\{x_n\}$, $n = 0, 1, \ldots$, породжених інверсними генераторами, утворимо послідовність s-мірних точок $X_n^{(s)}$, де

$$X_n^{(s)} = (x_n, x_{n+1}, \ldots, x_{n+s-1}), \;\; n = 0, 1, \ldots.$$

ОЗНАЧЕННЯ. *Говорять, що послідовність ПВЧ* $\{x_n\}$ *проходить серіальний тест на псевдовипадковість, якщо дескріпансія* $D_N^{(s)}$ *послідовності* s*-мірних точок* $X_n^{(s)}$ *прямує до* 0 *при* $N \to \infty$ *для* $s = 1, 2, \ldots$.

Для розглянутих інверсних генераторів в роботі доведені нижні та верхні оцінки дескріпантної функції $D_N^{(s)}$. Зокрема, для лінійно-інверсного генератора зі змінним зсувом

$$y_{n+1} \equiv a\overline{y}_n + b + cF(n+1)y_0 (mod\ p^m), \;\; \nu_p(b) = \nu$$

в теоремі 2.24 ми отримали оцінку:

$$D_\tau^{(3)} \leqslant \frac{\sqrt{p}}{\sqrt{p}-1} p^{-\frac{m}{2}+\nu} \left(\frac{1}{\pi} \log p^{m-\nu} + \frac{3}{5} \right)^3 + \frac{3}{2} p^{-m+\nu}.$$

звідки видно, що для $\nu < \frac{m}{2}$ $D_\tau^{(3)} \to 0$ при $p^m \to \infty$.

В **другому підрозділі** другого розділу досліджується конгруентний генератор, пов'язаний з цілими точками на еліпсі $x^2 + dy^2 \equiv 1 \pmod{p^m}$, де d - натуральне число, а p - нерозкладне просте число уявного квадратичного поля $\mathbb{Q}(\sqrt{-d})$. В розділі 1 дано опис групи E_m кільця цілих елементів $\mathbb{Z}[\theta]$. Якщо $u_0 + \theta v_0$ - породжуючий елемент групи E_m, то ми позначаємо по модулю p^m:

$$Z_t(k) = Z_t = \mathrm{Re}\left((u_0 + \theta v_0)^{2(p+1)t+2k} \right),$$
$$W_t(k) = W_t = \mathrm{Im}\left((u_0 + \theta v_0)^{2(p+1)t+2k} \right).$$

В прийнятих позначеннях доведена теорема:

ТЕОРЕМА. *Нехай* $a, b \in \mathbb{Z}_{p^m}$, $(a, b, p) = 1$. *Тоді для тригонометричної суми*

$$S(a, b; p^m) = \sum_{t \in \mathbb{Z}_{p^{m-1}}} e_{p^m}(aZ_t + bW_t)$$

ми маємо наступну оцінку

$$|S(a, b; p^m)| \leqslant 2p^{\frac{m}{2}}.$$

Для кожного $k \in \{0, 1, \ldots, p\}$ і цілих a, b таких, що $(a, b, p) = 1$ позначимо

$$aZ_t(k) + bW_t(k) = x_t(a, b; k) := x(t).$$

Послідовність $x(t)$ будемо називати циркулярною послідовністю псевдовипадкових чисел.

ТЕОРЕМА. *Послідовність* $\left\{\frac{x(t)}{p^m}\right\}$ *рівнорозподілена на відрізку* $[0, 1)$.

Інверсні генератори, які досліджуються в роботі, можуть бути узагальнені на випадок послідовностей псевдовипадкових чисел одиничного кола. Для цього нами доведена теорема:

ТЕОРЕМА (Аналог нерівності Турана-Ердьоша-Коксми). *Нехай* $M > 1$ *- ціле раціональне,* G_M *- кільце цілих гаусових чисел по модулю* M. *Тоді для кожної послідовності* $\{z_n\}$, $z_n \in G_M$, *дескрипансія точок* $\left\{\frac{z_n}{M}\right\}$ *задовольняє нерівності*

$$D_N \leqslant 2\left(1 - \left(1 - \frac{2\pi}{M}\right)^2\right) + \\ + \frac{1}{M} \sum_{\substack{\gamma \in G_M \\ \gamma \neq 0}} \min\left(\frac{1}{|\sin \pi \operatorname{Re} \gamma|}, \frac{1}{|\sin \pi \operatorname{Im} \gamma|}\right) \frac{1}{N}\left(|S_N| + O\left(N^{\frac{1}{2}}\right)\right),$$

де $S_N = \sum_{n=0}^{N-1} e_M(\operatorname{Re}(\gamma y_n))$.

