ВІДГУК
офіційного опонента про дисертацію Поповича Романа Богдановича "Елементи великого мультиплікативного порядку в скінченних полях" подану на здобуття наукового ступеня доктора фізико-математичних наук за спеціальністю 01.01.06 – алгебра та теорія чисел

Дисертаційна робота Р.Б. Поповича присвячена вирішенню проблеми побудови в явному вигляді елементів великого мультиплікативного порядку в скінченних полях на основі циклотомічних поліномів, на основі поліномів Куммера, на основі поліномів Артіна-Шраєра, рекурсивного типу та загального вигляду, на базі розвитку відомих та розробки нових методів.

Оманлива простота постановки проблем (обманчивая простота постановки проблем) знаходження примітивного елементу скінченного поля, та знаходження найменшого примітивного елементу скінченного поля споріднює ці проблеми з іншими класичними проблемами теорії чисел. Дослідженню цих проблем приділяли увагу класики математики, зокрема К. Гаусс, П. Ферма, Л. Діріхле, Е. Ландау, І.М. Віноградов, інші вчені. Важливою проблемою, яка пов'язана з вищенаведеними, є проблема знаходження елементів скінченного поля, які мають великий мультиплікативний порядок. Для вирішення поставленої проблеми дисертант розглядає задачі, які і самі викликають підвищений інтерес у науковців як з точки зору теорії скінченних полів, так і з прикладної точки зору. Можливими областями застосування елементів великого порядку в скінченних полях є теорія кодування та криптологія, зокрема: завадостійке кодування, генератори псевдовипадкових чисел, доведення простоти великих цілих чисел. Сама проблема і відповідні їй задачі вимагають розробки адекватних ефективних методів дослідження, за допомогою яких можна отримати елементи великого порядку та межі для цих порядків у явному та зручному для використання вигляді. З урахуванням вищенаведеного це дозволяє зробити висновок, що тема дисертації відноситься до сфери пріоритетних напрямків розвитку науки в Україні, а тематика дисертаційного дослідження Р.Б. Поповича є актуальною як з теоретичної, так із практичної точок зору.

Базуючись на методах і результатах елементарної теорії чисел, теорії скінченних полів, комбінаторики з теорією розбиттів, комп'ютерної алгебри і відповідних обчислень дисертант здійснив коректні постановки задач, пов'язаних з побудовою і дослідженням елементів великого мультиплікативного порядку в скінченних полях, обрав та реалізував обґрунтовані методи їх розв'язання. Дослідження відповідних елементів обґрунтовується доведеними математичними твердженнями та посиланнями на апробовані результати. Таким чином, результати дисертаційної роботи слід вважати науково обґрунтованими і такими, що мають теоретичне значення.

Результати дисертаційних досліджень є складовою частиною науково-дослідної теми 0115U000446 «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» ДК/КІБЕР, яка ведеться на кафедрі спеціалізованих комп'ютерних систем Інституту комп'ютерних технологій НУ «Львівська політехніка». Результати дисертаційних досліджень можуть бути використані при явній побудові відповідних елементів в скінченних полях, стати математичною основою розробок в галузі інформаційних технологій.

Основні результати дисертації отримані автором самостійно та опубліковані в 20 наукових працях без співавторів у провідних закордонних та українських наукових фахових виданнях, затверджених МОН України, серед них 6 у виданнях, включених до міжнародних наукометричних баз даних Web of Science і/або Scopus, додатково висвітлені в 2 статтях у збірниках наукових праць та в 10 матеріалах міжнародних наукових конференцій. Усі статті опубліковані дисертантом одноосібно. Результати дисертації апробовані на багатьох наукових конференціях і семінарах, у тому числі міжнародних. Положення і висновки представленої дисертації Р.Б. Поповича не містять положень і висновків із його кандидатської дисертації.

Достовірність отриманих результатів і висновків, сформульованих в дисертаційній роботі, забезпечується та підтверджується використанням апробованого математичного апарату та коректним доведенням тверджень.

У вступі обґрунтовано актуальність тематики, сформульовано мету та завдання дослідження, вказано наукову новизну отриманих результатів, їх наукове і практичне значення та апробацію. У першому розділі детально висвітлено історію дослідження задач, пов'язаних із темою дисертаційної роботи, та наведено приклади застосувань елементів великого мультиплікативного порядку у криптографічному захисті інформації. У другому розділі наведено необхідні для подальшого викладу відомі результати; описано, які задачі вирішуються в дисертаційній роботі та які підходи для цього використано. У третьому розділі досліджено явну побудову елементів великого порядку в розширеннях скінченних полів, які пов'язані з поняттям гауссового періоду. У першому підрозділі підсилено та узагальнено результат з праці О. Ахмаді, І. Шпарлінскі та Ж. Волоха на елементи більш загального вигляду, ніж гауссовий період. Це дає відповідь на відкрите питання, поставлене цими авторами. Доведено теорему 3.1. яка дає нижню межу для порядків певних елементів скінченого поля. Всі нижні межі в теоремі 3.1 використовують поняття розбиття, де кожна частина з'являється не більше, ніж p-1 разів. У другому підрозділі отримано, використовуючи відомі результати з теорії розбиттів, явні нижні межі для мультиплікативних порядків елементів у термінах p – характеристика поля, та r – степінь розширення. В третьому підрозділі наведено низку числових прикладів для отриманих у двох попередніх підрозділах результатів. Четвертий підрозділ присвячено модифікації нижніх меж для мультиплікативних порядків елементів. Це зроблено на основі оптимізації та підрахунку кількості розв'язків лінійної діофантової нерівності замість підрахунку кількості розбиттів. У п'ятому підрозділі підсилено відомі асимптотичні нижні межі для порядків елементів. У четвертому розділі розглянуто нижні межі для порядку елементів у розширеннях на основі поліномів Куммера. В першому підрозділі виписано умови, при яких такі розширення існують. У другому підрозділі розглянуто частковий випадок, коли виконується умова: m ділить $q-1$. В теоремі 4.3 отримано нижню межу, яка є точною величиною, на відміну від відомої

