ВІДГУК

офіційного опонента
на дисертаційну роботу Поповича Романа Богдановича
“Елементи великого мультиплікативного порядку в скінченних полях”,
що представлена на здобуття наукового ступеня доктора фізико-математичних
наук за спеціальністю 01. 01. 06 – алгебра та теорія чисел.

Актуальність теми дисертаційної роботи та її зв’язок з науковими програмами, планами, темами

Безперечно, однією з видатних подій в історії науки є створення у 70-х роках минулого сторіччя напрямку так званої сучасної криптографії, що вивчає алгоритми з публічним ключем та методи електронного підпису, протоколи обміну ключами та пов’язані з ними алгоритми Ель Гамаля, методи розподілу секрету.

Існуюча надія на появу реально діючого квантового комп’ютера обумовила задачі перегляду існуючих зараз алгоритмів. Пітер Шор довів, що на квантовому комп’ютері розклад цілого числа на прості множники можна виконати за поліноміальний час. Це означає, що широко відомий в наш час асиметричний алгоритм RSA не можна використати в постквантову епоху. Виявилося, що й протоколи Діффі–Хелмана для обміну ключів також не мають постквантової перспективи, тому що задача відшукання дискретного логарифму для мультиплікативної групи простого скінченого поля перестає бути складною.

Це призвело до того, що криптографи, не чекаючи на появу реально діючих квантових комп’ютерів, вже розпочали побудову нових алгоритмів, для яких задача постквантового криптографічного аналізу видається важкою. Одним з основних напрямків постквантової криптографії є поліноміальна криптографія від багатьох змінних (multivariate cryptography), що базується на використанні нелінійних систем рівнянь над скінченними полями та кільцями. Після деякої кризи, пов’язаної з криптоаналітичними результатами Я. Патаріна (Франція), цей напрямок переживає новий розквіт.

У багатьох задачах, як звичайної, так і постквантової криптографії виникає проблема генерації циклічнх підгруп великого порядку, для яких задача знаходження дискретного логарифму є складною. Одними з важливих випадків є великі циклічні підгрупи мультиплікативних груп скінченого поля або ж скінчених загальних лінійних груп. Ці алгебраїчні питання розглядалися

ще Камілом Жорданом, вони призвели до виникнення широко відомих циклів Зінгера та їх аналогів для простих груп Лі над діаграмами відмінними від A_n.

Дисертація Р.Б.Поповича присвячена дослідженню мультиплікативних порядків елементів у мультиплікативних групах скінчених полів та отриманню в явному вигляді нижніх меж для цих порядків. Отримані результати можуть бути застосовані в криптографічному захисті інформації (примітиви Діффі-Хелмана та Ель-Гамаля) і завадостійкому кодуванні. Це важливий напрям в теорії скінченних полів. В той час, як стосовно існування елементів скінченних полів з різними корисними властивостями наявна досить детальна теорія, питання явної побудови таких елементів були досліджені недостатньо.

Згідно теми дисертаційної роботи, отримані автором наукові результати виконано відповідно до державних програм та планів науково дослідних робіт на кафедрі спеціалізованих комп'ютерних систем Інституту комп'ютерних технологій, автоматики та метрології Національного університету "Львівська політехніка" як частина науково-дослідної теми "Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем" ДБ / КІБЕР (номер державної реєстрації 0115U000446, 2015 – 2016 рр.).

Підсумовуючи, зазначимо, що дисертаційна робота Романа Богдановича Поповича присвячена дуже важливим питанням, пов'язаним із сучасними викликами теорії та практики захисту інформації. Його результати відносяться до класичного напрямку алгебри, теоретичні результати якого в наш час знайшли надзвичайно важливі застосування в інформатиці. У роботі розглядається також питання тестування простоти великих натуральних чисел.

Таким чином, можна вважати, що тематика дисертаційної роботи відноситься до актуальних проблем напрямку 01.01.06 – алгебра та теорія чисел.

Оцінка змісту дисертації

Дисертація складається зі вступу, семи розділів, висновків та списку використаних джерел (150 назв).

У розділі 1 автор дає огляд літератури по тематиці дисертації. У розділі 2 пояснюється суть методів, які використано в роботі та необхідні відомі факти.