За допомогою цього аналогу в роботі доведено, що послідовність $z_0(u + iv)^m$, де $u + iv$ - породжуючий елемент групи E_n, є рівномірно розподіленою і непередбачуваною в одиничному колі комплексної

площини. В **останньому підрозділі** другого розділу вивчаються послідовності ПВЧ, які породжені еліптичною кривою над $\mathbb{Z}_{p^m}$. Доведена теорема:

ТЕОРЕМА. *Нехай $p > 3$ - просте число, $m > 3$ - натуральне; (x_0, y_0) - деякий розв'язок конгруенції $y^2 \equiv x^3 + ax + b \pmod p$, де $-3a$ квадратичний нелишок і $(y_0, p) = 1$. Тоді існують два многочлени $y_i(t)$, $i = 1, 2$ над кільцем $\mathbb{Z}_{p^m}$ такі, що для $(A, p) = 1$ і кожного розв'язку $y_i(t)$, $i = 1, 2$ конгруенції $y^2 \equiv x^3 + ax + b \pmod{p^m}$, справедлива оцінка тригонометричної суми*

$$\sum_{t=0}^{p^m-1} e_m(Ay_i(t)) = O\left(p^{\frac{m}{2}}\right)$$

з абсолютною сталою в символі "O".

ОЗНАЧЕННЯ. *Нехай (x_0, y_0) - розв'язок конгруенції $y^2 \equiv x^3 + ax + b \pmod{p^m}$ і нехай $y_i(t)$ - многочлени з попередньої теореми. Послідовність $\left\{\frac{y_i(t)}{p^m}\right\}$, $t = 0, 1, \ldots, p^{m-1} - 1$ називається послідовністю псевдовипадкових чисел, асоційованою з еліптичною кривою.*

З Теореми 2.38 випливає, що тригонометрична сума $\sum\limits_{t=0}^{N-1} e^{2\pi i \frac{hy_i(t)}{p^m}}$, $h \not\equiv 0 \pmod{p^m}$ має оцінку

$$\sum_{t=0}^{N-1} e^{2\pi i \frac{hy_i(t)}{p^m}} = O(p^{\frac{m-\mu}{2}} \log p^m),$$

де $\mu = \nu_p(h)$. Це означає, що послідовність псевдовипадкових чисел, асоційованих з еліптичною кривою, проходить тест на псевдовипадковість.

Третій розділ дисертації містить шість підрозділів, в яких вивчається питання розподілу значень арифметичних функцій над кільцями $\mathbb{Z}$ і $\mathbb{G}$. В **першому підрозділі** третього розділу побудована асимптотична формула для функції дільників $\tau_3(\omega)$ над кільцем цілих гаусових чисел з нормами в арифметичній прогресії. Основним результатом цього підрозділу є наступна теорема:

ТЕОРЕМА. *Нехай ℓ, q - позитивні цілі, $1 \leqslant \ell < q$, $(\ell, q) = 1$. Тоді для $x \to \infty$ ми маємо*

$$\sum_{\substack{N(\omega)\equiv\ell \pmod q \\ N(\omega)\leqslant x}} \tau_3(\omega) = \frac{x}{q^2}\mathfrak{I}(\ell,q)\prod_{\mathfrak{p}|q}\left(1-\frac{1}{N(\mathfrak{p})}\right)^2 P_2(\log x)+$$

$$+\frac{x}{q^2}\mathfrak{I}(\ell,q)\prod_{\mathfrak{p}|q}\left(1-\frac{1}{N(\mathfrak{p})}\right)P_1(\log x)+\frac{12x}{q^2}\mathfrak{I}(q,\ell)+O\left(x^{\frac{5}{7}+\varepsilon}\right),$$

де $\mathfrak{I}(q,\ell)$ - кількість розв'язків конгруенції $x^2+dy^2 \equiv \ell \pmod q$ і $P_j(u)$ - поліноми степені j з обчислювальними коефіцієнтами, крім того ці коефіцієнти і стала в залишковому члені не залежать від x, ℓ, q.

В **другому підрозділі** третього розділу ми досліджуємо функцію дільників $\tau(\omega)$, яка зважена сумою Клостермана $K(1,\omega;\gamma)$. Оскільки $K(1,\omega;\gamma)$ приймає тільки дійсні значення, то цікаво розглядати функцію $\tau(\omega)$, зважену функцією $K(1,\omega;\gamma)$, подібно тому, як вивчається функція дільників, зважена тригонометричною одиницею $e^{2\pi i \operatorname{Re}\frac{\omega}{\gamma}}$. В цьому підрозділі доведена наступна теорема

ТЕОРЕМА. *Нехай $\gamma = \gamma_1\gamma_2$, $(\gamma_1,\gamma_2) = 1$, γ_1 - безквадратна, γ_2 - квадратно-повна частини γ. Тоді для $(\alpha,\gamma) = 1$ справедлива асимптотична формула для $x \to \infty$:*

$$\sum_{N(\omega)\leqslant x}\tau(\alpha)K(1,\alpha\omega;\gamma) = A(x,\gamma)+O\left(x^{\frac{1}{3}}N(\gamma)^{\frac{1}{2}}\tau^3(\gamma)\log^2 x\right),$$

де

$$A(x,\gamma)=\begin{cases}0, & \text{якщо} \quad \gamma_2>1,\\ \frac{\pi\varphi(\gamma)}{4N(\gamma)}\sum\limits_{\mathfrak{p}|\gamma}\frac{\log N(\mathfrak{p})}{N(\mathfrak{p})-1}+\frac{\varphi(\gamma)}{4N(\gamma)}\left[\frac{\pi}{4}E+L'(1,\chi_4)\right], & \text{якщо} \quad \gamma_2=1.\end{cases}$$

