Міністерство освіти і науки України
Національний університет “Львівська політехніка”

На правах рукопису

ПОПОВИЧ РОМАН БОГДАНОВИЧ

УДК 512.624

ЕЛЕМЕНТИ ВЕЛИКОГО МУЛЬТИПЛІКАТИВНОГО ПОРЯДКУ В СКІНЧЕННИХ ПОЛЯХ

01.01.06 – алгебра та теорія чисел

Дисертація на здобуття наукового ступеня
доктора фізико-математичних наук

Науковий консультант:

Кириченко Володимир Васильович,
доктор фізико-математичних наук,
професор

Львів – 2016

Зміст

Перелік умовних позначень

F_q скінченне поле з q елементів, де q – степінь простого числа p

F_{q^n} розширення поля F_q степеня n.

F_q^* мультиплікативна група скінченого поля F_q.

Твірні мультиплікативної групи $F_{q^n}^*$ називають примітивними елементами.

ord β мультиплікативний порядок елемента $\beta \in F_q^*$, тобто найменше натуральне число u таке, що $\beta^u = 1$.

$\binom{n}{k}$ кількість сполучень з n елементів по k елементів.

$|S|$ кількість елементів множини S.

$G \times H$ прямий добуток груп G та H

$\gcd(a,b)$ найбільший спільний дільник чисел a та b

$a \mid b$ цей запис означає, що a ділить b.

$\rho_k(l)$ найбільший степінь простого числа k, що ділить ціле число l

Z_n кільце цілих чисел за модулем цілого числа n

Z_n^* мультиплікативна група цілих чисел за модулем n.

$\langle u_1,...,u_k \rangle$ група, породжена елементами $u_1,...,u_k$.

A^* група одиниць кільця A.

$U(C)$ число розбиттів числа C.

$U(C,d)$ число таких розбиттів C, для яких $u_1,\ldots,u_C \le d$, тобто кожна частина розбиття з'являється не більше, ніж d разів.

$Q(C,d)$ число таких розбиттів C, для яких $u_j = 0$, якщо $j \equiv 0 \bmod d$, тобто кожна частина не ділиться на d.

ВСТУП

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, 6, 97, 102] неявно застосовувалось вже в першій половині XIX століття Н. Абелем та Е. Галуа для дослідження розв'язків алгебраїчних рівняннь 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 [1, 97, 102]: 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 F_q^* ненульових елементів скінченного F_q з $q = p^n$ елементів є абелевою групою відносно множення [1, 97, 102]. Відомо, що вказана група циклічна, тобто для цієї мультиплікативної групи F_q^* існують твірні елементи, які часто називають примітивними. За винятком полів з двох або трьох елементів ($q = 2,3$), примітивний елемент не єдиний. Кількість примітивних елементів дорівнює значенню функції Ейлера $\varphi(q-1)$ від кількості ненульових елементів скінченого поля.

Також слід згадати результати про існування примітивних елементів певного (досить простого) вигляду [52-56, 100], зокрема, для розширень степеня 2, 3 та 4. Побудову примітивних елементів простого вигляду розглядали Х. Давенпорт, Л. Карліц, 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 [57, 59, 84, 96] 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 [75, 76] для цієї проблеми працюють у два етапи: на першому етапі знаходять “ невелику ” множину $A \subseteq F_q$, яка гарантовано містить примітивний елемент, а на другому етапі випробовують всі елементи множини A 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 [73]. Під “великим порядком” (англ. термін high order) 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 не є великим. У випадку алгоритмів маємо експоненційні 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 розглядають як для загальних(С. Гао, А. Конфлітті) [61, 73], так і для часткових (О. Ахмаді, І. Шпарлінскі, Ж. Волох, Й. Гатен, Д. Панаріо, М. Чанг, К. Ченг, Д. Ван) скінченних полів [22, 36, 44-47, 75, 78, 143, 144]. Для часткових випадків скінченних полів можна збудувати елементи, що мають набагато більші порядки. Огляди отриманих у цій області результатів можна знайти в працях [44] та [102, розділ 4.4].