Виклад результатів роботи починається з розділу 3, присвяченого розширенням скінченних полів на основі циклотомічних поліномів. А саме: розширенням вигляду $F_q[x]/(x^{r-1}+..+x+1)$, де q – степінь деякого простого числа p та q – примітивне за модулем числа r. Відомо, що ці розширення

існують для нескінченної кількості чисел r, якщо для числа q виконується гіпотеза Артіна. Для елементів більш загального вигляду, ніж гауссовий період, отримано явну експоненційну нижню межу для порядку цих елементів: кращу, ніж відома раніше для гауссового періоду. Це дало відповідь на відкрите питання, поставлене О. Ахмаді, І. Шпарлінскі та Ж. Волохом. Виведено, використовуючи результати з теорії розбиттів натурального числа, явні нижні межі для мультиплікативних порядків таких елементів в термінах p та r. Межі такого типу: явні й для будь-яких p та r, становлять особливий інтерес для прикладних застосувань (зокрема, криптографії), бо дозволяють просто порівнювати різні розширення скінченних полів. Наведено низку числових прикладів для отриманих результатів. Описано модифікацію нижніх меж для порядків на основі кількості розв'язків лінійної діофантової нерівності. Слід підкреслити, що ключовим моментом при отриманні результатів цього розділу є використання автоморфізмів Фробеніуса розширень полів.

У розділі 4 в розширеннях Куммера скінченних полів явно збудовано елементи мультиплікативного порядку більшого від 4^m. Це нижня межа, яка є точною величиною, на відміну від відомої раніше наближеної межі, що суттєво для низки прикладних застосувань. У довільних розширеннях скінченних скінченних полів на основі поліномів Куммера (вигляду $F_q[x]/(x^m - a)$) отримано експоненційну нижню межу для порядку. Власне знято умову подільності числа $q-1$ на m для будь-якого степеня розширення m. Розглянуто довільне розширення вигляду $F_q[x]/(x^m - a)$, і явно збудовано в ньому елементи мультиплікативного порядку принаймні $2^{\lfloor \sqrt[3]{2m} \rfloor}$. Запропонована автором ідея полягає в наступному: якщо $q-1$ має великий дільник m_1, то для побудови слід використати метод як для розширень Куммера; якщо ж $q-1$ не має великого дільника m_1, то число $m_2 = m/m_1$ є великим, і треба використати для побудови метод, аналогічний до методу для циклотомічних розширень. Слід зауважити, що у випадку розширень Куммера спряжені лінійного бінома знову є лінійними біномами. Для загального випадку розширень на основі поліномів Куммера це вже не справджується. У цій ситуації ефективним є запропонований метод комбінування двох підходів. Дану нижню межу підсилено з використанням максимуму функції кількості розв'язків діофантового рівняння або з використанням оцінки знизу для кількості розбиттів.

Розділ 5 присвячений розгляду розширень скінченних полів на основі поліномів Артіна-Шраєра (вигляду $F_{p^p} = F_p[x]/(x^p - x - a)$). У них збудовано в явному вигляді елементи великого порядку та дано також явну оцінку знизу на їх мультиплікативний порядок рівну 4^p. Для побудови використано такий же ж

підхід, як і для розширень Кумммера в розділі 4. Використовуючи комп'ютерні обчислення, показано, що ці елементи для простих чисел $p<126$ та $p=137, 163, 167, 173$ мають насправді набагато більший порядок рівний $N_p = p^{p-1}+...+p+1$. Виходячи з цього результату, виписано деякі примітивні елементи. Виведено нижню межу для добутку біноміальних коефіцієнтів, пов'язаному з тестуванням простоти великих натуральних чисел чи побудовою елементів великого мультиплікативного порядку в розширеннях Куммера або Артіна-Шраєра. Отримано обмеження на порядок деяких елементів у розширеннях Артіна-Шраєра скінченних полів при умові, що цей порядок менший від числа N_p.

У розділі 6 виведено нижню межу для порядку елементів, які задають послідовні розширення полів, у вежах скінченних полів, визначених Конвеєм. Використовуючи комп'ютерні обчислення та відомі розклади перших дванадцяти чисел Ферма на прості множники, знайдено певні примітивні елементи для перших дванадцяти полів у вежах Конвея. Сформульовано умову, при якій елементи вказаного вигляду є примітивними у всіх полях у вежах Конвея. Отримано певні обмеження та, як наслідок, нижню межу для мультиплікативного порядку деяких елементів у двійкових рекурсивних розширеннях скінченних полів, визначених Відеманом. Отримано нижні межі для порядків елементів у вежах скінченних полів характеристики більшої, ніж два. У частковому випадку вежі з трьох полів описано спряжені елемента, який задає друге розширення, над початковим полем, що дозволило отримати сильнішу нижню межу, ніж у загальному випадку. Стосовно веж скінченних полів характеристики більшої, ніж два, не було відомо ніяких результатів про порядки елементів.

Заключний розділ 7 присвячений підсиленню нижньої межі для мультиплікативного порядку деяких елементів у загальних розширеннях скінченних полів як на основі гіпотези Гао, так і без використання вказаної гіпотези. Також вивчено зв'язок між елементами великого порядку та доведенням простоти великих натуральних чисел. Зокрема, отримано результати, які описують можливі способи побудови контрприкладів для гіпотези Аграваля. Доведено результати, які дозволяють пов'язати із вказаною гіпотезою певний ланцюг підгруп відповідної мультиплікативної групи скінченного поля. Отримано експоненційні нижні межі для порядків підгруп у цьому ланцюзі груп.