Наступний **підрозділ 3.3** присвячено розподілу норм цілих гаусових чисел в арифметичній прогресії і вузьких секторах. Нехай функція

$$r_m(n) = \sum_{\substack{u,v\in\mathbb{Z}\\ u^2+v^2=n}} e^{4mi\arg(u+iv)}.$$

при $m = 0$ означає кількість зображень натурального числа n сумою двох квадратів. Позначимо через $A(x; \varphi_1, \varphi_2; a, p^\ell)$ число точок (u, v) в кругу $(u^2 + v^2) \leqslant x$ за умов

$$u, v \in \mathbb{Z},\ \varphi_1 < \arg(u + iv) \leqslant \varphi_2,\ u^2 + v^2 \equiv a \pmod{p^\ell},\ (a, p^\ell) = 1.$$

ТЕОРЕМА. *Для $x \to \infty$ справедлива наступна оцінка*

$$\sum_{\substack{n \equiv a \pmod{p^\ell} \\ n \leqslant x}} r_m(n) = \varepsilon \frac{\pi x}{p^\ell} k_0 \left(1 - \frac{\chi_4(p)}{p}\right) + O\left(\frac{x^{\frac{1}{2}+\varepsilon}}{p^{\frac{\ell}{4}}} M^{1+\varepsilon}\right) + \\ + O\left(p^{\frac{\ell}{2}} M^{1+\varepsilon}\right),$$

де $\varepsilon_m = 0$, якщо $m \neq 0$, $\varepsilon_0 = 1$, $k_0 = 1$, якщо $p > 2$, або $k_0 = 2$, якщо $p = 2$, $\ell \geqslant 3$; $M = |m| + 3$, $\varepsilon > 0$ довільне мале число; сталі в символах можуть залежати лише від ε.

Наступні теореми випливають із цього результату і Леми Віноградова.

ТЕОРЕМА. *В секторіальній області $u^2 + v^2 \leqslant x$, $u^2 + v^2 \equiv a \pmod{p^\ell}$, $\varphi_1 < \arg(u + iv) \leqslant \varphi_2$, $\varphi_2 - \varphi_1 \gg x$ справедлива наступна асимптотична формула*

$$A(x; \varphi_1, \varphi_2; a, p^\ell) := \sum_{\substack{u,v \\ u^2+v^2 \equiv a \pmod{p^\ell} \\ \varphi_1 < \arg(u+iv) \leqslant \varphi_2 \\ u^2+v^2 \leqslant x}} 1 = \\ = \frac{\varphi_2 - \varphi_1}{2} \cdot \frac{k_0 x}{p^\ell} \left(1 - \frac{\chi_4(p)}{p}\right) + O\left(\frac{x^{\frac{1}{2}+\varepsilon}}{p^{\frac{\ell}{4}}}\right).$$

ТЕОРЕМА. *Нехай p - просте число, $\ell \geqslant 3$, і $p^{\frac{3\ell}{2-4\kappa}} \leqslant x \leqslant p^{2\ell}$, $0 < \kappa \leqslant \frac{1}{8} - \frac{1}{4\ell}$, $\varphi_2 - \varphi_1 \gg x^{-\kappa}$. Тоді ми маємо*

$$A(x; \varphi_1, \varphi_2; a, p^\ell) = \frac{\varphi_2 - \varphi_1}{2} \cdot \frac{x}{p^\ell} \left(1 - \frac{\chi_4(p)}{p}\right) + O\left(\frac{x^{1-\kappa}}{p^\ell} \log x^\kappa\right).$$

В **підрозділі 3.4** розглянута проблема еліпса на арифметичній прогресії як аналог проблеми кола і доведені теореми:

ТЕОРЕМА. *Для* $D^{\frac{3}{2}} \leqslant x < D^2$, *справедлива асимптотична формула*

$$A(x,D) = \frac{\pi x}{\sqrt{d}D}\gamma_0 \prod_{p|D}\left(1-\left(\frac{d}{p}\right)\cdot\frac{1}{p}\right)+$$
$$+O\left(D^{\frac{1}{2}}\tau(D)\exp\left(c\frac{(\ln D)^{\frac{1}{2}}}{\ln\ln D}\right)\right)+O\left(\frac{x^{\frac{1}{2}}}{D^{\frac{1}{4}}}\tau(D)\right),$$

де $\gamma_0 = 1$, *якщо*

$$\gamma_0 = \begin{cases} 1, & \text{якщо} \quad D \not\equiv 0 \pmod 4, \\ 2, & \text{якщо} \quad D \equiv 0 \pmod 4, \end{cases}$$

і $\tau(D)$ *- число дільників* $D \in \mathbb{N}$.

