Національна Академія Наук України
Інститут математики

ПОПОВИЧ РОМАН БОГДАНОВИЧ

УДК 512.624

ЕЛЕМЕНТИ ВЕЛИКОГО МУЛЬТИПЛІКАТИВНОГО ПОРЯДКУ В СКІНЧЕННИХ ПОЛЯХ

01.01.06 – алгебра та теорія чисел

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора фізико-математичних наук

Київ – 2016

Дисертацією є рукопис.

Робота виконана на кафедрі спеціалізованих комп'ютерних систем
Національного університету "Львівська політехніка"
Міністерства освіти і науки України.

Науковий консультант:

доктор фізико-математичних наук, професор
Кириченко Володимир Васильович,
Київський національний університет
імені Тараса Шевченка, завідувач кафедри геометрії

Офіційні опоненти:

доктор фізико-математичних наук, професор
Варбанець Павло Дмитрович,
Одеський національний університет імені І. І. Мечникова,
завідувач кафедри комп'ютерної алгебри та дискретної
математики

доктор фізико-математичних наук, професор
Глазунов Микола Михайлович,
Національний авіаційний університет, м. Київ,
професор кафедри електроніки

доктор фізико-математичних наук, професор
Устименко Василь Олександрович,
Університет Марії Кюрі-Склодовської,
м. Люблін, Польща,
завідувач кафедри алгебри і дискретної математики

Захист відбудеться "4" жовтня 2016 р. о 15 год. на засіданні спеціалізованої вченої ради Д 26.206.03 в Інституті математики НАН України за адресою: 01004, м. Київ, вул. Терещенківська, 3.

З дисертацією можна ознайомитись у бібліотеці Інституту математики НАН України за адресою: 01004, м. Київ, вул. Терещенківська, 3.

Автореферат розісланий "30" серпня 2016 р.

Вчений секретар
спеціалізованої вченої ради С. І. Максименко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Основу сучасних швидких та якісних технологій обробки інформації становлять комп'ютери – від персональних до супер-ЕОМ. Для ефективної роботи на комп'ютері необхідно навчитися будувати моделі реальних об'єктів та процесів їх перетворення. Досить часто згаданими моделями можуть бути такі алгебраїчні структури, як скінченні поля.

Однією з областей застосування є кодування інформації при передачі через канал зв'язку. Найкращих результатів досягнуто, коли символи, що передаються, розглядаються як елементи певних алгебраїчних структур, зокрема скінченних полів (також використовують назву поля Галуа). При цьому простими стають процедури кодування й декодування, зменшується ймовірність неправильного декодування даних. Іншою областю застосування є криптографія: захист інформації шляхом її перетворення, що виключає прочитання цієї інформації сторонньою особою. Широко вживаний алгоритм RSA шифрування з відкритим ключем ґрунтується на алгебраїчному понятті скінченого кільця чи поля.

Поняття поля[1] неявно застосовувалось вже в першій половині XIX століття Н. Абелем та Е. Галуа для дослідження розв'язків алгебраїчних рівнянь п'ятого та вищих степенів. У 1871 році Р. Дедекінд запровадив для множини дійсних та комплексних чисел поняття "тіло" (нім. körper), щоб підкреслити їх замкненість щодо арифметичних операцій. В 1893 році Е. Мур ввів для цих алгебраїчних структур назву "поле" (англ. field) та довів класифікаційну теорему для скінченних полів[2]: порядок скінченного поля є натуральним степенем простого числа; для довільного $q = p^n$ існують скінченні поля з q елементами і всі вони ізоморфні. П. Ферма, Л. Ейлер, Г. Лейбніц, Ж. Лагранж, А. Лежандр, К. Гаусс, Е. Галуа, Е. Мур, Г. Вебер, Д. Веддерберн, Е. Стейніц, Ж. Сере, Т. Шенеман, Р. Дедекінд, Л. Діксон, Е. Артін, А. Вейль – це далеко не повний перелік математиків, які заклали підвалини теорії скінченних полів.

Множина ненульових елементів скінченного поля є абелевою групою відносно множення. Відомо, що вказана група циклічна[3], тобто для цієї мультиплікативної групи існують твірні елементи, які часто називають примітивними. За винятком полів з двох або трьох елементів, примітивний елемент не єдиний. Кількість примітивних елементів дорівнює значенню функції Ейлера від кількості ненульових елементів скінченого поля.

Також слід згадати результати про існування примітивних елементів певного (досить простого) вигляду[4], зокрема, для розширень степеня 2, 3 та 4. Побудову примітивних елементів простого вигляду розглядали Х. Давенпорт, Л. Карліц,

---

[1] Варден Б. Л. ван дер. Алгебра / Б. Л. ван дер Варден. – М.: Наука, 1976. – 648 с.
Дрозд Ю. А. Конечномерные алгебры / Ю. А. Дрозд, В. В. Кириченко – Київ: Вища школа, 1980. – 192 с.

[2] Lidl R. Finite Fields / R. Lidl, H. Niederreiter. – Cambridge: Cambridge University Press, 1997. –755 p.

[3] Mullen G. L. Finite Fields / G. L. Mullen, D. Panario – Boca Raton: CRC Press, 2013. – 1068 p.

[4] Cohen S.D. Consecutive primitive roots in a finite field / S.D. Cohen // Proc. Amer. Math. Soc. – 1985. – Vol. 93, no. 2. – P. 189–197.

С. Коен, Д. Мілс, Г. Макней, Р. Гіудікі, К. Маргагліо. Показано, що існують примітивні елементи, які є поліномами першого степеня відносно елемента, який задає розширення початкового поля. Отримано й низку результатів[5] про існування примітивних елементів із різними додатковими властивостями. Зокрема, доведено існування нормальних примітивних елементів. Це зроблено в працях Х. Давенпорта, Л. Карліца, С. Коена, Р. Шуфа, С. Гучинскої, Х. Лестри, Д. Хаченбергера, К. Хсу, Т. Хана, Р. Ванга, К. Као, Р. Фенга, Г. Капетанакіса, Т. Тіана, В. Кві.

Якщо елемент a – примітивний в полі F_q, то для кожного ненульового елемента x з цього поля існує єдине ціле число n між нулем та $q-2$ таке, що $x = a^n$. Це ціле число називають дискретним логарифмом для x за основою a. Хоча обчислення a^n є відносно простим (наприклад, піднесення до степеня з використанням послідовних піднесень до квадрату, так званий "індійський алгоритм"), обернена операція обчислення дискретного логарифму є обчислювально складною. Це використано в низці криптографічних протоколів.

Тому важливим є отримання в явному вигляді твірного елемента для мультиплікативної групи скінченого поля. На сьогодні задача ефективної побудови (тобто з поліноміальним часом виконання $\log(q^n)^{O(1)}$ арифметичних операцій у полі F_{q^n}) примітивного елемента заданого скінченого поля є обчислювально важкою і залишається відкритою. Усі відомі алгоритми[6] для цієї проблеми працюють у два етапи: на першому етапі знаходять "невелику" множину, яка гарантовано містить примітивний елемент, а на другому етапі випробовують всі елементи вказаної множини на примітивність.

У багатьох випадках, маємо поліноміальні алгоритми для першого етапу. На жаль, при сьогоднішньому стані знань, другий етап вимагає розкладу числа $q-1$ на прості множники (елемент α примітивний тоді і тільки тоді, коли $\alpha^{(q-1)/d} \neq 1$ для кожного простого дільника d числа $q-1$), для чого невідомий поліноміальний алгоритм. У напрямку знаходження примітивного елемента для скінченого поля слід виокремити праці Л. Карліца, Х. Давенпорта, Е. Баха, Й. Ванга, В. Шоупа, І. Шпарлінскі, М. Хуанга, А. Нараяна.

Через це задачу послаблюють і ставлять задачу знайти елемент великого мультиплікативного порядку. С. Гао спробував формалізувати поняття елементів "великого порядку" даючи наступне визначення[7]. Під "великим порядком" елемента у скінченому полі F_{q^n}, ми розуміємо, що порядок елемента повинен бути більший, ніж кожен поліном від $\log(q^n)$, коли q^n стає як завгодно великим. Можна провести паралель між поділом алгоритмів стосовно оцінки їх обчислювальної складності та поділом елементів скінченного поля на елементи великого порядку та порядку, який

---

[5] Cohen S. D. The primitive normal basis theorem – without a computer / S. D. Cohen, S. Huczynska // J. London Math. Soc. – 2003. – Vol. 67, no. 1. – P. 41–56.

[6] Gathen J. Orders of Gauss periods in finite fields / J. von zur Gathen, I. E. Shparlinski // Appl. Algebra Engrg. Comm. Comput. – 1998. – Vol. 9, no. 1. – P. 15–24.

[7] Gao S. Elements of provable high orders in finite fields / S. Gao // Proc. Amer. Math. Soc. – 1999. – Vol. 107, no. 6. – P. 1615–1623.

не є великим. У випадку алгоритмів маємо еспоненційні та поліноміальні алгоритми. Для експоненційних алгоритмів оцінка обчислювальної складності більша від будь-якого полінома від обсягу вхідних даних (тобто від логарифма від значення вхідної величини). Для поліноміальних алгоритмів оцінка обмежена деяким поліномом. Поняття елемента великого порядку аналогічне до поняття експоненційного алгоритму. Елемент, який не є елементом великого порядку, можна порівняти з поліноміальним алгоритмом.

При цьому переважно вважаємо, що число q відносно невелике (щоб можна було збудувати примітивні елементи в полі F_q безпосереднім перебиранням), а число n може бути дуже великим. Тобто, побудову елементів великого порядку для простих полів при такій постановці задачі переважно не розглядають.

Питання побудови елементів великого мультиплікативного порядку[3,8] розглядають як для загальних (С. Гао, А. Конфлітті), так і для часткових скінченних полів (О. Ахмаді, І. Шпарлінскі, Ж. Волох, Й. Гатен, Д. Панаріо, М. Чанг, К. Ченг, Д. Ван). Для часткових випадків скінченних полів можна збудувати елементи, що мають набагато більші порядки.

При побудові елементів великого порядку переважає комбінаторний підхід. Для отримання елемента великого порядку беруть деякий двочлен від елемента, що задає розширення. Як правило, це лінійний двочлен. Щоб отримати нижню межу для порядку, аналізують добутки елементів, спряжених з вибраним. Використовують як лінійні, так і нелінійні спряжені. Можна залучати як додатні, так і від'ємні степені цих спряжених.

Відомо дуже мало результатів, коли жодне обмеження не накладене на степінь розширення поля. С. Гао дав алгоритм побудови елементів великого порядку для загальних розширень F_{q^n} скінченного поля F_q з нижньою межею для порядку $\exp((\log n)^2)$. Його алгоритм припускає виконання певної правдоподібної, але досі не доведеної гіпотези. Зауважимо, що наведені обчислювальні дані підтверджують гіпотезу лише для полів характеристики два, а для більшої від двох такі дані в літературі відсутні. А. Конфлітті, спираючись на вказану гіпотезу, виконав точніший аналіз результатів С. Гао. Трудність підходу полягає в тому, що степінь полінома, який описує спряжені до початково вибраного елемента, росте експоненційно із збільшенням номера. Тому в обидвох випадках отримано лише слабо суперполіноміальні нижні межі. Таким чином, маємо порівняно скромний результат, який ще й спирається на недоведене припущення.

