Відгук
офіційного опонента про дисертаційну роботу Поповича Романа Богдановича
“Елементи великого мультиплікативного порядку в скінченних полях”,
яка подана на здобуття на здобуття наукового ступеня
доктора фізико-математичних наук
за спеціальністю 01.01.06 – алгебра та теорія чисел

Дисертаційна робота присвячена питанню явної побудови елементів великого мультиплікативного порядку та примітивних елементів для скінченних полів різного вигляду. Області застосування як примітивних елементів, так і елементів великого порядку в скінченних полях такі: криптографія (зокрема, протокол Діффі-Хелмана, криптосистема Ель-Гамаля з відкритим ключем), доведення простоти великих чисел, завадостійке кодування, генератори псевдовипадкових чисел.

Дисертаційна робота складається зі вступу, семи розділів, висновків та списку використаних джерел. 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* подано спеціальні терміни, відомі поняття та означення; викладено допоміжні твердження, а також попередні відомості і факти, що стосуються теми дисертації. Проведено огляд відомих результатів, наведених у літературі. У *другому* розділі наведено необхідні для подальшого викладу відомі результати; описано, які задачі вирішуються в дисертаційній роботі та які підходи для цього використано.

Основний зміст роботи викладений у розділах із третього по сьомий.

У *третьому* розділі розглянуто явну побудову елементів великого мультиплікативного порядку в розширеннях скінченних полів, які пов’язані з поняттям гауссового періоду. Такі розширення існують для нескінченної кількості чисел, що задають степінь розширення, в припущенні виконання гіпотези Артіна. Більш точно, розглянуто побудову елементів великого порядку в скінченних полях вигляду $F_q(\theta) = F_{q^{r-1}} = F_q[x]/(x^{r-1} + \ldots + x + 1)$ (на основі циклотомічних поліномів). Покращено та узагальнено результат 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 мультиплікативних порядків певних елементів скінченого поля. Нижні межі у цій теоремі 3.1 використовують поняття розбиття числа. Прийом, який використано при отриманні результатів у теоремі 3.1, наслідку 3.1 та наслідку 3.2, полягає в заміні елемента на його автоморфний образ. Дійсно, відомо, що спряжені елементи над будь-яким підполем мають той самий мультиплікативний

порядок. Тому, при отриманні нижньої межі для порядку якогось елемента скінченого поля цей елемент можна замінити на спряжений йому. Далі вивести нижню межу для елемента-заміни.

У *четвертому розділі* збудовано елементи великого порядку спочатку для розширень Куммера, а потім для більш загального випадку розширень на основі поліномів Куммера. Розширення на основі поліномів Куммера – це розширення вигляду $F_q[x]/(x^m - a)$. У другому підрозділі розглянуто частковий випадок розширення, коли виконується умова: m ділить $q-1$. Третій підрозділ присвячено розгляду випадку, коли знято наведену умову подільності. Отримано нижню межу для порядку елементів в розширеннях на основі поліномів Куммера як результат комбінування двох різних підходів: для розширень Куммера та розширень на основі циклотомічних поліномів, описаних у третьому розділі.

У *п'ятому розділі* збудовано елементи великого порядку для розширень Артіна-Шраєра. Методика така ж, як і для розширень Куммера. Також, використовуючи комп'ютерні обчислення, виписано примітивні елементи для деяких часткових випадків розширень.

У *шостому розділі* йдеться про рекурсивні розширення скінченних полів. Отримано нижні межі для порядків для різних типів таких полів. Знову ж із використанням комп'ютерних обчислень виписано примітивні елементи для деяких часткових випадків.

У перших двох підрозділах *сьомого розділу* описано побудову елементів великого порядку в скінченних полях загального вигляду: спочатку на основі гіпотези Гао, а потім без використання цієї гіпотези.

У третьому підрозділі *сьомого розділу* йдеться про задачу, яка яскраво демонструє зв'язок між алгеброю й теорією чисел. Власне йдеться про елементарну для розуміння задачу із теорії чисел: тестування (доведення) простоти великих натуральних чисел. Широко відомий алгоритм AKS для розв'язання цієї задачі зводить її до алгебраїчної задачі побудови великої підгрупи мультиплікативної групи скінченого поля, пов'язаного з числом, яке розглядаємо. Автор досліжує низку підгруп, пов'язаних із цією задачею, та наводить нижні межі для їх порядків.