ТЕОРЕМА. *Для* $0 < \varphi_2 - \varphi_1 \leqslant \frac{\pi}{2}$ *справедливі наступні асимптотичні формули*

$$A(x;\varphi_1;\varphi_2;D) = \frac{(\varphi_2-\varphi_1)x}{2\sqrt{d}D}\gamma_0 \prod_{p|D}\left(1-\left(\frac{d}{p}\right)\cdot\frac{1}{p}\right)+$$
$$+O\left(D^{\frac{1}{2}}\tau(D)\exp\left(c\frac{(\ln D)^{\frac{1}{2}}}{\ln\ln D}\right)\right)+O\left(\frac{x^{\frac{1}{2}}}{D^{\frac{1}{4}}}\tau(D)\right)$$

зі сталими в символах "O*", які залежать від* d *і* $\varepsilon > 0$.

В **підрозділі 3.5** побудована асимптотична формула для кількості зображень натуральних чисел сумою значень позитивних бінарних квадратичних форм. Нехай $u_1,\ldots,u_n$, $v_1,\ldots,v_n$– фіксований набір векторів із $\mathbb{Q}^2$. Для $\lambda \in \mathbb{Q}$ і $\overline{u},\overline{v} \in \mathbb{Q}^{2n}$ покладаємо

$$\mathrm{V}_{n,k}(\lambda;\overline{u},\overline{v}) = \sum_{(C)} e^{2\pi i\overline{u}\cdot\overline{v}},$$

де $C = \{w_j \in \mathbb{Z}^2,\ j = 1,\ldots,n \mid \sum_{j=1}^{n}\left(Q(w_j+v_j)\right)^k = \lambda\}$.
Розглянемо функцію, задану рядом

$$Z_{n,k}(s;\overline{u},\overline{v}) = \sum_{\lambda>0}\frac{\mathrm{V}_{n,k}(\lambda;\overline{u},\overline{v})}{\lambda^s}, \qquad (\mathrm{Re}\, s > 1).$$

В роботі ми показали, що в критичній смузі $\frac{1}{2} \leqslant \operatorname{Re} s \leqslant 1$ функція $Z_{n,k}(s;\overline{u},\overline{v})$ має степеневий зріст, а тому ми отримали асимптотичну формулу для суматорної функції

$$\mathrm{W}(\lambda;\overline{u},\overline{v}) = \sum_{\lambda \leqslant x} \mathrm{V}_{n,k}(\lambda;\overline{u},\overline{v})$$

і довели наступну теорему:

ТЕОРЕМА. *Для довільного набору $\overline{v} \in \mathbb{Q}^{2n}$ справедлива оцінка*

$$\sum_{\lambda \leqslant x} \mathrm{V}_{n,k}(\lambda;\overline{0},\overline{v}) = \sum_{\frac{n}{2} < l \leqslant n} c_k(l) x^{\frac{l}{n}} + O(x^{\frac{3}{4}} \log^3 x)$$

з обчислювальними сталими $c_k(l)$, причому

$$c_k(n) = \left(\Gamma\left((\pi)^{-\frac{1}{k}} \frac{1}{k}\right)\right)^r \frac{2k^2}{n(n+k)}; \quad r = \sum_{\substack{j=1 \\ u_j \in \mathbb{Z}^2}}^{n} 1.$$

Як видно із теореми доцільно вважати, що $\frac{k}{2} < n \leqslant k$, тому що для $n \leqslant \frac{k}{2}$ ми не можемо виділити головний член асимптотики.

В останньому підрозділі третього розділу досліджується перетворення Лапласа для пари Z-функцій Гекке зі зсувом. Нехай

$$F_m(s;\delta,\gamma) = \sum_{\substack{\delta_1,\delta_2 \in \mathbb{Z}[i] \\ \delta_1\delta_2 \equiv q \mod \gamma}} Z_m\left(s;\frac{\delta_1}{\gamma},0\right) Z_m\left(\overline{s};0,\frac{\delta_2}{\gamma}\right).$$

є сумою добутків двох функцій Гекке зі зсувом і нехай

$$L_{F_m}(s;\delta,\gamma) = \int_0^\infty F_m(x;\delta,\gamma)\mathrm{e}^{-sx}\mathrm{d}x, \quad s = \sigma + it \in \mathbb{C}$$

ТЕОРЕМА. *Нехай δ і γ гаусові цілі, $(\delta,\gamma) = 1$. Тоді*

$$L_{F_m}(s;\delta,\gamma) = \lambda_0(s,\delta,m) +$$
$$+4\pi^3 \mathrm{e}^{i\frac{\pi-s}{2}} \left[\pi \prod_{\mathfrak{p}|\gamma} \left(1 - \tfrac{1}{N(\mathfrak{p})}\right)^{-1} \left(\log N(\mathfrak{p}) + \tfrac{\varphi(\gamma)}{\pi} b_0(\gamma)\right) - \tfrac{i(\pi-s)}{2}\right],$$

де

$$b_0(\gamma) = \pi \prod_{\mathfrak{p}|\gamma} \left(1 - \frac{1}{N(\mathfrak{p})}\right)^{-1} \left(E + \frac{L'(1,\chi_4)}{L(1,\chi_4)} + \sum_{\mathfrak{p}|\gamma} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p}-1)}\right),$$