Якщо поле володіє додатковими властивостями, то є методи, які обходять цю трудність та будують елемент порядку більшого, ніж q^{n^c} для деякої константи c. Обидва методи працюють лише для випадків часткових полів.

Так, ґрунтуючись на властивостях гауссових періодів, Й. Гатен та І. Шпарлінскі запропонували в 1995 році алгоритм, який будує елемент

---

[8] Cheng Q. On the construction of finite field elements of large order / Q. Cheng // Finite Fields Appl. – 2005. – Vol. 11, no. 3. – P. 358–366.

субекспоненційного порядку в полях на основі циклотомічних поліномів. Це був перший приклад елемента великого порядку в скінченних полях.

Сучасна техніка у широко відомому алгоритмі AKS тестування простоти та його подальших вдосконаленнях (М. Агравал, Н. Кайал, Н. Саксена, Д. Бернштейн, П. Беррізбейтіа, Ж. Волох) полягає у використанні поліномів першого степеня для породження великої мультиплікативної підгрупи за модулем натурального числа та деякого полінома. К. Ченг побачив зв'язок цієї задачі із проблемою знаходження елемента великого порядку для часткових скінченних полів та застосував цю ідею для отримання нового розв'язку цієї проблеми. Він розглядав розширення Куммера F_{q^n}, де степінь розширення n ділить число $q-1$. Близькими до розширень Куммера є розширення на основі підпросторових поліномів.

Ж. Волох у своїх працях та зробленому ним огляді розглядав описані раніше результати та деякі власні результати з такої точки зору: для отримання елемента великого порядку беремо елемент малого порядку. Тобто елементи малого та великого порядку завжди йдуть в парі. Слід розглядати пари координат точок на плоских кривих. При певних умовах, якщо одна з кординат має малий порядок, то інша має великий мультиплікативний порядок.

Особливий інтерес становить побудова елементів у рекурсивних розширеннях скінченних полів – вежах скінченних полів характеристики два або більшої від двох (Л. Бруін, Д. Конвей, Д. Відеман, Х. Іто, Т. Каджівара, Х. Сонг). З прикладної точки зору такі побудови дуже привабливі, оскільки операції над елементами скінченого поля можна виконувати рекурсивно, а тому ефективно.

Області застосування як примітивних елементів, так і елементів великого порядку в скінченних полях (А. Менезес, Р. Ооршот, С. Ванстоун) такі: криптографія (зокрема, протокол Діффі-Хелмана, криптосистема Ель-Гамаля з відкритим ключем), доведення простоти великих чисел, завадостійке кодування, генератори псевдовипадкових чисел.

У цьому напрямку слід також виділити роботи з опису генераторів псевдовипадкових чисел у кільцях цілих гауссових чисел із оцінкою криптографічної якості цих генераторів (П. Варбанець), використання комп'ютерних обчислень для обґрунтування гіпотез алгебри та теорії чисел (М. Глазунов), алгебраїчної комбінаторики та можливих криптографічних застосувань (О. Устименко), скінченновимірних алгебр (Ю. Дрозд, В. Кириченко), скінченних майже-кілець (Я. Сисак).

Все вищесказане свідчить про актуальність дослідження питання про явну побудову елементів великого мультиплікативного порядку та примітивних елементів для скінченних полів різного вигляду, чому й присвячено дисертаційну роботу.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження проводились 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.).

Мета і задачі дослідження. *Об’єктом дослідження* є мультиплікативні групи скінчених полів.

Предметом дослідження є мультиплікативні порядки елементів у мультиплікативних групах скінчених полів.

Метою дослідження є отримання в явному вигляді нижніх меж та елементів скінченних полів з мультиплікативними порядками, які задовольняють ці межі.

Завдання дослідження:

1. Покращення відомих та отримання нових нижніх меж для порядків елементів у скінченних полях на основі циклотомічних поліномів.
2. Виведення нижніх меж для порядків елементів у скінченних полях на основі поліномів Куммера.
3. Одержання нижніх меж для порядків елементів у скінченних полях на основі поліномів Артіна-Шраєра. Знаходження певних примітивних елементів у вказаних полях.
4. Визначення нижніх меж для порядків елементів у вежах Відемана скінченних полів.
5. Оцінювання нижніх меж для порядків елементів у вежах Конвея скінченних полів. Побудова певних примітивних елементів у цих полях.
6. Дослідження нижніх меж для порядків елементів у вежах скінченних полів характеристики більшої, ніж два.
7. Покращення нижніх меж для порядків елементів у скінченних полях загального вигляду.
8. Дослідження зв’язку між тестуванням простоти великих натуральних чисел і певними підгрупами мультиплікативної групи скінченого поля. Отримання нижніх меж для порядків цих підгруп.

Методи дослідження. У роботі використовуються методи теорії скінченних полів (зокрема, автоморфізми Фробеніуса), комбінаторики (зокрема, теорія розбиттів), теорії чисел, а також комп’ютерні обчислення.

Наукова новизна одержаних результатів. Усі теоретичні результати, що виносяться на захист є новими і головні з них полягають у наступному.

1. У розширеннях скінченних полів на основі циклотомічних полів (вигляду $F_q[x]/(x^{r-1}+..+x+1)$) 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.
2. У розширеннях Куммера скінченних полів збудовано в явному вигляді елементи порядку більшого, ніж 4^m. У довільних розширеннях скінченних полів на основі поліномів Куммера (вигляду $F_q[x]/(x^m-a)$) отримано експоненційну нижню межу для порядку $2^{\lfloor\sqrt[3]{2m}\rfloor}$.

3. У розширеннях скінченних полів на основі поліномів Артіна-Шраєра (вигляду $F_p[x]/(x^p - x - a)$) збудовано в явному вигляді елементи експоненційного порядку принаймні 4^p.
4. У розширеннях скінченних полів на основі поліномів Артіна-Шраєра для випадку $p < 126$ та $p = 137, 163, 167, 173$ виписано з використанням комп'ютерних обчислень деякі примітивні елементи.
5. Отримано нижню межу для мультиплікативного порядку елементів у вежах Відемана скінченних полів.
6. Виведено нижню межу для мультиплікативного порядку елементів у вежах Конвея скінченних полів.
7. Для перших дванадцяти полів у вежі Конвея знайдено з використанням комп'ютерних обчислень певні примітивні елементи. Сформульовано умову, при якій елементи вказаного вигляду є примітивними у всіх полях у вежі Конвея.
8. Одержано нижні межі для порядків елементів у вежах скінченних полів характеристики більшої, ніж два. У частковому випадку вежі з двох полів описано спряжені елемента, який задає друге розширення, над початковим полем, що дозволило отримати сильнішу нижню межу, ніж у загальному випадку.
9. Підсилено нижню межу для мультиплікативного порядку деяких елементів у загальних розширеннях скінченних полів як на основі гіпотези Гао, так і без використання вказаної гіпотези.
10. Виведено нижні межі для порядків підгруп мультиплікативної групи скінченних полів, пов'язаних з тестуванням простоти великих натуральних чисел.

Наведені результати одержані вперше.

Практичне значення одержаних результатів. Дисертаційна робота має теоретичний характер. Результати роботи можуть бути використані при явній побудові елементів великого мультиплікативного порядку в скінченних полях при подальшому дослідженні скінченних полів. Вони також можуть стати математичною основою для різноманітних розробок в галузі інформаційних технологій, зокрема елементи великого порядку можуть бути застосовані в криптографії та завадостійкому кодуванні. Отримані результати можуть бути використані при читанні спецкурсів у вищих навчальних закладах.

Особистий внесок автора. Усі теоретичні результати, що виносяться на захист, одержані автором самостійно та опубліковані у наукових статтях без співавторів.

Апробація результатів дисертації. Результати дисертації оприлюднено на наступних конференціях:

1. Second Workshop on Mathematical Cryptology (Santander, Spain, 2008);

2. Восьмій Міжнародній алгебраїчній конференції в Україні (Луганськ, 2011);

3. Міжнародній математичній конференції, присвяченій 70-річчю професора Володимира Кириченка (Миколаїв, 2012);

4. Міжнародній конференції, присвяченій 120-річчю від дня народження Стефана Банаха (Львів, 2012);

5. Міжнародній алгебраїчній конференції, присвяченій 100-річчю від дня народження С. М. Чернікова (Київ, 2012);

6. Дев'ятій Міжнародній алгебраїчній конференції в Україні (Львів, 2013);

7. Міжнародній науковій конференції "Сучасні проблеми механіки і математики" (Львів, 2013);

8. Міжнародній алгебраїчній конференції, присвяченій 100-річчю від дня народження Л. А. Калужніна (Київ, 2014);

9. Десятій Міжнародній алгебраїчній конференції в Україні (Одеса, 2015).

10. Другій (Львів, 2005) та третій (Львів, 2007) міжнародних конференціях "Сучасні комп'ютерні системи та мережі: розробка та використання";

11. Десятій Міжнародній науково-технічній конференції "Комп'ютерні науки та інформаційні технології" (Львів, 2015).

Крім цього, результати дисертації доповідалися на таких семінарах:

- алгебраїчному семінарі Інституту математики НАН України (Київ, 2016 р., керівник – член-кор. НАН України, д. ф.-м. н., професор Ю. А. Дрозд);

- львівському міському алгебраїчному семінарі (Львівський національний університет імені Івана Франка, 2011 – 2016 рр., керівник – д. ф.-м. н., професор М. Я. Комарницький);

- семінарі відділу алгебри Інституту прикладних проблем механіки і математики імені Я. С. Підстригача НАН України (Львів, 2012–2016 р., керівник – д. ф.-м. н., професор В. М. Петричкович),

- математичному семінарі Інституту прикладних проблем механіки і математики ім. Я. С. Підстригача НАН України (Львів, 2016 р., керівники – член-кор. НАН України, д. ф.-м. н., професор Б. Й. Пташник, д. ф.-м. н., професор М.М. Войтович, д. ф.-м. н. В. О. Пелих, д. ф.-м. н., професор В. М. Петричкович);

- першому науковому семінарі "Кіберфізичні системи: досягнення та виклики" Інституту комп'ютерних технологій, автоматики та метрології Національного університету "Львівська політехніка" (Львів, 2015 р., керівник – д. т. н., професор А. О. Мельник);

- науковому семінарі кафедри спеціалізованих комп'ютерних систем (Львів, 2008–2016 р.р., керівник – д. т. н., професор Р. Б. Дунець).

Публікації. Результати дисертації опубліковані в 20 наукових статтях [1–20] у провідних закордонних та українських наукових фахових виданнях із фізико-математичних наук, затверджених МОН України, 6 із яких [13, 14, 15, 17, 18, 19] надруковано у виданнях, включених до міжнародних наукометричних баз Web of Science і/або Scopus, і додатково висвітлені в 2 статтях у збірниках наукових праць та 10 матеріалах і тезах міжнародних наукових конференцій [21–32].

