Варбанець Сергій Павлович, доцент кафедри комп&rsquo;ютерної алгебри та дискретної математики, Одеський національний університету імені І. І. Мечникова. Назва дисертації: &laquo;Метод тригонометричних сум в теорії конгруентних генераторів псевдовипадкових чисел та асимптотичних задачах теорії чисел&raquo;. Шифр та назва спеціальності 01.01.08 математична логіка, дискретна математика і теорія алгоритмів. Спецрада Д 26.001.18 Київського національного університету імені Тараса Шевченка

Мiнiстерство освiти i науки Укрiїни

Київський нацiональний унiверситет iменi Тараса Шевченка

Квалiфiкацiйна наукова праця

на правах рукопису

Варбанець Сергiй Павлович

УДК 511.33, 519.2

ДИСЕРТАЦIЯ

Метод тригонометричних сум в теорiї

конгруентних генераторiв

псевдовипадкових чисел та асимптотичних

задачах теорiї чисел

01.01.08 - математична логiка, теорiя алгоритмiв i дискретна математика

Подається на здобуття наукового ступеня

доктора фiзико-математичних наук

Дисертацiя мiстить результати власних дослiджень. Використання iдей,

результатiв i текстiв iнших авторiв мають посилання на вiдповiдне джерело

С.П. Варбанець

Науковий консультант

Кореновський Анатолiй Олександрович

доктор фiзико-математичних наук, професор

Київ - 2021

ЗМIСТ

Вступ 16

Роздiл 1. Тригонометричнi суми над кiльцем цiлих чисел уявного

квадратичного поля 28

1.1. Повнi тригонометричнi суми над G . . . . . . . . . . . . . . . . . . 33

1.1.1. Чиста сума . . . . . . . . . . . . . . . . . . . . . . . . . . . . 35

1.1.2. Твiстовi суми Клостермана на G . . . . . . . . . . . . . . . . 42

1.2. Тригонометричнi суми спецiального виду . . . . . . . . . . . . . . . 46

1.2.1. Узагальненi суми Клостермана над кiльцем цiлих елементiв

уявного квадратичного розширення поля Q(

√

−d) . . . . . . 46

1.2.2. Багатовимiрнi (кратнi) суми Клостермана над Z[θ] . . . . . . 74

1.2.3. Багатовимiрнi норменi суми Клостермана над Z[θ] . . . . . . 81

1.3. Твiстовi тригонометричнi суми Клостерманiвського типу . . . . . . 91

Висновки до роздiлу 1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 99

Роздiл 2. Генерування послiдовностей псевдовипадкових чисел 101

2.1. Iнверснi конгруентнi генератори зi змiнним зсувом . . . . . . . . . . 107

2.1.1. Зображення елементiв послiдовностi {yn} у виглядi многочленiв вiд номера елемента i iнiцiального значення y0. . . . . 107

2.1.2. Тригонометричнi суми на псевдовипадкових числах, породжених iнверсними генераторами. . . . . . . . . . . . . . . . 123

2.1.3. Рiвнорозподiленiсть i непередбачуванiсть послiдовностей ПВЧ,

породжених iнверсними конгруентними генераторами. . . . . 158

2.2. Циркулярнi генератори . . . . . . . . . . . . . . . . . . . . . . . . . 171

2.3. Рiвномiрний розподiл комплексних чисел по модулю p

m в одиничному колi . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 176

15

2.4. Послiдовностi ПВЧ, породженi елiптичною кривою над кiльцем Zpm 183

Висновки до роздiлу 2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 190

Роздiл 3. Асимптотичнi формули над кiльцем цiлих елементiв уявного квадратичного поля 192

3.1. Функцiя дiльникiв τ3(ω) в арифметичнiй прогресiї . . . . . . . . . . 192

3.2. Функцiя дiльникiв, зважена сумою Клостермана . . . . . . . . . . . 207

3.3. Норми гаусових цiлих чисел в арифметичнiй прогресiї i вузьких секторах . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 215