E - стала Ойлера, $L(s,\chi_4)$ L-функція Діріхле з нетривіальним характером mod4. *Крім того, функція $\lambda_0(s,\delta,m)$ є аналітичною для $|\sigma| < \frac{\pi}{2}$, а оцінка*
$|\lambda_0(s,\delta,m)| \ll (1+|s|)^{-1}$ *справедлива для $|\sigma| \leqslant \theta$, $0 < \theta < \frac{\pi}{2}$.*

ВИСНОВКИ

Дисертаційна робота присвячена застосуванням методу тригонометричних сух в проблемах генерування послідовностей псевдовипадкових чисел, які задовольняють умовам їх рівномірного розподілу на відрізку $[0,1)$, і розв'язанню проблем побудови асимптотичних формул суматорних функцій, асоційованих з мультиплікативними функціями цілих раціональних або цілих гаусових чисел. Інтерес до цих проблем пов'язано з використанням псевдовипадкових чисел в задачах моделювання реальних процесів, а також для деяких мультиплікативних функцій над кільцем уявного квадратичного розширення поля раціональних чисел. Умовно результати дисертаційної роботи можна розділити на три частини: (i) будуються оцінки повних та твістових сум над кільцем чисел поля $\mathbb{Q}(\sqrt{-d})$; (ii) застосовуються тригонометричні суми спецального вигляду для оцінки якісності послідовностей псевдовипадкових чисел, породжуваних інверсними конгруентними генераторами; (iii) методом тригонометричних сум будуються асимптотичні формули для суматорних функцій, пов'язаних з мультиплікативними функціями над кільцями цілих раціональних і цілих гаусових чисел.

В першій частині роботи розглядаються нормені суми Клостермана над кільцем цілих чисел поля $\mathbb{Q}(\sqrt{-d})$ та деякі узагальнення таких тригонометричних сум.

Другий розділ дисертації містить спеціальні конгруенції, які породжують послідовності псевдовипадкових чисел. Проводяться дослідження дискрінантної функції цих послідовностей, за допомогою яких виявляється якісність послідовностей ПВЧ.

В третьому розділі вивчається: (i) функція дільників $\tau_3(\omega)$ в арифметичній прогресії; (ii) норми гаусових цілих чисел в арифметичній прогресії і вузьких секторах; (iii) перетворення Лапласа для пари Z-функцій Геке; (iv) зображення натуральних чисел квадратичними формами; (v) проблема еліпса на арифметичній прогресії.

Основними науковими результатами дисертації є такі:

— оцінки повних і змішених тригонометричних сум над кільцем цілих гаусових чисел;
— нові оцінки сум Клостермана n-го порядку над кільцем цілих гаусових чисел;
— оцінки узагальнених сум Клостермана над кільцем цілих гаусових чисел;
— нормені суми Клостермана n-го порядку;
— нові оцінки дискріпантної функції інверсного генератора зі змінним зсувом;
— побудовані інверсні генератори другого порядку і знайдені оцінки відповідних дискріпантних функцій;
— побудовано сімейство циркулярних генераторів, доведена псевдовипадковість породжуваних ними послідовностей псевдовипадкових чисел;
— досліджено на псевдовипадковість послідовність, породжена лінійно-інверсним генератором;
— побудовано асимптотична формула в проблемі еліпса на арифметичній прогресії;
— досліджена асимптотична поведінки суматорної функції для функції дільників, зваженої тригонометричними одиницями;
— знайдена асимптотична формула для суматорної функції, асоційованої з кількістю зображень натуральних чисел k-тими степенями квадратичної форми;
— досліджені аналітичні властивості перетворення Лапласа для пари Z-функцій Геке з зсувом.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Варбанец С.П., Савастру О.В., Многомерные суммы Клостермана над $\mathbb{Z}[i]$, *Вісник ОНУ, Сер. "Математика і механіка"*,

15(2010), вип. 18, С.38–45.

2. Varbanets P., Varbanets S., On inversive congruential generator with a variable shift for pseudorandom numbers with prime power modulus, *Annales Univ. Sci. Budapest., Sect. Comp.*, **32**(2010), P.151–176.
3. Varbanets S., Savastru O., Norm Kloosterman sums over $\mathbb{Z}[i]$, *Algebra and Discrete Mathematics*, **11**(2011), no. 2, P.82–91.
4. Varbanets P., Varbanets S., Linear-inversive congruential generator of PRN's, *Proceedings of* 4^{th} *Chaotic Modeling and Simulation International Conference, 31 May – 3 June 2011, Agios Nikolaos, Crete Greece*, 2011, P.617-624.
5. Varbanets S.P., Savastru O.V., Представление натуральных чисел квадратичными формами, *Вісник ОНУ, Сер. "Математика і механіка"*, **17**(2012), Вип. 1-2(13-14), С.43–53.
6. Варбанец П.Д., Варбанец С.П., Инверсный конгруэнтный генератор с переменным здвигом, *Ученые записки Орловского Ун-та, Научный журнал*, **6**(2012), часть 2, С.266–272.
7. Varbanets P.D., Varbanets S.P., Inversive congruential generator with a variable shift, *Proceedings of* 5^{th} *Chaotic Modeling and Simulation International Conference, 12 – 15 June 2012, Athens Greece*, 2012, P.605-612.
8. Varbanets P., Varbanets S., Generalizations of Inversive Congruential Generator, *Analytic and Probabilistic Methods in Number Theory, Proceedings of the Fifth International Conference in Honour of J. Kubilius, Palanga, Lithuania, 4-10 Septembre 2011*, 2012, P.265-282.
9. Varbanets S., Linear-inversive PRN's generator with power of two modulus, *Вісник ОНУ, Сер. "Математика і механіка"*, **18**(2013), Вип. 1(17), С.94–103.
10. Radova A.S., Varbanets S.P., Divisor function $\tau_3(\omega)$ in arithmetic progression, *Annales Univ. Sci. Budapest., Sect. Comp.*, **41**(2013), P.261–279.
11. Varbanets P.D., Varbanets S.P., Inversive congruential generator with a variable shift, *Chaotic Modeling and Simulation (CMSIM)*, **1**(2013), P.231–238.
12. Varbanets P., Varbanets S., Twisted exponential sums and the distribution of solutions of the congruence $f(x, y) \equiv 0 \pmod{p^m}$