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, семи розділів, висновків та списку використаних джерел. Повний обсяг дисертації становить 302 сторінки друкованого тексту, з яких 286 сторінок основного тексту. Дисертація містить 6 таблиць та 2 рисунки. Список використаних джерел обсягом 16 сторінок налічує 150 найменувань.

Автор висловлює подяку своєму науковому консультанту, професору Володимиру Васильовичу Кириченку за підтримку в роботі.

ОСНОВНИЙ ЗМІСТ РОБОТИ

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. Щоб зробити виклад замкненим і для зручності посилань, деякі з відомих тверджень і теорем формулюються у належному для цього вигляді. Проведено огляд відомих результатів, наведених у літературі.

Кільце – це алгебраїчна структура з двома операціями, які задовольняють такі умови: відносно першої операції (додавання) – це абелева група, відносно другої операції (множення) – це півгрупа; друга операція дистрибутивна зліва та справа відносно першої операції. Якщо відносно другої операції існує нейтральний елемент, то кільце називають кільцем з одиницею. Якщо друга операція комутативна, то кільце називають комутативним. Поле – це комутативне кільце з одиницею, в якому кожен ненульовий елемент має обернений відносно операції множення. Якщо поле має скінченне число елементів, то його називають скінченним або полем Галуа. Усі ненульові елементи скінченного поля утворюють циклічну групу, яку ще називають мультиплікативною групою скінченного поля. Порядок елемента цієї групи називають мультиплікативним порядком цього елемента в скінченному полі.

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** 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 $F_q(\theta) = F_{q^{r-1}} = F_q[x]/(x^{r-1} + ... + x + 1)$ (на основі циклотомічних поліномів). Умову, при якій вказане фактор-кільце є полем, наведено в роботі[2]. Вона полягає в тому, що $r \geq 3$ – просте число, а q – примітивний корінь з одиниці за модулем r. Розширення такого вигляду розглядалися в роботах[6,9].

У першому підрозділі покращено та узагальнено результат з праці О. Ахмаді, І. Шпарлінскі та Ж. Волоха[9] 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 вказаних роботах[6,9] та теоремі 3.1 використовують поняття розбиття. Розбиття натурального числа C – це така послідовність невід'ємних цілих чисел $u_1,\ldots,u_C$, що $\sum_{j=1}^{C} j u_j = C$. Число j називаємо частиною розбиття, а число u_j описує кількість повторень частини j у розбитті. $U(C,d)$ позначає кількість таких розбиттів числа C, для яких $u_1,\ldots,u_C \leq d$. Всі нижні межі в теоремі 3.1 використовують поняття розбиття, де кожна частина з'являється не більше, ніж $p-1$ разів.

Теорема 3.1. *Нехай q – степінь простого числа p, $r = 2s+1$ – просте число взаємно просте з q, q – примітивний корінь за модулем r, θ задає розширення $F_q(\theta) = F_{q^{r-1}}$, e – довільне ціле число, f – довільне ціле число взаємно просте з r, a – будь-який ненульовий елемент скінченого поля F_q. Тоді справедливі наступні твердження:*

(a) *елемент $\theta^e(\theta^f + a)$ має мультиплікативний порядок принаймні $U(r-2, p-1)$,*

(b) *елемент $(\theta^{-f} + a)(\theta^f + a)$ для $a^2 \neq -1$ має мультиплікативний порядок принаймні $U((r-3)/2, p-1)$, і цей порядок ділить $q^{(r-1)/2} - 1$,*

(c) *елемент $\theta^{-2e}(\theta^{-f} + a)(\theta^f + a)^{-1}$ для $a^2 \neq 1$ має мультиплікативний порядок принаймні $U((r-3)/2, p-1)$, і цей порядок ділить $q^{(r-1)/2} + 1$,*

(d) *елемент $\theta^e(\theta^f + a)$ для $a^2 \neq \pm 1$ має мультиплікативний порядок принаймні $[U((r-3)/2, p-1)]^2/2$.*

Із теореми 3.1 отримуємо отримуємо оцінку для порядку елементів вигляду $\beta = \theta + \theta^{-1} = \theta^{-1}(\theta^2 + 1)$ у циклотомічних розширеннях скінченних полів. Такі елементи називають гауссовими періодами за аналогією із розширеннями поля

[9] Ahmadi O. Multiplicative order of Gauss periods / O. Ahmadi, I. E. Shparlinski, J. F. Voloch // Int. J. Number Theory. – 2010. – Vol. 6, no. 4. – P. 877–882.

раціональних чисел. К. Ф. Гаусс використав відповідні поняття, щоб показати, що правильний 17-кутник можна збудувати за допомогою лінійки та циркуля.

Наслідок 3.1. *Гауссовий період* β *має мультиплікативний порядок принаймні* $U(r-2, p-1)$ *і цей порядок ділить* $q^{(r-1)/2}-1$.

Нижня межа $U(r-2, p-1)$ для мультиплікативного порядку гауссового періоду β покращує раніше відому межу $U((r-3)/2, p-1)$ О. Ахмаді, І. Шпарлінскі та Ж. Волоха.

Нехай a – довільний ненульовий елемент поля F_q. Позначимо

$$\gamma=(\theta^{-1}+a)(\theta+a)^{-1} \text{ та } z=\begin{cases}\beta^2\gamma, \text{ якщо } \rho_2(q^{(r-1)/2}-1)=2,\\ \beta\gamma^2, \text{ якщо } \rho_2(q^{(r-1)/2}+1)=2.\end{cases}$$

На підставі теореми 3.1, для порядку введеного елемента z отримано наступну нижню межу.

Наслідок 3.2. *Елемент* z *для* $a^2\neq 1$ *має мультиплікативний порядок принаймні* $[U(r-2, p-1)U((r-3)/2, p-1)]/2$.

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. Такий прийом використовуємо для полів на основі циклотомічних поліномів. Зокрема, елемент $\theta^e(\theta^f+a)$ заміняємо на $\theta^g(\theta+a)$, де $g\equiv ef^{-1} \bmod r$. На основі цього зменшуємо степінь елемента як полінома від змінної θ і можемо показати, що цей елемент має більше попарно різних степенів.

У другому підрозділі, використовуючи відомі результати з теорії розбиттів, перетворюємо нижні межі з теореми 3.1 та наслідку 3.2 у термінах розбиттів у явні нижні межі для мультиплікативних порядків елементів у термінах p – характеристика початкового поля та r – степінь розширення початкового поля. Розрізняємо такі два випадки.

Випадок 1. Число r велике порівняно з p.

У цьому разі у всіх одержаних оцінках фігурують обидві величини p та r.

Наслідок 3.3. *Нехай* e *– довільне ціле число,* f *– довільне ціле число взаємно просте з* r, a *– довільний ненульовий елемент поля* F_q. *Тоді правильні такі нижні оцінки для порядків елементів:*

(а) *якщо виконується умова* $r\geq p^2+2$, *то елемент* $\theta^e(\theta^f+a)$ *має мультиплікативний порядок більший, ніж*

$$\left(\frac{p(p-1)}{160(r-2)}\right)^{\sqrt{p}} \exp\left(2.5\sqrt{(1-\frac{1}{p})(r-2)}\right);$$

(b) *якщо виконується умова* $r \geq 2p^2+3$, *то елемент* $\theta^e(\theta^f+a)$ *при* $a^2 \neq \pm 1$ *має мультиплікативний порядок більший, ніж*

$$\frac{1}{2}\left(\frac{p(p-1)}{80(r-3)}\right)^{2\sqrt{p}} \exp\left(2.5\sqrt{2}\sqrt{(1-\frac{1}{p})(r-3)}\right);$$

(c) *якщо виконується умова* $r \geq 2p^2+3$, *то елемент* z *при* $a^2 \neq 1$ *має мультиплікативний порядок більший, ніж*

$$\frac{1}{2}\left(\frac{p^2(p-1)^2}{12800(r-2)(r-3)}\right)^{\sqrt{p}} \exp\left(2.5(1+\frac{\sqrt{2}}{2})\sqrt{(1-\frac{1}{p})(r-3)}\right).$$

Випадок 2. Число r є того самого порядку, що й число p, або мале порівняно з p. У цьому разі у всіх виведених оцінках присутня лише величина r. Дійсно, скажімо при умові $r-2<p$ кількість розбиттів з обмеженням $U(r-2,p-1)$ співпадає з кількістю розбиттів без обмеження $U(r-2)$.

Наслідок 3.4. *Нехай* e *– довільне натуральне число,* f *– довільне натуральне число взаємно просте з* r, a *– довільний ненульовий елемент скінченого поля* F_q. *Тоді справедливі такі нижні оцінки для порядків елементів:*

(a) *якщо виконується умова* $r<p+2$, *то елемент* $\theta^e(\theta^f+a)$ *має мультиплікативний порядок більший, ніж*

$$\frac{\exp\left(2.5\sqrt{r-2}\right)}{13(r-2)};$$

(b) *якщо виконується умова* $r<2p+3$, *то елемент* $\theta^e(\theta^f+a)$ *при* $a^2 \neq \pm 1$ *має мультиплікативний порядок більший, ніж*

$$\frac{2\exp\left(2.5\sqrt{2}\sqrt{r-3}\right)}{169(r-3)^2};$$

(c) *якщо виконується умова* $r<2p+3$, *то елемент* r *при* $a^2 \neq 1$ *має мультиплікативний порядок більший, ніж*

$$\frac{\exp\left(2.5(1+\frac{\sqrt{2}}{2})\sqrt{r-3}\right)}{169(r-2)(r-3)}.$$

У 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 обчислення кількості розв'язків лінійної діофантової нерівності замість обчислення кількості розбиттів. Явні оцінки в термінах чисел p та r виведені в другому підрозділі з оцінок в термінах розбиттів. Проте, такі межі отримані лише при обмеженнях $r \geq p^2 + 2$ та $r < p + 2$. Важливий в прикладних застосуваннях випадок, коли $p + 2 \leq r < p^2 + 2$, залишився не описаним. Слід також зауважити, що отримані раніше у другому підрозділі вирази є громіздкими. Ось чому ми даємо в четвертому підрозділі кращі явні нижні межі для довільних p та r як для порядку гауссового періоду, так і елементів подібного вигляду.