3.4. Проблема елiпса на арифметичнiй прогресiї . . . . . . . . . . . . . . 226

3.5. Зображення натуральних чисел квадратичними формами . . . . . . 238

3.6. Перетворення Лапласа для пари Z-функцiй Гекке . . . . . . . . . . 249

Висновки до роздiлу 3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 258

Висновки 259

Список використаних джерел 261

Додаток 278

ВИСНОВКИ

Дисертацйнароботаприсвяченазастосуваннямметодутригонометричнихсух

впроблемахгенеруванняпослдовностейпсевдовипадковихчиселякзадовольняютьумовамїхрвномрногорозподлунавдрзкурозв’язаннюпроблем

побудовиасимптотичнихформулсуматорнихфункцйасоцйованихзмультиплкативнимифункцямицлихрацональнихабоцлихгаусовихчиселнтерес

доцихпроблемпов’язанозвикористаннямпсевдовипадковихчиселвзадачах

моделюванняреальнихпроцесватакождлядеякихмультиплкативнихфункцйнадкльцемуявногоквадратичногорозширенняполярацональнихчисел

Умовнорезультатидисертацйноїроботиможнароздлитинатричастинибудуютьсяоцнкиповнихтатвстовихсумнадкльцемчиселполя

√

−

застосовуютьсятригонометричнсумиспецальноговиглядудляоцнкияксност

послдовностейпсевдовипадковихчиселпороджуванихнверснимиконгруентнимигенераторамиметодомтригонометричнихсумбудуютьсяасимптотичн

формулидлясуматорнихфункцйпов’язанихзмультиплкативнимифункцями

надкльцямицлихрацональнихцлихгаусовихчисел

ВпершйчастинроботирозглядаютьсянорменсумиКлостермананадкльцемцлихчиселполя

√

−тадеякузагальненнятакихтригонометричних

сум

ДругийроздлдисертацїмститьспецальнконгруенцїякпороджуютьпослдовностпсевдовипадковихчиселПроводятьсядослдженнядискрпантноїфункцїцихпослдовностейзадопомогоюякихвиявляєтьсяякснстьпослдовностей

ПВЧ

Втретьомуроздлвивчаєтьсяфункцядльниквτωварифметичнй

прогресїнормигаусовихцлихчиселварифметичнйпрогресївузькихсекторахперетворенняЛапласадляпарифункцйГекезображення



натуральнихчиселквадратичнимиформамипроблемаелпсанаарифметичнйпрогресї

Основниминауковимирезультатамидисертацїєтак

—оцнкиповнихзмшенихтригонометричнихсумнадкльцемцлихгаусовихчисел

—новоцнкисумКлостерманагопорядкунадкльцемцлихгаусових

чисел

—оцнкиузагальненихсумКлостермананадкльцемцлихгаусовихчисел

—норменсумиКлостерманагопорядку

—новоцнкидискрпантноїфункцїнверсногогенератораззмннимзсувом

—побудованнверснгенераторидругогопорядкузнайденоцнкивдповднихдискрпантнихфункцй

—побудованосмействоциркулярнихгенераторвдоведенапсевдовипадковстьпороджуванихнимипослдовностейпсевдовипадковихчисел

—дослдженонапсевдовипадковстьпослдовнстьпородженалнйнонверснимгенератором

—побудованоасимптотичнаформулавпроблемелпсанаарифметичнй

прогресї

—дослдженаасимптотичнаповеднкисуматорноїфункцїдляфункцїдльниквзваженоїтригонометричнимиодиницями

—знайденаасимптотичнаформуладлясуматорноїфункцїасоцйованоїз

клькстюзображеньнатуральнихчиселтимистепенямиквадратичної

форми

—дослдженаналтичнвластивостперетворенняЛапласадляпарифункцйГекеззсувом