over $\mathbb{Z}[i]$, *Annales Univ. Sci. Budapest., Sect. Comp.*, **41**(2013), P.95–103.

13. Varbanets P., Varbanets S., Generalized twisted exponential sum, *Siauliai Math. Semin.*, **8**(2013), no. 16, P.267–279.
14. Rudetski V., Tran The Vinh, Varbanets P., Varbanets S., Linear-inversive congruential pseudo-random numbers with prime power modulus, *Proceedings,* 6^{th} *Chaotic Modeling and Simulation International Conference 11-14 June 2013, Yeditepe University, Istanbul, Turkey*, 2013, P.575-581.
15. Rudetski V., Tran The Vinh, Varbanets P., Varbanets S., Analogue of Turan-Erdös-Koksma inequality for a discrepancy of complex PRN's, *Proceedings,* 6^{th} *Chaotic Modeling and Simulation International Conference 11-14 June 2013, Istanbul, Turkey*, 2013, P.567-573.
16. Varbanets S., Sequences of PRN's produced by circular generator, *Вісник ОНУ, Сер. "Математика і механіка"*, **19**(2014), Вип. 1(21), С.71–80.
17. Varbanets S., Generalized twisted Kloosterman sum over $\mathbb{Z}[i]$, *Ukr. Math. Journal.*, **66**(2014), no. 5, P.609–618.
18. Varbanets P., Varbanets S., Exponential sums over norm groups, *Siauliai Math. Semin.*, **9**(2014), no. 17, P.83–92.
19. Varbanets P., Varbanets S., Circular generator of PRN's, 7^{th} *CHAOS Conference Proceedings, 7-10 June 2014, Lisbon Portugal*, 2014, P. 523-532.
20. Varbanets S., Vorobyov Ya., The Laplace transform for a pair of the Hecke Z-functions, *Siauliai Math. Semin.*, **10**(2015), no. 18, P.103–112.
21. Varbanets P., Varbanets S., Twisted exponential sums over the ring of Gaussian integers, *Siauliai Math. Semin.*, **10**(2015), no. 18, P.213–223.
22. Varabnets S., Circular generator of PRN's, *Researches in Mathematics and Mechanics*, **21**(2016), Is. 1(27), P.100–108.
23. Varbanets S., Inversive generator of the second order for the sequence of PRN's, *Chaotic Modeling and Simulation (CMSIM)*, **3**(2016), P.267–279.
24. Varbanets S., Inversive generator of the second order for the sequence of PRN's, 8^{th} *CHAOS Conference Proceedings, 26-29*

May 2015, Henri Poicare Institute, Paris, France, 2016, P. 877-889.

25. Radova A., Varbanets S., On exponential sums involving the divisor function over $\mathbb{Z}[i]$, *Annales Univ. Sci. Budapest., Sect. Comp.*, **46**(2017), P.235–246.
26. Varbanets S., Sequences of PRN's produced by circular generator, *Chaotic Modeling and Simulation (CMSIM)*, **2**(2017), P.159-168.
27. Varbanets S., Varbanets S., Inversive generator of the second order with a variable shift for the sequence of PRN's, *Annales Univ. Sci. Budapest., Sect. Comp.*, **46**(2017), P.255–273.
28. Varbanets S., Exponential sums over the sequences of PRN' s produced by inversive generators, *Annales Univ. Sci. Budapest., Sect. Comp.*, **48**(2018), P. 225-232.
29. Varbanets S., The sequences of PRN's produced by inversive generators of qth order, *Proceedings of* 3^{rd} *International Conference on Computer Algebra and Information Technologies,Odessa, Ukraine, 20-25 August 2018*, 2018, P.175-177.
30. Varbanets P., Sergey Varbanets S., Problem of ellipse in arithmetic progression, *VoronoÏ's Impact on Modern Science, Proceedings of The Sixth International Conference on Analytic Number Theory and Spatial Tessellations, Kyiv, Ukraine September 24-28, 2018*, **6**(2018), Volume 1, P.124-137.
31. Varbanets S., Vorobyov Ya., Norm of Gaussian integers in arithmetical progressions and narrow sectors, *Algebra and Discrete Mathematics*, **29**(2020), Is. 2, P.259–270.
32. Varbanets S., Vorobyov Ya., Inversive generators of second order, 13^{th} *CHAOS Conference Proceedings, 9-12 June 2020, Florence, Italy*, 2020, P.1073-1086.