Теорема 3.3. *Нехай q – степінь простого числа p, $r = 2s+1$ – просте число взаємно просте з q, q – примітивний корінь за модулем r, θ задає розширення $F_q(\theta) = F_{q^{r-1}}$, e – довільне ціле число, f – ціле число взаємно просте з r, a – довільний ненульовий елемент скінченого поля F_q. Тоді маємо такі нижні оцінки для порядків елементів:*

(a) *елемент $\theta^e(\theta^f + a)$ має мультиплікативний порядок принаймні*

$$\begin{cases} 2^{\sqrt{2(r-2)}-2}, \text{ якщо } p = 2, \\ 3^{\sqrt{r-2}-2}, \quad \text{якщо } p = 3, \\ 5^{\sqrt{(r-2)/2}-2}, \text{ якщо } p \geq 5, \end{cases}$$

(b) *елемент $\theta^e(\theta^f + a)$ при $a^2 \neq \pm 1$ має мультиплікативний порядок принаймні*

$$\begin{cases} 2^{2\sqrt{r-3}-5}, \text{ якщо } p = 2, \\ 3^{\sqrt{2(r-3)}-4}/2, \text{ якщо } p = 3, \\ 5^{\sqrt{r-3}-4}/2, \text{ якщо } p \geq 5, \end{cases}$$

(c) *елемент z при $a^2 \neq 1$ має мультиплікативний порядок принаймні*

$$\begin{cases} 2^{(\sqrt{2}+1)\sqrt{r-3}-5}, \text{ якщо } p=2, \\ 3^{(\sqrt{2}+1)\sqrt{r-3}/2-4}/2, \text{ якщо } p=3, \\ 5^{(\sqrt{2}+1)\sqrt{r-3}/2-4}/2, \text{ якщо } p\geq 5. \end{cases}$$

Наслідок 3.8. *Гауссовий період* β *має мультиплікативний порядок принаймні*

$$\begin{cases} 2^{\sqrt{2(r-2)}-2}, \text{ якщо } p=2, \\ 3^{\sqrt{r-2}-2}, \text{ якщо } p=3, \\ 5^{\sqrt{(r-2)/2}-2}, \text{ якщо } p\geq 5. \end{cases}$$

Нижня межа в наслідку 3.8 підсилює попередню відому межу $2^{\sqrt{r-1}-2}$ з праці[10] для мультиплікативного порядку елемента β.

У п'ятому підрозділі підсилено відомі асимптотичні нижні межі для порядків елементів, розглянутих у попередніх підрозділах.

У **четвертому розділі** розглядаємо явні нижні межі для мультиплікативного порядку елементів у розширеннях скінченних полів на основі поліномів Куммера (вигляду $F_q[x]/(x^m-a)$). В першому підрозділі висвітлюємо питання, при яких умовах такі розширення існують. У цьому підрозділі немає нових результатів – він носить технічний характер. Умови, при яких вказане фактор-кільце є полем, полягають в наступному:

Нехай F_q *– скінченне поле характеристики* $p\geq 5$. *Тоді над полем* F_q *існує нерозкладний біном степеня* m *в тому і тільки в тому випадку, коли:*

1) кожен простий дільник числа m *є також дільником числа* $q-1$,

2) якщо m *ділиться на* 4, *то* $q-1$ *ділиться на* 4.

Крайнім випадком виконання наведених двох умов є умова, що число m ділить число $q-1$ (тоді m не перевищує q). У цьому випадку отримуємо так звані розширення Куммера скінченних полів. У другому підрозділі розглядаємо власне такі розширення. Отримано нижню межу для порядку, яка є точною величиною, на відміну від відомої раніше наближеної межі[8], що суттєво для низки прикладних застосувань.

Теорема 4.3. *Припустимо, що* $m\geq 39$. *Для будь-якого ненульового елемента* b *поля* F_q *елемент* $\theta+b$ *розширення Куммера* F_{q^m} *має порядок більший, ніж* 4^m.

---

[10] Gathen J. Orders of Gauss periods in finite fields / J. von zur Gathen, I. E. Shparlinski // Appl. Algebra Engrg. Comm. Comput. – 1998. – Vol. 9, no. 1. – P. 15–24.

У праці[11] елементи великого порядку сконструйовано для розширень вигляду $F_q[x]/(x^{2^t}-a)$ та $F_q[x]/(x^{3^t}-a)$ без умови $q \equiv 1 (\mathrm{mod}\, m)$. Нижні межі для мультиплікативних порядків дорівнюють $\exp((\log m)^2)$, де $m = 2^t$ та $m = 3^t$ відповідно. У третьому підрозділі, покращуємо та узагальнюємо цей результат. Для будь-якого степеня розширення m, знімаємо умову подільності числа $q-1$ на m. Числа q, m та елемент a з початкового поля F_q припускаємо такими, що розширення $F_q[x]/(x^m-a)$ існує. Показуємо в лемі 4.6, що число m є добутком двох чисел m_1 та m_2, де m_1 є дільником $q-1$, а m_2 є порядком q за модулем m.

Розглядаємо довільне розширення вигляду $F_q[x]/(x^m-a)$, і явно будуємо в ньому елементи мультиплікативного порядку принаймні $2^{\lfloor \sqrt[3]{2m} \rfloor}$. Ідея полягає в наступному. Якщо число $q-1$ має великий дільник m_1, то використовуємо для побудови метод, аналогічний методу для розширень Куммера з другого підрозділу четвертого розділу. Якщо ж число $q-1$ не має великого дільника m_1, то число m_2 є великим, і використовуємо для побудови метод, аналогічний до методу для розширень на основі циклотомічних поліномів з другого розділу. Слід зауважити, що у випадку розширень Куммера спряжені лінійного бінома $\theta + b$ 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 побудови елементів великого порядку. Основним результатом третього підрозділу є така теорема, у формулюванні якої прослідковується описане комбінування підходів.

Теорема 4.4. *Нехай b – довільний ненульовий елемент поля F_q. Тоді елемент*

$$\gamma = \begin{cases} \theta + b, \text{ якщо } m_1 \le \lfloor \sqrt{2m_2} \rfloor, \\ \theta^{m_2} + b, \text{ якщо } m_1 > \lfloor \sqrt{2m_2} \rfloor \end{cases}$$

має в полі $F_q(\theta) = F_q[x]/(x^m - a)$ мультиплікативний порядок принаймні

$$\begin{cases} 2^{\lfloor \sqrt[3]{2m} \rfloor}, \text{ якщо } 2 \le m_1 < 869, \\ 2^{\lfloor \sqrt[3]{4m} \rfloor}, \text{ якщо } m_1 \ge 869. \end{cases}$$

У четвертому підрозділі підсилюємо нижню межу з використанням максимуму функції кількості розв'язків діофантового рівняння, а в п'ятому підрозділі – з використанням оцінки знизу для кількості розбиттів.

---

[11] J. F. Burkhart, N. J. Calkin, S. Gao, J. C. Hyde-Volpe, K. James, H. Maharaj, S. Manber, J. Ruiz, E. Smith, Finite field elements of high order arising from modular curves / Des. Codes Cryptogr. – 2009. – Vol. 51, no. 3. – P. 301–314.

У **п'ятому розділі** розглянуто побудову елементів великого мультиплікативного порядку в розширеннях скінченних полів вигляду $F_p[x]/(x^p - x - a)$ (на основі поліномів Артіна-Шраєра). Такі розширення існують для будь-якого простого числа p та довільного ненульового елемента a з початкового поля F_p.

У першому підрозділі в теоремі 5.1 явно будуємо елементи великого порядку в таких полях та даємо явну оцінку знизу на їх мультиплікативний порядок. При цьому використовуємо для побудови метод, аналогічний методу для розширень Куммера. Аналогія з розширеннями Куммера вказана без доведення та деталізації в праці[12].

Теорема 5.1. *Припустимо, що* $p \geq 41$. *Для будь-якого ненульового елемента* b *поля* F_p *елемент* $\theta + b$ *поля* F_{p^p} *має порядок більший, ніж* 4^p.

Також показуємо, що елемент θ має в F_{p^p} мультиплікативний порядок, який є дільником числа N_p. Використовуючи той факт, що числа $p-1$ та $N_p = (p^p - 1)/(p-1) = \sum_{i=0}^{p-1} p^i$ є взаємно простими, можна утворити елементи більшого порядку.

Наслідок 5.2. *Припустимо, що* $p \geq 41$. *Для будь-якого примітивного елемента* α *поля* F_p *та ненульового елемента* b *поля* F_p *елемент* $\alpha(\theta + b)$ *поля* F_{p^p} *має порядок більший, ніж* $(p-1) \cdot 4^p$.

У другому підрозділі розглядаємо з використанням комп'ютерних обчислень явну побудову деяких примітивних елементів у розширеннях Артіна-Шраєра. Наведений приклад показує, що отримана в першому підрозділі нижня межа для порядку є значно меншою від реальних мультиплікативних порядків елементів. Виникає припущення, що елемент θ має в скінченному полі F_{p^p} мультиплікативний порядок, рівний N_p. Припущення перевірено нами для певних значень простого числа p у середовищі комп'ютерної алгебри Maple. Використано відомі розклади числа N_p на прості множники, отримані в межах так званого Cunnigham проекту, щоб обчислити відповідні степені елемента θ.

Теорема 5.2. *Елемент* $\theta + i$, $i = 0,..., p-1$, *має в* F_{p^p} *мультиплікативний порядок, який дорівнює* N_p *для* $p < 126$ *та для* p=137,163,167,173.

---

[12] Cheng Q. Constructing finite field extensions with large order elements / Q. Cheng // SIAM J. Discrete Math. – 2007. – Vol. 21. – P. 726–730.

На підставі теореми 5.2, можна явно побудувати деякі примітивні елементи в розширеннях Артіна-Шраєра. Про ці результати йдеться в теоремі 5.3 та наслідку 5.3.

Теорема 5.3. *Всі примітивні елементи поля* F_{p^p} *можна записати у вигляді* $\alpha \cdot u$, *де* α *– примітивний елемент в* F_p, *а порядок елемента* u *дорівнює* N_p.

Наслідок 5.3. *Якщо* α *– примітивний елемент в* F_p *і елемент* θ *має в* F_{p^p} *мультиплікативний порядок* N_p, *то елемент* $\alpha(\theta+i)^j$ $(i=0,\ldots,p-1;\ j=1,\ldots,p-1)$ *– примітивний в* F_{p^p}.

У третьому підрозділі наводимо нижню межу для добутку біноміальних коефіцієнтів, пов'язаному з тестуванням простоти або побудовою елементів великого мультиплікативного порядку в розширеннях Куммера та розширеннях Артіна-Шраєра скінченних полів. Нехай m – натуральне число. Задача знаходження таких цілих чисел d_-, d $(0 \le d_- \le d < m)$, для яких добуток біноміальних коефіцієнтів

$$C(d_-,d)=\binom{m}{d_-}\binom{d}{d_-}\binom{2m-d_--d-1}{m-d-1}$$

є великим, виникає у двох наступних випадках.

1. Оптимізація алгоритму AKS тестування простоти великих натуральних чисел.

2. Згідно з підрозділом 4.2 маємо оцінку для розширень Куммера, а згідно з другим підрозділом цього розділу – аналогічну оцінку для розширень на основі поліномів Артіна-Шраєра, які вказують, що елементи вигляду $\theta+b$ мають мультиплікативний порядок принаймні

$$D=\max_{0\le d_-\le d<m} C(d_-,d)$$

для відповідних чисел d_-, d.

Основний результат третього підрозділу наведений в такій теоремі.

Теорема 5.6. *При* $m \ge 8$ *правильна наступна нижня межа:*

$$D > \frac{h^m}{30m^{3/2}},$$

де $h = 4\cdot 5^{5/4}/3^{3/2}$.

Отримана нижня межа для добутку біноміальних коефіцієнтів є точною величиною та порівняною із відповідним наближеним значенням із праці[13]. Виходячи із теореми 5.6, маємо наступний наслідок.