Зі сказано зрозуміло, що дисертант досяг поставленої мети та отримав нові й цікаві з наукової точки зору результати. Основні з цих результатів стосуються: підсилення нижньої межі для гауссових періодів, отримання нижньої межі для елементів у розширеннях на основі поліномів Куммера, отримання примітивних елементів для перших дванадцяти полів у вежах Конвея.

Результати дисертації Поповича Р.Б. носять характер завершеного наукового дослідження і, без сумніву, представляють інтерес для фахівців у теорії скінченних полів. Достовірність тверджень забезпечена строгими доведеннями, які з достатньою повнотою наведені в дисертації. У своїй роботі

здобувач продемонстрував належний рівень математичної культури та володіння сучасними техніками теорії скінченних полів.

Результати кандидатської дисертації не включені в докторську дисертацію.

Зміст автореферату повністю відповідає основним положенням дисертації.

Основні результати роботи достатньо повно відображені в 20 наукових статтях в провідних закордонних та українських наукових фахових виданнях, з них 6 у виданнях, що відображені в міжнародних наукометричних базах даних, і додатково висвітлені в 2 статтях у збірниках наукових праць та 10 матеріалах і тезах наукових конференцій. Автор дисертації добре апробував свої результати у виступах на конференціях і семінарах.

Дисертаційна робота оформлена згідно з вимогами до оформлення дисертацій. Викладення матеріалу чітке, логічне і послідовне, але є ряд зауважень:

1) В третьому розділі розглядається поле $\mathbb{F}_q$, де q є примітивним коренем за модулем простого r, тобто q є простим або степеню простого p. Тому тут неявним чином вважається, що таке p (або q) існує. За теоремою Лінника має місце нерівність $p \le r^c$, де c – стала, але її оцінка поки що невідома. Тому виникає проблема ефективного визначення пари (p,q), для якої результати здобувача можна використовувати.
2) Об'єм дисертаційної роботи задано великий. Його можна було б зменшити за рахунок зменшення добре відомих результатів з теорії скінчених полів та комбінаторики, а також прикладів (див. сторінки 154-156, 160-170, 243-245 тощо).
3) Деякі формулювання лем і теорем неповні, в тому сенсі, що спочатку вводяться деякі величини, а потім в теоремах або лемах вони з'являються без пояснень. Наприклад, на сторінці 238 введені величини x та y, як корені рівнянь $x^p-x-1=0$ та $y^p-y-x^{p-1}=0$ над розширенням скінченого поля $\mathbb{F}_p$, а потім на сторінці 242 вони з'являються без пояснень.
4) Зустрічаються технічні помилки (наприклад, "абсолютний член многочлена" замість "вільний член"; "$f^{(i)}(x)=f^{(i-1)}(x)$" замість "$f^{(i)}(x)=f(f^{(i-1)}(x))$"; формулювання теореми 4.5 зовсім незрозуміле; "мультиплікативний порядок підгрупи" замість "порядок підгрупи мультиплікативної групи поля")
5) Розділ 7 можна було б розділити на два розділи меншого обсягу. В одному з них дати матеріал про побудову елементів великого порядку в скінченних полях загального вигляду, а в іншому – про підгрупи мультиплікативної групи скінченого поля, пов'язані з доведенням простоти великих натуральних чисел.

Ці зауваження та деякі граматичні й стилістичні помилки, які інколи зустрічаються в тексті, не мають принципового значення і не зменшують загальної позитивної оцінки роботи.

Дисертація є завершеною науковою роботою. В ній отримано нові науково обґрунтовані результати, що в сукупності вирішують наукову проблему суттєвого значення для теорії скінченних полів. Отримані результати можуть бути використані при подальших дослідженнях властивостей елементів скінченних полів.

Вважаю, що дисертаційна робота Поповича Романа Богдановича "Елементи великого мультиплікативного порядку в скінченних полях" задовольняє вимоги "Порядку присудження наукових ступенів" щодо докторських дисертацій, а її автор заслуговує присудження йому наукового ступеня доктора фізико-математичних наук за спеціальністю 01.01.06 – алгебра та теорія чисел.

Доктор фізико-математичних наук,
завідувач кафедри комп'ютерної алгебри
та дискретної математики П.Д. Варбанець

Підпис Варбанця П.Д. підтверджую
Вчений секретар Одеського національного
університету імені І. І. Мечникова С.В. Курандо

19.09.2016р.

Надійшов до спеціалізованої вченої ради Д 26.206.03 23.03.2016р.
секретар ради /Артеменко Ж.В./

Міністерство освіти і науки України
Одеський національний університет імені І.І. Мечникова
Код в ЄДРПОУ 02071601

Інститут математики Академії наук України
Канцелярія