АНОТАЦІЯ

Варбанець С. П. **Метод тригонометричних сум в теорії конгруентних генераторів псевдовипадкових чисел та асимптотичних задачах теорії чисел** — Рукопис.

Дисертація на здобуття наукового ступеня доктора фізико-математичних наук за спеціальністю 01.01.08 — математична логіка, дис-

кретна математика і теорія алгоритмів. — Київський національний університет імені Тараса Шевченка, Київ, 2021.

Побудовані нові нетривіальні оцінки повних чистих або твістових сум з многочленом в показнику над кільцем цілих елементів уявного квадратичного розширення поля раціональних чисел. Досліджені спеціальні тригонометричні суми Клостерманівського типу над кільцем цілих чисел уявного квадратичного розширення поля раціональних чисел. Побудовані інверсні конгруентні генератори за модулем степені простого раціонального числа p, наведені узагальнення інверсного конгруентного генератора. Побудовано новий тип генераторів, для яких рекурсія генерування основана на властивостях елементів так званої норменої групи, яка є підгрупою мультиплікативної групи класів лишків кільця $\mathbb{Z}[i]$ за модулем p^m, де p - просте раціональне число, яке не розпадається в полі $\mathbb{Q}(\sqrt{-d})$, $d > 0$. Розглядаються оцінки тригонометричних суми на послідовностях ПВЧ, через які оцінюється дескріпантна функція послідовностей ПВЧ. Отримані оцінки дескріпансії узагальнених послідовностей ПВЧ, породжених інверсними генераторами, покращують результати Нідерайтера і Шпарлінського. Побудовані асимптотичні формули суматорних функцій для спеціальних арифметичних функцій над кільцями цілих раціональних або цілих чисел уявного квадратичного розширення поля раціональних чисел. Також отримані оцінки залишкових членів для суматорних функцій, пов'язаних з розподлілом значень $\tau_3(\alpha)$. Побудована асимптотична формула для кількості цілих гаусових чисел у вузькому секторі кола радіусу $x^{\frac{1}{2}}$, норми яких належать арифметичній прогресії, різниця якої росте з зростанням і не перевищує $x^{\frac{2}{3}}$, а розмір кутового сектору прямує до нуля. Подібні оцінки були отримані нами в проблемі еліпсу на арифметичній прогресії. Знайдено аналітичний вираз перетворення Лапласа добутку пар Z-функцій Геке $Z_m\left(s; \frac{\delta_1}{\gamma}, 0\right) Z_m\left(\overline{s}; 0, \frac{\delta_2}{\gamma}\right)$. Досліджена проблема зображення натуральних чисел квадратичними формами від n змінних, яка узагальнює проблему Варинга. Побудована нова асимптотична формула для кількості точок всередині еліпса на арифметичній прогресії.

Ключові слова: тригонометричні суми, сума Клостермана, псевдовипадкові числа, дискріпансія, асимптотична формула, функція діль-

ників.

АННОТАЦИЯ

Варбанец С. П. **Метод тригонометрических сумм в теории конгруэнтных генераторов псевдослучайных чисел и асимптотических задачах теории чисел** — Рукопись.

Диссертация на соискание ученой степени доктора физико-математических наук по специальности 01.01.08 — математическая логика, дискретная математика и теория алгоритмов. — Киевский национальный университет имени Тараса Шевченка, Киев, 2021.

Построены новые нетривиальные оценки полных чистых или твистовых сумм с многочленом в показателе над кольцом целых элементов мнимого квадратичного расширения поля рациональных чисел. Исследовались специальные тригонометрические суммы Клостермановского типа над кольцом целых чисел мнимого квадратичного расширения поля рациональных чисел. Построены инверсные конгруэнтные генераторы по модулю степени простого рационального числа p, приведены обобщения инверсного конгруэнтного генератора. Построен новый тип генераторов, для которых рекурсия генерирования основана на свойствах элементов так называемой норменной группы, которая является подгруппой мультипликативной группы классов вычетов кольца $\mathbb{Z}[\theta]$ по модулю p^m, где p - простое рациональное число, которое не разлагается в поле $\mathbb{Q}(\sqrt{-d})$, $d > 0$. Рассматриваются оценки тригонометрических сумм на последовательностях псевдослучайных чисел, которые важны для получения нетривиальных оценок дескрипансии последовательностей ПСЧ. Полученные нами оценки дескрипансии обобщённых последовательностей ПСЧ, порождённых инверсными генераторами, улучшают результаты Нидерайтера и Шпарлинского. Построены асимптотические формулы суматорных функций для специальных арифметических функций над кольцами целых рациональных или целых чисел мнимого квадратичного расширения поля рациональных чисел. Также получены оценки остаточных членов для суматорных функций, связанных с распределением значений $\tau_3(\alpha)$. Построена асимптотическая формула для числа целых гаусових чисел в узком секторе