[13] Bernstein D. Proving primality in essentially quartic random time / D. Bernstein // Math. Comp. – 2007. – Vol. 76, no. 257. – P. 389–403.

Наслідок 5.2. *Для* $m \geq 8$ *виконується наступна нерівність:*

$$D > \frac{(5{,}7556)^m}{30m^{3/2}}.$$

У четвертому підрозділі отримано обмеження на можливі значення порядку елементів вигляду $\theta + b$ у розширеннях Артіна-Шраєра скінченних полів при умові, що цей порядок менший, ніж число N_p.

У **шостому розділі** вказуємо нижню межу для мультиплікативного порядку деяких елементів у рекурсивних розширеннях скінченних полів характеристики два, визначених Конвеєм[14] та Відеманом[15], а також у рекурсивних розширеннях скінченних полів характеристики більшої від двох.

З точки зору теорії скінченних полів, поля скінченних номерів, введені Конвеєм, зручніше описувати в термінах послідовних розширень попередніх полів з використанням нерозкладних поліномів. Зокрема, так ці поля описано в праці Відемана, і цей підхід використано в першому та другому підрозділах цієї роботи. Більш точно, ми розглядаємо наступні скінченні поля, ізоморфні полям номерів:

$$c_{-1} = 1,\ L_{-1} = F_2(c_{-1}) = F_2;$$

для $i \geq -1,\ L_{i+1} = L_i(c_{i+1})$, де елемент c_{i+1} задовольняє рівняння

$$c_{i+1}^2 + c_{i+1} + \prod_{j=-1}^{i} c_j = 0.$$

Будемо позначати числа Ферма $N_j = 2^{2^j} + 1$ ($j \geq 0$). Наступна теорема описує властивість елементів c_i, які задають послідовні розширення полів у вежі Конвея: при послідовному піднесенні до степенів чисел Ферма не пропускати чергове поле.

Теорема 6.1. *При* $i \geq 2$, *правильна така умова:* $(c_i)^{\prod_{j=0}^{k} N_{i-j}} \in L_{i-k-1} \setminus L_{i-k-2}$ *для* $0 \leq k \leq i-1$.

Будемо при $k \geq 0$ використовувати позначення $a_k = \prod_{j=0}^{k} c_j$. Уведені елементи a_i володіють властивістю, аналогічною до властивості елементів c_i.

Теорема 6.2. *При* $i \geq 2$, *справедлива така умова:* $(a_i)^{\prod_{j=0}^{k} N_{i-j}} \in L_{i-k-1} \setminus L_{i-k-2}$ *для* $0 \leq k \leq i-1$.

Використовуючи доведені властивості елементів c_i та a_i, отримано вирази для мультиплікативних порядків цих елементів.

---

[14] Conway J.H. On Numbers and Games / J.H. Conway – New York: Academic Press, 1976. – 238 p.

[15] Wiedemann D. An iterated quadratic extension of GF(2) / D. Wiedemann // Fibonacci Quart. – 1988. – Vol. 26, no. 4. – P. 290–295.

Теорема 6.3. *При* $i \geq 2$, *правильні такі рівності:*

(a) $\operatorname{ord} c_i = \prod_{j=1}^{i} \alpha_j$, *де число* α_j *ділить* N_j, $\alpha_j > 1$;

(b) $\operatorname{ord} a_i = \prod_{j=1}^{i} \beta_j$, *де число* β_j *ділить* N_j, $\beta_j > 1$.

Описано певне обмеження на порядок елементів c_i у відповідній фактор-групі.

Теорема 6.4. *Припустимо, що* $i \geq 1$. *Якщо* m_i *– найменше натуральне число з властивістю* $(c_i)^{m_i} \in K_{i-1}$ *та* $m_i = 2^k + 1$, *то* $k = 2^i$.

На підставі теореми 6.4, в наслідку 6.2 наводимо нижню межу для мультиплікативного порядку розглянутих раніше елементів у двійкових рекурсивних розширеннях скінченних полів, визначених Конвеєм.

Наслідок 6.2. *Мультиплікативний порядок елементів* c_i *та* a_i *дорівнює* $\prod_{j=1}^{i} N_j$ *для* $1 \leq i \leq 4$ *та має значення принаймні* $\prod_{j=1}^{4} N_j \cdot \prod_{j=5}^{i} (3 \cdot 2^{j+2} + 1)$ *для* $i \geq 5$.

Раніше не були відомі ніякі нетривіальні нижні межі для порядків елементів у вежах Конвея. Наш результат дає такі межі.

Безпосередня перевірка показує: елемент c_0 примітивний в L_0, а елемент c_1 примітивний в L_1. Разом з тим Х. Ленстра довів: якщо $i \geq 2$, то елемент c_i не є примітивним у полі L_i. Деякі примітивні елементи для L_2, L_3 та L_4 знайдені Л. Бруіном з використанням середовища SageMath. Покращуючи ці результати, у другому підрозділі описуємо деякі примітивні елементи для перших дванадцяти полів у вежах Конвея. Для цього спочатку даємо формулювання, яке вказує, що при виконанні певної умови порядки елементів c_i та a_i є максимально можливими.

Теорема 6.5. *Нехай* $i \geq 5$. *Якщо для всіх* $5 \leq j \leq i$ *виконується умова:*

$\alpha_j = N_j$ *– найменше натуральне число, що задовольняє співвідношення* $(c_j)^{\alpha_j} \in L_{j-1}$,

то $\operatorname{ord} a_i = \operatorname{ord} c_i = \prod_{j=1}^{i} N_j$.

Отримуємо наслідок, який показує, що при виконанні умови з теореми 6.5 елементи $c_i c_0$ та $a_i a_0$, які виникають завдяки домноженню відповідно елементів c_i та a_i на $c_0 = a_0$ є примітивними.

Наслідок 6.3. *Нехай* $i \geq 5$. *Якщо для всіх* $5 \leq j \leq i$ *виконується умова:*

$\alpha_j = N_j$ *– найменше натуральне число, що задовольняє співвідношення* $(c_j)^{\alpha_j} \in L_{j-1}$,

то елемент $c_i c_0$ *та елемент* $a_i a_0$ *є примітивними.*

Використовуючи відомі розклади перших дванадцяти чисел Ферма на прості множники та комп'ютерні обчислення, здійснено перевірку умови із теореми 6.5.

Теорема 6.6. *При* $5 \le j \le 11$, *число* $\alpha_j = N_j$ *є найменшим натуральним числом, для якого виконується співвідношення* $(c_j)^{\alpha_j} \in L_{j-1}$.

Як наслідок із теореми 6.6 маємо, що при $5 \le i \le 11$ порядки елементів c_i та a_i є максимально можливими. Також, на основі цього результату, отримуємо, що при $5 \le i \le 11$ елементи $c_i c_0$ та $a_i a_0$, є примітивними.

Наслідок 6.4. *При* $2 \le i \le 11$, *мультиплікативний порядок елемента* c_i *та елемента* a_i *дорівнює* $\prod_{j=1}^{i} N_j$.

Наслідок 6.5. *При* $2 \le i \le 11$, *елемент* $c_i c_0$ *та елемент* $a_i a_0$ *є примітивними.*

Таким чином, одержаний нами результат описує певні примітивні елементи у перших дванадцяти полях у вежі Конвея. Більш того, наслідок 6.3 дає умову, при виконанні якої елементи цього вигляду є примітивними для всіх полів у вежі.

У третьому підрозділі наводимо нижню межу для мультиплікативного порядку деяких елементів у двійкових рекурсивних розширеннях скінченних полів, визначених Відеманом. Більш точно, розглядаємо наступні скінченні поля, визначені Відеманом, які будують рекурсивно:

$$x_{-1} = 1, E_{-1} = F_2(x_{-1}) = F_2;$$

для $i \ge -1$, $E_{i+1} = E_i(x_{i+1})$, де x_{i+1} задовольняє рівняння

$$x_{i+1}^2 + x_{i+1} x_i + 1 = 0.$$

Цей підрозділ пов'язаний з відкритим питанням, поставленим Відеманом. Недоведена на сьогодні гіпотеза Відемана полягає в такому: порядок $\operatorname{ord} x_i$ елемента x_i завжди дорівнює N_i. Якщо це так, то $u_r = \prod_{i=0}^{r} x_i$ є примітивним елементом у E_r для будь-якого r. У цьому разі порядок елемента u_r дорівнює добутку $\prod_{i=0}^{r} N_i$.

При цьому доводимо твердження, які накладають обмеження на можливі значення порядку елемента x_i: описуємо деякі власні дільники чисел Ферма N_i, які не дорівнюють мультиплікативному порядку $\operatorname{ord} x_i$. Ці формулювання можуть мати й самостійне значення.

Теорема 6.7. *Порядок* $\operatorname{ord} x_i$ $(i \ge 0)$ *не може бути дільником числа вигляду* $2^k + 1$, *де* k *– натуральне число та* $k < 2^i$.

Теорема 6.8. *Порядок* $\operatorname{ord} x_i$ $(i \geq 0)$ *не може бути дільником числа вигляду* $s \cdot 2^k + 1$, *де* $s = 3,5$ *та* k *– невід'ємне ціле число.*

Основним результатом третього підрозділу є теорема 6.9. При її доведенні використовуємо теореми 6.7 та 6.8, комп'ютерні обчислення й відомі розклади перших дванадцяти чисел Ферма на прості множники. Зокрема, показано, що для $0 \leq i \leq 11$ мультиплікативний порядок $\operatorname{ord} x_i = N_i$, тобто є максимально можливим.

Теорема 6.9. *Порядок елемента* x_i *дорівнює* N_i *для* $0 \leq i \leq 11$ *та є принаймні* $7 \cdot 2^{i+2} + 1$ *для* $i \geq 12$.

Оскільки числа Ферма є попарно взаємно простими, то можемо визначити мультиплікативний порядок елемента u_r.

Наслідок 6.6. *Порядок елемента* $u_r = \prod_{i=0}^{r} x_i$ *дорівнює* $\prod_{i=0}^{r} N_i$ *для* $0 \leq r \leq 11$ *та є принаймні* $\prod_{i=0}^{11} N_i \cdot \prod_{i=12}^{r} (7 \cdot 2^{i+2} + 1)$ *для* $r \geq 12$.

У праці[16] отримано оцінку для порядку елементів у наведеній вежі, а саме $\exp(2^{2^i \delta})$, де δ – абсолютна константа. Проте, значення константи невідоме. Наша межа не залежить ні від якої невідомої константи.

Четвертий та п'ятий підрозділи присвячено отриманню нижніх меж для порядку елементів у вежах скінченних полів недвійкової характеристики. Раніше не були відомі ніякі нетривіальні нижні межі для порядків елементів у цьому випадку.

У четвертому підрозділі ми явно будуємо у вежах скінченних полів недвійкової характеристики елементи великого мультиплікативного порядку. Більш точно, явно будуємо елементи великого порядку в недвійкових ($p \geq 3$) рекурсивних розширеннях скінченних полів $F_{p^{p^r}}$, даючи оцінку знизу на їх мультиплікативний порядок. Різні варіанти таких розширень, зокрема, розглядалися низкою авторів (Х. Ітo, Т. Каджівара, Х. Сонг) з точки зору ефективного виконання в них операцій додавання та множення.