наближеної межі. У третьому підрозділі знято цю умову для будь-якого m. Показано в лемі 4.6, що $m = m_1 m_2$, де m_1 є дільником $q-1$, а m_2 є порядком q за модулем m. Явно збудовано елементи порядку принаймні $2^{\lfloor \sqrt[3]{2m} \rfloor}$. Ідея полягає в наступному: якщо $q-1$ має великий дільник m_1, то слід використати метод як для розширень Куммера; в іншому разі m_2 є великим, і слід використати метод як для циклотомічних розширень. У четвертому підрозділі підсилено нижню межу з використанням максимуму функції кількості розв'язків діофантового рівняння, а в п'ятому – з використанням оцінки знизу для кількості розбиттів. У п'ятому розділі розглянуто побудову елементів великого порядку в розширеннях Артіна-Шраєра. У першому підрозділі в теоремі 5.1 явно збудовано елементи великого порядку. У другому підрозділі розглянуто з використанням комп'ютерних обчислень явну побудову деяких примітивних елементів. У третьому підрозділі виведено нижню межу для добутку біноміальних коефіцієнтів, пов'язаному з тестуванням простоти або побудовою елементів великого порядку в розширеннях Куммера та Артіна-Шраєра. У шостому розділі отримано нижню межу для порядку деяких елементів у рекурсивних розширеннях скінченних полів характеристики два, визначених Конвеєм та Відеманом, а також у рекурсивних розширеннях полів характеристики більшої від двох. У першому підрозділі в наслідку 6.2 наведено нижню межу для порядку деяких елементів у розширеннях, визначених Конвеєм. В другому підрозділі описано деякі примітивні елементи для перших дванадцяти полів у вежах Конвея. Також сформульовано в наслідку 6.3 умову, при якій розглянуті в першому підрозділі елементи є примітивними. У третьому підрозділі одержано в теоремі 6.9 нижню межу для порядку деяких елементів у розширеннях, визначених Відеманом. Четвертий та п'ятий підрозділи присвячено отриманню нижніх границь для порядку елементів у вежах скінченних полів характеристики більшої, ніж два. У сьомому розділі в першому підрозділі розглянуто побудову елементів великого порядку в загальних скінченних полях на основі гіпотези Гао. У другому підрозділі побудовано елементи великого порядку в цих полях без використання гіпотези

Гао. Для отримання нижніх меж застосовано наслідок із ABC теореми Стовера–Мейсона для поліномів. У третьому підрозділі вивчено зв'язок між елементами великого порядку та доведенням простоти великих натуральних чисел. У роботі для отримання деяких результатів використано комп'ютерно-алгебраїчні обчислення (теорема 5.2, теорема 6.6, теорема 6.9). Автореферат дисертації за своїм змістом відповідає основним положенням дисертаційної роботи, дає змогу зрозуміти основний зміст роботи, в ньому не міститься відомостей, що відсутні у дисертації.

Дисертаційна робота загалом написана чітко й послідовно, але як і кожна велика робота, містить окремі недоліки: зустрічаються деякі описки (стр. 53), граматичні некоректності (стр. 55, ст. 7 знизу); бажано також посилатися на узагальнену гіпотезу Рімана (GRH) тому що GRH відноситься до L-функцій, за допомогою яких виводяться оцінки множин, які містять примітивні елементи поля;

Втім ці зауваження не впливають на загальну позитивну оцінку роботи. В дисертаційній роботі розв'язана проблема побудови в явному вигляді елементів великого мультиплікативного порядку в скінченних полях. Дисертаційна робота Поповича Р.Б. виконана на високому теоретичному рівні і являє собою завершену кваліфікаційну наукову працю. Тема дисертації та постановка задач дослідження відповідають паспорту спеціальності 01.01.06 – алгебра та теорія чисел. Вважаю, що дисертаційна робота Поповича Романа Богдановича є завершеною науковою працею, задовольняє всім вимогам «Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника» (постанова Кабінету Міністрів України №567 від 24.07.2013 року), які висуваються до докторських дисертацій, а її автор заслуговує на присудження наукового ступеня доктора фізико-математичних наук за спеціальністю 01.01.06 – алгебра та теорія чисел.

Офіційний опонент,
професор кафедри електроніки
Національного авіаційного університету,
доктор фіз.-мат. наук, с.н.с. Глазунов М.М.

Особистий підпис Глазунова М.М.
ЗАСВІДЧУЮ
Заст. начальника відділу управління персоналом
Національного авіаційного університету

21.09.2016 р.

Надійшов до спеціалізованої вченої ради Д 26.206.03 21.03.2016 р.
секретар ради