Результати, що їх викладено в дисертації є новими, вони строго доведені. Це вимагало від автора розробки нового аналітичного апарату, подолання значних технічних труднощів. На базі дисертаційної роботи було б доцільним підготувати монографію. Хотів би виділити результати Романа Богдановича що

дають відповідь на питання видатного експерта з криптографії та теорії чисел Ігоря Шпарлінського (Сідней, Австралія), з яким маю досвід співпраці (зокрема, при проведенні Інституту Вищих Досліджень НАТО у Влорі, 2008 рік). Мені відомо, що публікація Р. Б. Поповича в журналі "Finite fields and their applications" зацікавила спеціалістів з різних університетів світу (Австралія, Сінгапур, Індія, Канада, Сполучені Штати, різні Європейські наукові установи). Тому я б рекомендував дисертанту видавати монографію англійською мовою через World Scientific або Springer.

Рекомендації щодо використання результатів дисертації

Підсумовуючи вище сказане, вважаю, що дисертаційна робота Романа Богдановича Поповича, яка розв'язує кілька важливих проблем, містить низку конструктивних результатів. Це закладає новий напрямок в теорії скінчених полів та її криптографічних застосувань. Вважаю, що результати дисертаційної роботи будуть використатися дослідниками Університету Марії Кюрі Склодовської в Любліні (кафедра алгебри та дискретної математики Інституту математики та кафедра безпеки інформації Інституту інформатики), Київського національного університету імені Тараса Шевченка, Інституту кібернетики ім. В. М. Глушкова НАН України (відділ акад. І. М. Коваленка та інші підрозділи) , Інституту телекомунікацій та глобального інформаційного простору НАН України, Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" (кафедра математичних методів захисту інформації Фізико-технічного інституту) та відомому семінарі професора М. М. Савчука.

Зауваження щодо змісту дисертаційної роботи

У роботі для отримання невеликої частини результатів використано комп'ютерні обчислення. Цим сьогодні вже нікого не здивуєш. Проте бажано у майбутньому по можливості отримати доведення без застосування комп'ютерних обчислень.

У дисертації в оглядовій частині варто було б згадати про праці, пов'язані з великими циклічними підгрупами скінчених загальних лінійних груп.

Оцінка мови, стилю та оформлення дисертації та автореферату

Оформлення дисертаційної роботи й автореферату цілком відповідає встановленим вимогам. Робота й автореферат написано на досить високому стилістичному рівні та з використанням загальновизначеної сучасної наукової термінології, що забезпечує доступність їх сприйняття та використання. Дисертація в цілому досить ясно та чітко написана, незважаючи на певну

кількість описок та опечаток, неминучих у роботі такого значного обсягу. Звичайно, такі зауваження не впливають на високу оцінку роботи.

Основні результати своєчасно опубліковані в фахових журналах із фізико-математичних наук, що відповідають вимогам Міністерства освіти і науки України; зокрема, дві статті опубліковано в журналі "Finite fields and their applications", який є одним із основних із напрямку скінченних полів, його імпакт-фактор дорівнює 1,299. Автореферат дисертації правильно відображає її зміст. Результати кандидатської дисертації пошукувача в докторській дисертації не містяться.

Загальний висновок

Таким чином, дисертаційна робота є значним внеском до теорії скінченних полів; у ній, зокрема, збудовано в явному вигляді елементи великого мультиплікативного порядку для низки класів скінченних полів.

Дисертаційна робота Поповича Романа Богдановича виконана на актуальну тему, на високому науковому рівні, висунуті на захист результати та обґрунтовані положення, математично доведені, мають наукову новизну та практичну цінність, робота повністю відповідає вимогам Міністерства освіти і науки України, що пред'являются до докторських дисертацій, та чинному "Порядку присудження наукових степенів", затвердженого постановою Кабінету Міністрів України № 567 від 24 липня 2013 року, а її автор, Попович Р. Б., заслуговує на присудження наукового ступеня доктора фізико-математичних наук за спеціальністю 01.01.06 – алгебра та теорія чисел.

Офіційний опонент:
завідувач кафедри алгебри та дискретної математики
Університету ім. Марії Склодовської Кюрі, м. Люблін, Польща
доктор фізико-математичних наук, професор, V. Ustymenko

В. О. Устименко

000001353
Uniwersytet Marii Curie-Skłodowskiej
Instytut Matematyki
pl. Marii Curie-Skłodowskiej 1
20-031 Lublin tel. (081) 537-61-20

Підпис д.ф.-м.н., проф. Устименка В.О. засвідчую:

Секретар Інституту Математики
Університету ім Марії Склодовської Кюрі в Любліні

М. Крут

Інститут математики Академії наук України
Канцелярія

Надійшов до спеціалізованої вченої ради Д26.206.03 23.09.2016 р.
секретар ради /Артеменко Ж.В./