Розглядаємо скінченні поля, які будують рекурсивно:

$E_1 = F_p(x_1)$, де x_1 задовольняє рівняння $x_1^p - x_1 - 1 = 0$;

$E_r = E_{r-1}(x_r)$, $r = 2,3,...$, де x_r задовольняє рівняння

$$x_r^p - x_r - \prod_{i=0}^{r-1} x_i^{p-1} = 0.$$

Як вже було сказано раніше при розгляді результатів із підрозділу 5.1, поліном $\mathrm{x}_1^{\mathrm{p}} - \mathrm{x}_1 - 1$ є нерозкладним над полем F_p. Поліном $x_r^p - x_r - \prod_{i=0}^{r-1} x_i^{p-1}$ є нерозкладним

[16] Voloch J.F. Elements of high order on finite fields from elliptic cures / J.F. Voloch // Bull. Austral. Math. Soc. – 2010. – Vol. 81, no. 3. – P. 425–429.

над полем E_r, на основі праці[2]. Тобто, у результаті отримуємо таку вежу скінченних полів недвійкової характеристики:

$$F_p \subset E_1 = F_p(x_1) \subset E_2 = E_1(x_2) \subset \ldots$$

Зауважимо, що число елементів мультиплікативної групи E_r^* $(r = 1,2,\ldots)$ дорівнює величині $p^{p^r} - 1$. Для довільних простого числа p та натурального числа r вводимо числа наступного вигляду $N_{p,r} = \dfrac{p^{p^r} - 1}{p^{p^{r-1}} - 1}$. З одного боку їх можна розглядати як узагальнення чисел Ферма $N_{2,r} = \dfrac{2^{2^r} - 1}{2^{2^{r-1}} - 1} = 2^{2^{r-1}} + 1$, а з іншого боку – як узагальнення чисел вигляду $N_{p,1} = \dfrac{p^p - 1}{p - 1}$, які виникають у п'ятому розділі при розгляді порядків елементів у розширеннях Артіна-Шраєра. У цьому разі справедлива рівність: $N_{p,r} = \sum_{i=0}^{p-1} (p^{p^{r-1}})^i$. Наступна теорема є узагальненням відомих результатів про можливі прості дільники чисел Ферма та чисел $N_{p,1}$.

Теорема 6.10. *Нехай p – непарне просте число. Тоді будь-який простий дільник числа $N_{p,r}$ має вигляд $2kp^r + 1$ для деякого натурального числа k.*

Користуючись теоремою 6.10, в теоремі 6.11 отримано нижню межу для порядків елементів x_i, які задають розширення у недвійковій вежі.

Теорема 6.11. *Нехай r - довільне натуральне число. Елемент $u_r = \prod_{i=1}^{r} x_i$ поля E_r має мультиплікативний порядок принаймні $\prod_{i=1}^{r} (2p^i + 1)$.*

У п'ятому підрозділі розглядаємо частковий випадок вежі, введеної в четвертому підрозділі, а саме вежі, що складається з трьох скінченних полів, які будуємо рекурсивно:

$E_1 = F_p(x)$, де $p \geq 3$ та x задовольняє рівняння $x^p - x - 1 = 0$;

$E_2 = E_1(y)$, де y задовольняє рівняння $y^p - y - x^{p-1} = 0$.

Тобто, отримуємо таку вежу скінченних полів недвійкової характеристики:

$$F_p \subset E_1 = F_p(x) \subset E_2 = E_1(y).$$

У цьому частковому випадку вежі з трьох полів описано спряжені елемента y над полем F_p. Ці спряжені є лінійними поліномами від формальної змінної y.

Теорема 6.12. *Спряжені* y^{p^i} $(i = 0,1,..., p^2 - 1)$ *елемента* y *над* F_p *мають вигляд:*

$$y^{p^i} = y + u\sum_{k=0}^{s}(x+k)^{p-1} + v\sum_{l=s+1}^{p-1}(x+l)^{p-1},$$

де $u = v = 0$ *або* $u \equiv v + 1 \pmod p$, $0 \le s \le p-1$.

Виходячи з опису спряжених елемента y, отримуємо такий основний результат п'ятого підрозділу, який сформульовано в теоремі 6.13.

Теорема 6.13. *Елемент* y *поля* $F_{p^{p^2}}$ *має порядок більший, ніж величина* $\dfrac{p^p - 1}{p-1}$.

Таким чином, для часткового випадку $r = 2$, маємо кращий результат, ніж у загальному випадку.

У **сьомому розділі** вказуємо нижню межу для мультиплікативного порядку деяких елементів у загальних розширеннях скінченних полів як на основі певної правдоподібної, але поки що недоведеної гіпотези, так і без використання вказаної гіпотези. Також вивчаємо зв'язок між елементами великого порядку та доведенням простоти великих натуральних чисел.

В першому підрозділі розглянуто побудову елементів великого порядку в скінченних полях загального вигляду на основі гіпотези С. Гао. Підхід С. Гао спирається на висловлену ним гіпотезу, яка стверджує таке: для довільного цілого числа n існує такий поліном $g(x) \in F_q[x]$ степеня d (найближче більше ціле число до $2\log_q n$), що поліном $x^m - g(x)$ має нерозкладний дільник $f(x)$ степеня n, де m – найменший степінь числа q, який більший або дорівнює числу n. Поліном $x^m - g(x)$, який фігурує в гіпотезі, аналогічний до полінома Куммера $x^m - a$. Розширення на основі поліномів Куммера розглянуто нами в четвертому розділі. Лише замість константи (елемента a початкового поля F_q) в гіпотезі С. Гао маємо поліном $g(x)$ невеликого степеня (степінь якого у вказаній гіпотезі обмежено величиною $2\log_q n$). Поліном $f(x)$, який породжує розширення початкового поля F_q, є дільником полінома $x^m - g(x)$.

Нами вдосконалено підхід С. Гао та його модифікацію А. Конфлітті за рахунок більш вдалого визначення множини, що дозволяє утворювати попарно різні степені елемента θ, який задає розширення початкового скінченого поля.

Теорема 7.1. *Візьмемо* d *– найближче більше ціле число до величини* $2\log_q n$, t *– найближче менше ціле число до величини* $\log_d n$. *Тоді елемент* θ *має в полі* $F_q(\theta) = F_{q^n} = F_q[x]/f(x)$ *мультиплікативний порядок принаймні*

$$\binom{n+t-1}{t}\prod_{i=0}^{t-1}\frac{1}{d^i}.$$

Отримана нами нижня межа покращує результат Гао-Конфлітті, оскільки відношення R нашої нижньої межі до відомої межі дорівнює $R = \prod_{i=1}^{t-1} \frac{n+i}{n} \cdot \frac{t}{i}$ і завжди більше від одиниці.

У другому підрозділі побудовано елементи великого порядку в скінченних полях загального вигляду без використання гіпотези Гао. Основні результати другого підрозділу – теорема 7.5 та теорема 7.7.

Теорема 7.5. *Нехай скінченне поле має вигляд* $F_{q^n} = F_q[x]/(x^n + x + a)$. *Тоді елемент* θ *має мультиплікативний порядок принаймні* $\frac{(n-1)n}{2}$.

Для отримання нижньої межі в теоремі 7.7, застосовуємо наслідок із ABC теореми Стовера–Мейсона для поліномів.

Теорема 7.7. *Нехай скінченне поле має вигляд* $F_{q^n} = F_q[x]/(x^n + x + a)$ *та* $p \geq 3n-1$. *Тоді елемент* θ *має мультиплікативний порядок принаймні*

$$\frac{(2n-1)(n-1)}{2}.$$

Останній підрозділ присвячений вивченню зв'язку між елементами великого порядку та доведенням простоти великих натуральних чисел. Прості числа мають фундаментальне значення в математиці в цілому: є небагато краще відомих або простіших для розуміння проблем в абстрактній математиці, ніж питання швидкого визначення є дане число простим чи складеним. Ефективні тести простоти також необхідні в прикладних застосуваннях: у низці криптографічних протоколів використовують великі прості числа.

У 2002 р. М. Агравал, Н. Кайал, Н. Саксена запропонували детермінований поліноміальний алгоритм AKS, який визначає: є вхідне число n простим чи складеним. Доведено, що AKS виконується за час $(\log n)^{7.5+o(1)}$. Х. Ленстра та К. Померанс вказали суттєво змінену версію AKS з часом виконання $(\log n)^{6+o(1)}$. Відомі також імовірнісні варіанти AKS з часом виконання $(\log n)^{4+o(1)}$. Для подальшого покращення оцінки часу виконання було запропоновано наступну гіпотезу: якщо r – просте число, яке не ділить n, та якщо $(X-1)^n = X^n - 1 \pmod{n, X^r - 1}$, то або n – просте або справедливе порівняння $n^2 \equiv 1 \pmod{r}$.

Якщо ця гіпотеза, яку часто називають гіпотезою Агравала, виявиться справедливою, то це покращить оцінку часу виконання алгоритму AKS до $(\log n)^{3+o(1)}$. Х. Ленстра та К. Померанс дали евристичний аргумент, який припускає, що наведена гіпотеза хибна. Проте, М. Агравал, Н. Кайал, Н. Саксена зауважили, що певний варіант гіпотези може все ж бути правильним (наприклад, якщо покладаємо $r > \log n$).

Ідея алгоритму AKS полягає в такому: показати, що множина елементів вигляду $X + a$, де a – цілі числа, породжує "достатньо велику" підгрупу відповідної мультиплікативної групи скінченого поля. З цієї точки зору можна трактувати гіпотезу Аггравала в такий спосіб. Якщо рівність

$$(X-1)^n = X^n - 1 \,(\mathrm{mod}\, n, X^r - 1)$$

виконується, то множина, що складається лише з одного елемента $X - 1$, породжує достатньо велику підгрупу.

Наведені далі дві теореми описують можливі підходи до побудови контрприкладів для гіпотези Аггравала. У цьому разі користуємось китайською теоремою про залишки. Вона встановлює ізоморфізм між кільцем $Z_n[X]/\Phi_r(X)$, у якому розглядаємо рівність із гіпотези, та прямим добутком кілець $\prod_{i=1}^{k} Z_{p_i}[X]/\Phi_r(X)$. Усі фактор-кільця із добутку є полями, оскільки кожне просте число p_i примітивне за модулем r. Це спрощує розгляд відповідних рівностей.

Теорема 7.8. *Нехай $p_1,...,p_k$ – попарно різні прості числа, $n = p_1...p_k$, r – просте число, число p_i примітивне за модулем r для $i = 1,...,k$. Якщо для кожного $i = 1,...,k$ існує таке ціле число a_i, що*

$$n \equiv p_i^{a_i} \bmod 2r\left(\left(p_i\right)^{\frac{r-1}{2}} - 1\right),$$

то

$$(X-1)^n = X^n - 1 \,(\mathrm{mod}\, n, X^r - 1).$$

Застосовуючи теорему 7.8 для випадку $r = 5$, отримуємо наступну теорему.