круга радиусом $x^{\frac{1}{2}}$, нормы которых принадлежат арифметической прогрессии, разность которой растёт с ростом и не превышает $x^{\frac{2}{3}}$, а раствор углового сектора стремится к нулю. Оценки, подобные результату о нетривиальности оценки Z-функции Гекке со сдвигом, были нами получены в проблеме эллипса на арифметической прогрессии. Для эллипса $u^2 + dv^2 \equiv 1 \pmod{D}$, d-безквадратное целое, $(d, D) = 1$ построена асимптотическая формула о числе натуральных чисел вида $n = u^2 + dv^2$ в арифметической прогрессии $n \equiv 1 \pmod{D}$ при условии, что $x \to \infty$. Найдено аналитическое выражение для преобразования Лапласа произведения пар Z-функций Гекке $Z_m\left(s; \frac{\delta_1}{\gamma}, 0\right) Z_m\left(\overline{s}; 0, \frac{\delta_2}{\gamma}\right)$. Исследована проблема представления натуральных чисел квадратичными формами от n переменных, которая обобщает проблему Варинга. Построена новая асимптотическая формула для числа точек внутри эллипса на арифметической прогрессии.

Ключевые слова: тригонометрические суммы, сумма Клостермана, псевдо-случайные числа, дискрепансия, асимптотическая формула, функция делителей.

ABSTRACT

Varbanets S. P. **Method on exponential sums in theory of congruential generators of the pseudorandom numbers and asymptotic problems in number theory.** — Manuscript.

Thesis for the doctor of mathematical and physical sciences degree in speciality 01.01.08 — mathematical logic, discrete mathematics and theory of algorithms. — Taras Shevchenko National University of Kyiv, Kyiv, 2021.

This thesis is devoted to investigation the generating problems of the sequences of pseudorandom numbers using a competitive recursion of the prime power modulus, as well as the problems of analytical number theory that arise with constructing the asymptotic formulas for summatory functions associated with the distribution of divisor functions τ_k, $k = 2, 3$ over the rings of rational integers or Gaussian integers. We introduced the construction of new non-trivial estimates of purely com-

pleted or twisted exponential sums with a polynomial in the exponent over the ring of Gaussian integers. In addition, there are investigated the special exponential sums of Klosterman type over the ring of integers of an imaginary quadratic expansion of the field of rational numbers. The studied norm Klosterman sums have no analogue in the rational case, and their estimates are used to obtain the estimates of an error terms in problems of analytic number theory such as the problem of circle (or ellipse) in arithmetic progression and in the coding theory with Klosterman code problems etc. The obtained estimates of the norm Klosterman sums are related to the results of P. Deligne and E. Bombieri on the Riemann hypothesis for algebraic varieties. R. Evans, G. Perelmuter, S. Stepanov, R. Dabrovsky, V. Fischer, H. Ivanets and others were engaged in the development of methods for estimating of such sums. The significance of the obtained results on estimates of completed exponential sums is that the asymptotic formulas for estimates of the distribution of arithmetic functions on arithmetic progressions are based on such estimates. The second part of thesis is devoted to construction the inversive congruential generators modulo the power of prime rational number p. We gave the generalizations of the inversive congruential generator. We also investigated the inversive congruential generator of second order. Here also we constructed a new type of generators for which the relative recursion is based on the properties of elements from so-called the norm group, which is a subgroup of the multiplicative group of residue classes of the ring $\mathbb{Z}[\theta]$ modulo the p^m. We used the constructed exponential sums to obtain the non-trivial estimates for discrepancy function of sequences of PRN's. The obtained estimates of discrepant function improve the results of Niederreiter and Shparlinskii. The last part of thesis was being devoted to the problems of analytical number theory. We constructed the asymptotic formulas of summatory functions for special arithmetic functions over the ring of rational numbers and the ring of integers of imaginary quadratic extension of the field of rational numbers. The obtained results are testified the uniform distribution of the values of these arithmetic functions on the segments of natural numbers or narrow sectors on the complex plane. We investigated the distribution of values of divisor function $\tau_3(\alpha)$ with norm in arithmetic progression. Here we also constructed an asymptotic formula for the number of Gaussian integers in a narrow sector of a circle of radius $x^{\frac{1}{2}}$, the norms of which belong

to an arithmetic progression which difference increases with increasing x and does not exceed $x^{\frac{2}{3}}$, and the size of the corner sector goes to zero. We obtained a similar result in the problem of an ellipse on an arithmetic progression. In this work there are investigated the problem of representing the natural numbers by the values of positively defined quadratic of the power of k. And finally in the last part of thesis we find the analytical expression for the Laplace transform of the product of pairs of Hecke Z-functions $Z_m\left(s; \frac{\delta_1}{\gamma}, 0\right) Z_m\left(\overline{s}; 0, \frac{\delta_2}{\gamma}\right)$.

Key words: exponential sums, Kloosterman sum, pseudo-random numbers, discrepancy, asymptotic formula, divisor function.