Теорема 7.9. *Нехай $p_1,...,p_k$ – попарно різні прості числа і нехай $n = p_1...p_k$. Припустимо, що справедливі такі умови:*

(1) *k – непарне число;*

(2) *$p_i (\mathrm{mod}\, 5) \in \{2,3\}$ для $i = 1,...,k$;*

(3) *$p_1 (\mathrm{mod}\, 16) \in \{3,5,11,13\}$ та для $i = 2,...,k$ виконується: якщо $p_i \equiv p_1 (\mathrm{mod}\, 5)$, то $p_i \equiv p_1 (\mathrm{mod}\, 16)$, в іншому разі $p_i \equiv p_1^3 (\mathrm{mod}\, 16)$;*

(4) *$p_i - 1$ ділить $n - 1$ для $i = 1,...,k$;*

(5) *$p_i + 1$ ділить $n + 1$ для $i = 1,...,k$.*

Тоді $(X-1)^n = X^n - 1 \,(\mathrm{mod}\ n, X^5 - 1)$ та $n^2 \equiv 1 (\mathrm{mod}\, 5)$.

Отриманий раніше Х. Ленстра результат є частковим випадком доведеної нами теореми 7.9. Згідно з цією теоремою маємо евристику, яка припускає існування багатьох контрприкладів для гіпотези Аггравала у випадку $r = 5$. Виходячи з попередньої теореми, можна будувати контрприклади також при $r > 5$. Зокрема, гіпотезу перевірено М. Аггравалом, Н. Кайалом, Н. Саксеною для чисел $r < 100$ та $n < 10^{10}$. Також гіпотезу перевірено нами з використанням комп'ютерних обчислень

для випадку $r=5$ та $10^{100}<n<10^{100}+10^5$. Проте ні один контрприклад поки що не знайдено.

Наведені далі формулювання дозволяють пов'язати із гіпотезою Аграваля певний ланцюг підгруп відповідної мультиплікативної групи скінченного поля.

Теорема 7.10. *Якщо справедливе співвідношення*

$$(X-1)^n = X^n - 1 \,(\mathrm{mod}\, n, X^r - 1),$$

то

$$\langle X \rangle \subset \langle X+1 \rangle \subset \langle X-1 \rangle$$

є строго зростаючим ланцюгом підгруп групи $(Z_p[X]/(X^{r-1}+...+X+1))^*$ *для будь-якого простого дільника* p *числа* n.

Теорема 7.11. *Якщо* p *– просте число та* $a \neq 0,1,-1 \,(\mathrm{mod}\ p)$, *то* $X+a \notin \langle X-1 \rangle$ *в групі* $(Z_p[X]/(X^{r-1}+...+X+1))^*$.

Отже, на підставі теореми 7.10 та теореми 7.11, маємо такий строго зростаючий ланцюг підгруп:

$$\langle X \rangle \subset \langle X+1 \rangle \subset \langle X-1 \rangle \subset \langle X-1, X+2 \rangle.$$

Більш того, для $r=5$ справедлива наступна теорема.

Теорема 7.12. *Якщо просте число* p *не дорівнює 2, 3, 5, 11, 19 та* $p^2 \neq 1 \,(\mathrm{mod}\, 5)$, *то порядок елемента* $X+2$ *в полі* $Z_p[X]/(X^5+X^4+X^3+X^2+X+1)$ *не ділить число* $10(p^2-1)$.

Таким чином, нами пов'язано із задачею тестування простоти великих натуральних чисел певний ланцюг підгруп мультиплікативної групи скінченного поля. Доведені теореми 7.10, 7.11 та 7.12 дозволяють припустити, що такий варіант гіпотези Аграваля може бути правильним: якщо r – просте число, яке не ділить n, якщо $(X-1)^n = X^n - 1 \,(\mathrm{mod}\, n, X^r - 1)$ і якщо $(X+2)^n = X^n + 2 \,(\mathrm{mod}\, n, X^r - 1)$, то або n – просте число або $n^2 \equiv 1 \,(\mathrm{mod}\, r)$. Модифікована гіпотеза означає, що множина $\{X-1, X+2\}$ утворює достатньо велику підгрупу відповідної групи.

Спираючись на результати із третього розділу, нами отримано експоненційні нижні межі для порядків підгруп, пов'язаних з гіпотезою Аграваля. Раніше не були відомі ніякі нетривіальні нижні межі для порядків підгруп у цьому ланцюгу. Перші дві підгрупи породжені одним елементом, а третя – двома елементами.

Наслідок 7.1. *Виконується наступна нерівність:*

$$|\langle X+1 \rangle| > \frac{r}{13(r-2)} \exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right).$$

Наслідок 7.2. *Справедлива наступна нерівність:*

$$|\langle X-1 \rangle| > \frac{2r}{13(r-2)} \exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right).$$

Теорема 7.13. *Правильна така нижня оцінка для мультиплікативного порядку підгрупи* $\langle X-1, X+2\rangle$:

$$|\langle X-1, X+2\rangle| > \frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot(1+\frac{\sqrt{2}}{2})\sqrt{r-3}\right)}{169(r-2)(r-3)}.$$

ВИСНОВКИ

У дисертації досліджено мультиплікативні порядки елементів у мультиплікативних групах скінчених полів. Отримано в явному вигляді елементи скінченних полів та нижні межі для цих порядків. Результати дисертації мають теоретичний характер. Їх можна використати при явній побудові елементів великого мультиплікативного порядку в скінченних полях при подальшому дослідженні скінченних полів. Такі елементи також можуть бути корисними в прикладних застосуваннях, зокрема криптографії та завадостійкому кодуванні.

У дисертації одержані наступні нові результати.

У розширеннях скінченних полів на основі циклотомічних поліномів (вигляду $F_q[x]/(x^{r-1}+..+x+1)$, де q є степенем простого числа p та примітивним за модулем числа r) для елементів більш загального вигляду, ніж гауссовий період, отримано явну експоненційну нижню межу для порядку цих елементів: кращу, ніж відома раніше для гауссового періоду. Такі розширення існують для нескінченної кількості чисел r, якщо для числа q виконується гіпотеза Артіна. 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 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. Також одержано асимптотичні нижні межі для мультиплікативних порядків елементів.

У 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. Розглядаємо довільне розширення вигляду $F_q[x]/(x^m-a)$, і явно будуємо в ньому елементи мультиплікативного порядку принаймні $2^{\lfloor\sqrt[3]{2m}\rfloor}$. Ідея

полягає в наступному: якщо $q-1$ має великий дільник m_1, то використовуємо для побудови 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 використовуємо 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. Власне у цій ситуації ефективним є запропонований метод комбінування двох підходів. Підсилено вказану нижню межу з використанням максимуму функції кількості розв'язків діофантового рівняння або з використанням оцінки знизу для кількості розбиттів.

У розширеннях скінченних полів на основі поліномів Артіна-Шраєра (вигляду $F_{p^p} = F_p[x]/(x^p - x - a)$) збудовано в явному вигляді елементи великого (експоненційного) порядку та дано також явну оцінку знизу на їх мультиплікативний порядок рівну 4^p. 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.

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 від два. У частковому випадку вежі з двох полів описано спряжені елемента, який задає друге розширення, над початковим полем, що дозволило отримати сильнішу нижню межу, ніж у загальному випадку.

Підсилено нижню межу для мультиплікативного порядку деяких елементів у загальних розширеннях скінченних полів як на основі певної правдоподібної, але поки що недоведеної 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 Агравала. 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.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Попович Р. Елементи великого порядку в розширеннях Артіна-Шраєра скінченних полів / Р. Попович // Математичні студії. – 2013. – Т. 39, № 2. – С. 115–118.
2. Попович Р. Про елементи великого порядку в розширеннях скінченних полів на основі поліномів Куммера / Р. Попович // Наук. вісник Ужгород. ун-ту, серія матем. і інф. – 2013. – Т. 24, № 1. – С. 139–144.
3. Попович Р. Покращення нижньої оцінки для порядку елементів одного класу скінченних полів / Р. Попович // Математичний вісник НТШ. – 2013. – Т. 10. – С. 39–44.
4. Попович Р. Про оцінки для мультиплікативних порядків елементів скінченних полів на основі циклотомічних поліномів / Р. Попович // Вісник НУ Львів. політех., фіз.-мат. науки. – 2013. – № 768. – С. 59–62.
5. Попович Р. Побудова елементів великого порядку в скінченних полях загального вигляду / Р. Попович // Прикладні проблеми механіки і математики, ІППММ АН України. – 2013. – Т. 11. – С. 85–89.
6. Попович Р. Нижня межа для порядку елементів в розширеннях скінченних полів вигляду F_{p^p} / Р. Попович // Вісник Львів. ун-ту, серія мех.-мат. – 2013. – № 78. – С. 141–147.
7. Попович Р. Нижня оцінка мультиплікативного порядку елементів у вежах скінченних полів характеристики $p \geq 3$ / Р. Попович // Наук. вісник Ужгород. ун-ту, серія матем. і інф. – 2014. – Т. 25, № 1. – С. 120–123.
8. Попович Р. Про підгрупи мультиплікативної групи одного класу скінченних полів / Р. Попович // Вісник НУ Львів. політех., фіз.-мат. науки. – 2014. – № 804. – С. 108–111.
9. Попович Р. Про ізоморфізм скінченних полів характеристики два / Р. Попович // Математичний вісник НТШ. – 2014. – Т. 11. – С. 12–20.
10. Попович Р. Елементи великого порядку в одній вежі скінченних полів / Р. Попович // Наук. вісник Ужгород. ун-ту, серія матем. і інф. – 2014. – Т. 26, № 2. – С. 178–183.
11. Попович Р. Обмеження на порядок елементів у вежах Конвея скінченних полів / Р. Попович // Прикладні проблеми механіки і математики, ІППММ АН України. – 2015. – Т. 13. – С. 53–57.
12. Попович Р. Нижня межа для мультиплікативного порядку елементів у розширеннях Куммера скінченних полів / Р. Попович // Вісник Львів. ун-ту, серія мех.-мат. – 2015. –№ 80. – С. 134–139.
13. Попович Р. Деякі примітивні елементи для розширень Артіна-Шраєра скінченних полів / Р. Попович // Український математичний вісник. – 2015. – Т. 12, № 1. – С. 86–96. (Переклад: Popovych R. B/ Some primitive elements for the Artin–Schreier extensions of finite fields / R. B. Popovych // J. Math. Sci. – 2015. – Vol. 210, no. 1. – P. 67–75).
14. Popovych R. Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$ / R. Popovych // Finite Fields Appl. – 2012. – Vol. 18, no. 4. – P. 700–710.

15. Popovych R. Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$ / R. Popovych // Finite Fields Appl. – 2013. – Vol. 19, no. 1. – P. 86–92.
16. Popovych R. Lower bounds on the orders of subgroups connected with Agrawal conjecture / R. Popovych // Carpathian mathematical publications – 2013. – Vol. 5, no. 2. – P. 310–314.
17. Popovych R. Sharpening of explicit lower bounds on elements order for finite field extensions based on cyclotomic polynomials / R. Popovych // Український математичний журнал – 2014. – Vol. 66, no. 6. – P. 815–825.
18. Popovych R. On elements of high order in general finite fields / R. Popovych // Algebra and Discrete Mathematics – 2014. – Vol. 18, no. 2. – P. 295–300.
19. Popovych R. Lower bound on product of binomial coefficients / R. Popovych // Buletinul Academiei de Ştiinţe a Republicii Moldova. Matematica – 2015. – Vol. 78, no. 2. – P. 21–26.
20. Popovych R. On the multiplicative order of elements in Wiedemann's towers of finite fields / R. Popovych // Carpathian mathematical publications – 2015. – Vol. 7, no. 2. – P. 220–225.
21. Попович Р. Деякі зауваження відносно реалізації AKS тесту простоти / Р. Попович // Вісник НУ Львів. політех., комп'ютерні системи та мережі. – 2006. –№ 573. – С. 157–160.
22. Попович Р. Удосконалення алгоритму AKS доведення простоти цілих чисел / Р. Попович // Вісник НУ Львів. політех., комп'ютерні системи та мережі. – 2007. –№ 603. – С. 112–116.
23. Popovych R. A note on Agrawal conjecture / R. Popovych // Second Workshop on Mathematical Cryptology (October 23-25, 2008, Santander, Spain): book of extended abstr. – Santander, 2008. – P. 125-127.
24. Popovych R. Elements of high order in finite field / R. Popovych // 8th International Algebraic Conference in Ukraine (5–12 липня 2011 р., Луганськ): зб. тез доп. – Луганськ, 2011. – С. 73.
25 Popovych R. Elements of high order in finite field extensions based on Kummer polynomials / R. Popovych // International Mathematical Conference devoted to the 70 year anniversary of Prof. Vladimir Kirichenko (13–19 червня 2012 р., Миколаїв): зб. тез доп. – Миколаїв, 2012. – С. 40.
26. Popovych R. Large order elements in Artin-Schreier extensions of finite fields / R. Popovych // International Conference on Algebra dedicated to 100th anniversary of S.M. Chernikov (20–26 серпня 2012 р., Київ): зб. тез доп. – Київ, 2012. – С. 117.
27. Popovych R. On Agrawal conjecture / R. Popovych, B. Popovych // International Conference dedicated to 120th anniversary of S. Banach (17–21 вересня 2012 р., Львів): зб. тез доп. – Львів, 2012. – С. 261.
28. Popovych R. Sharpening of explicit lower bounds on elements order for finite field extensions $F_q[x]/\Phi_r(x)$ / R. Popovych // 9th International Algebraic Conference in Ukraine (8–13 липня 2013 р., Львів): зб. тез доп. – Львів, 2013. – С. 147.
29. Popovych R. Construction of high order elements in finite fields based on Kummer polynomials / R. Popovych // International Scientific Conference "Modern

Problems of Mechanics and Mathematics" (21–25 травня 2013 р., Львів): зб. доп. – Т.3, Львів, 2013. – С. 213–215.
30. Popovych R. Construction of high order elements in finite fields based on Kummer polynomials / R. Popovych // International algebraic conference dedicated to 100th anniversary of L.A. Kaluzhnin (7–12 липня 2014 р., Київ): зб. тез доп. – Київ, 2014. – С. 68.
31. Popovych R. Multiplicative orders of elements in towers of finite fields of characteristic two / R. Popovych // 10th International Algebraic Conference in Ukraine (20–27 серпня 2015 р., Одеса): зб. тез доп. – Одеса, 2015. – С. 90.
32. Popovych R. Improvement to AKS algorithm of big integers primality proving / R. Popovych // 3rd int. conf. "Advanced Computer Systems and Networks: Design and application" (20–22 вересня 2007 р., Львів): зб. доп. – Львів, 2007. – P.146 -148.

АНОТАЦІЯ

Попович Р. Б. *Елементи великого мультиплікативного порядку в скінченних полях*. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора фізико-математичних наук за спеціальністю 01.01.06 – алгебра та теорія чисел. – Інститут математики НАН України, Київ, 2016.

Дисертаційна робота присвячена дослідженню порядків елементів у мультиплікативних групах скінчених полів та отриманню в явному вигляді нижніх меж для цих порядків. У розширеннях скінченних полів на основі циклотомічних поліномів для елементів більш загального вигляду, ніж гауссовий період, отримано явну нижню межу для порядку: кращу, ніж відома раніше для гауссового періоду. Це дало відповідь на відкрите питання О. Ахмаді, І. Шпарлінскі та Ж. Волоха. Виведено, використовуючи результати з теорії розбиттів, нижні межі в термінах характеристики поля та степеня розширення. У розширеннях на основі поліномів Куммера одержано експоненційну нижню межу: знято умову подільності кількості елементів мультиплікативної групи на степінь розширення. У розширеннях на основі поліномів Артіна-Шраєра побудовано елементи великого порядку та вказано явну оцінку знизу на цей порядок. Отримано нижню межу для порядку у вежах Конвея. Знайдено певні примітивні елементи для перших дванадцяти полів у цих вежах. Сформульовано умову, за якої елементи такого вигляду є примітивними у всіх полях у вежах Конвея. Одержано нижню межу для порядку у вежах Відемана. Знайдено нижні межі для веж полів характеристики більшої, ніж два. Підсилено нижню межу у загальних розширеннях скінченних полів. Вивчено зв'язок між елементами великого порядку та доведенням простоти великих натуральних чисел.

Ключові слова: скінченне поле, примітивний елемент, мультиплікативний порядок, нижня межа, циклотомічний поліном, поліном Куммера, поліном Артіна-Шраєра, рекурсивні розширення, вежа полів, тестування простоти, комп'ютерні обчислення, розбиття.

ABSTRACT

Popovych R. B. *Elements of high multiplicative order in finite fields*. – Manuscript.

A thesis for obtaining the degree of doctor of sciences in physics and mathematics in the speciality 01.01.06 – algebra and number theory. – Institute of mathematics of NAS of Ukraine, Kyiv, 2016.

The thesis is devoted to research of multiplicative orders of elements in multiplicative groups of finite fields and obtaining explicit lower bounds on these orders. Finite field elements and lower bounds on their orders are obtained in explicit form. Such elements can be useful in a range of applications, particularly in cryptography and error-correcting coding. In extensions of finite fields based on cyclotomic polynomials for elements of a more general form than Gauss period, an explicit exponential lower bound on the order of the elements: stronger than previously known for Gaussian period is received. Such extensions exist for infinitely many of extension degrees if for the number of elements of the base field the Artin's conjecture is true. This gave an answer to the open question posed by O. Ahmadi, I. Shparlinski and J. Voloch. Using the results from the theory of partitions of natural numbers, explicit lower bounds for the multiplicative order in terms of the characteristics of the main field and the degree of expansion are obtained. A number of numerical examples for the obtained results is given. A modification of the lower bounds on the orders is described on a base of a number of solutions of linear Diophantine inequality. Elements of multiplicative order bigger, than 4^m, are constructed in Kummer extensions of finite fields. This lower bound is the exact value unlike the previously known approximate bound that is essential for a number of applications. In arbitrary finite extensions of finite fields based on Kummer polynomials, exponential lower bound on the order is received. Actually, the divisibility condition of the number of elements of the finite field multiplicative group by the extension degree is dropped. We consider any extension of the form $F_q[x]/(x^m - a)$, and construct in the extension elements with multiplicative order at least $2^{\lfloor \sqrt[3]{2m} \rfloor}$. The idea is as follows: if the number of non-zero finite field elements has a big divisor m_1, we use for the construction the method as for Kummer extensions; if the number has no a big divisor m_1, then $m_2 = m/m_1$ is big, and we use for the construction the method similar to that in cyclotomic extensions. Note, that in the case of Kummer extensions, conjugates of linear binomial are again linear binomials. This is not true for general extensions on a base of Kummer polynomials. Actually in this situation the proposed method of combining of two approaches is effective. In extensions of finite fields based on Artin-Shreier polynomials elements of large (exponential) order are built explicitly and also the lower bound on their multiplicative order is given. Using computer calculations, some primitive elements are listed for these extensions. Lower bound is derived on a product of binomial coefficients connected with primality proving or construction of high multiplicative order elements for Kummer or Artin-Schreier finite field extensions. Lower bound is obtained on the order of elements in the towers of finite fields defined Conway. Some primitive elements are found for the first twelve fields in Conway towers. A condition under which the mentioned elements are primitive in all fields in Conway towers is formulated. The lower bound on the order of elements in the finite fields towers, defined by Wiedemann, is obtained. We got lower bounds on elements

order for towers of finite fields of characteristic bigger than two. In the partial case of towers with two fields, conjugates of element, that defines the second extension, are described, what allowed to obtain better lower bound than in general case. Lower bound on the multiplicative order of some elements in general extensions of finite fields is strengthened both on the base of the Gao hypothesis and without using of this hypothesis. The relationship between elements of high order and big integers primality proving is studied. The results are proved that allow to connect with the hypothesis a certain chain of subgroups of the correspondent finite field multiplicative group. Exponential lower bounds are obtained on the orders of groups in this chain of subgroups.

Key words: finite field**,** primitive element, multiplicative order, lower bound, cyclotomic polynomial, Kummer polynomial, Artin-Shreier polynomial, recurcive extensions, tower of fields, primality testing, computer calculations, partition.

АННОТАЦИЯ

Поповыч Р. Б. *Елементы большого мультипликативного порядка в конечных полях*. – На правах рукописи.

Диссертация на соискание ученой степени доктора физико-математических наук по специальности 01.01.06 – алгебра и теория чисел. – Институт математики НАН Украины, Киев, 2016.

Диссертация посвящена исследованию порядков элементов в мультипликативных группах конечных полей и получению в явном виде нижних границ для этих порядков. В расширениях конечных полей на основе циклотомических полиномов для элементов более общего вида, чем гауссовый период, получено явную нижнюю границу для порядка: лучшую, чем известная ранее для гауссового периода. Это дало ответ на открытый вопрос О. Ахмади, И. Шпарлински и Ж. Волоха. Выведено, используя результаты по теории разбиений, нижние границы в терминах характеристики поля и степени расширения. В расширениях на основании полиномов Куммера получено экспоненциальную нижнюю границу: снято условие делимости количества элементов мультипликативной группы на степень расширения. В расширениях на основании полиномов Артина-Шраера построено элементы большого порядка и указано явную оценку снизу на этот порядок. Получено нижнюю границу для порядка в башнях Конвея. Найдено определенные примитивные элементы для первых двенадцати полей в этих башнях. Сформулировано условие, при котором элементы такого вида являются примитивными во всех полях в башнях Конвея. Получено нижнюю границу для порядка в башнях Видемана. Найдены нижние границы для башен полей характеристики большей, чем два. Усилена нижняя оценка в общих расширениях конечных полей. Изучено связь между элементами большого порядка и доказательством простоты больших натуральных чисел.

Ключевые слова: конечное поле, примитивный элемент, мультипликативный порядок, нижняя граница, циклотомический полином, полином Куммера, полином Артина-Шраера, рекурсивные расширения, башня полей, тестирование простоты, компьютерные вычисления, разбиения.