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 [75] запропонували в 1995 році алгоритм, який будує елемент 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. Ітo, 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 школи П. Варбанця [65, 139–142] з опису генераторів псевдовипадкових чисел у кільцях цілих гауссових чисел із оцінкою криптографічної якості цих генераторів, праці М. Глазунова [2–5] із використання комп’ютерних обчислень для обґрунтування гіпотез алгебри та теорії чисел, праці О. Устименко [93, 134–138] з алгебраїчної комбінаторики та можливих криптографічних застосувань, працю Ю. Дрозда, В. Кириченка [2] із скінченновимірних алгебр, праці школи Я. Сисака [126, 127] із скінченних майже-кілець.

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. 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.

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 і 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 [7–19, 108–114] у провідних закордонних та українських наукових фахових виданнях із фізико-математичних наук, затверджених МОН України, 6 із яких [19, 108, 109, 111, 112, 113] надруковано у виданнях, включених до міжнародних наукометричних баз Web of Science і/або Scopus, і додатково висвітлені в 2 статтях [20, 21] у збірниках наукових праць та 10 матеріалах і тезах міжнародних наукових конференцій [115–124].

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.

Короткий зміст дисертації

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 відповідному для цього вигляді. Проведено огляд відомих результатів, наведених у літературі.

У **другому розділі** наведено необхідні для подальшого викладу відомі результати; описано, які задачі вирішуються в дисертаційній роботі та які підходи для цього використано.

У **третьому розділі** розглянуто явну побудову елементів великого порядку в розширеннях скінченних полів, які пов’язані з поняттям гауссового періоду, а саме в полях вигляду $F_q(\theta) = F_{q^{r-1}} = F_q[x]/(x^{r-1} + \ldots + x + 1)$ (на основі циклотомічних поліномів).

У першому підрозділі підсилено та узагальнено результат з праці О. Ахмаді, І. Шпарлінскі та Ж. Волоха [22] на елементи більш загального вигляду, ніж гауссовий період. Це дає відповідь на відкрите питання, поставлене цими авторами. Доведено теорему 3.1. яка дає нижню межу для порядків певних елементів скінченого поля. Всі нижні межі в теоремі 3.1 використовують поняття розбиття, де кожна частина з'являється не більше, ніж p-1 разів.

У другому підрозділі отримано, використовуючи відомі результати з теорії розбиттів, явні нижні межі для мультиплікативних порядків елементів у термінах p – характеристика поля, та r – степінь розширення. В третьому підрозділі наведено низку числових прикладів для отриманих у двох попередніх підрозділах результатів. Четвертий підрозділ присвячено модифікації нижніх меж для мультиплікативних порядків елементів. Це зроблено на основі оптимізації та підрахунку кількості розв'язків лінійної діофантової нерівності замість підрахунку кількості розбиттів. У п'ятому підрозділі підсилено відомі асимптотичні нижні межі для порядків елементів.

У **четвертому розділі** розглядаємо нижні межі для порядку елементів у розширеннях на основі поліномів Куммера (вигляду $F_q[x]/(x^m - a)$). В першому підрозділі виписуємо умови, при яких такі розширення існують. У другому підрозділі розглядаємо частковий випадок, коли виконується умова: m ділить $q-1$. В теоремі 4.3 отримано нижню межу, яка є точною величиною, на відміну від відомої наближеної межі. У третьому підрозділі знімаємо цю умову для будь-якого m. Показуємо в лемі 4.6, що $m = m_1 m_2$, де m_1 є дільником $q-1$, а m_2 є порядком q за модулем m. Явно будуємо елементи порядку принаймні $2^{\lfloor \sqrt[3]{2m} \rfloor}$. Ідея полягає в наступному: якщо $q-1$ має великий дільник m_1, то використовуємо метод як для розширень Куммера; в іншому разі m_2 є великим, і використовуємо метод як для циклотомічних розширень. У четвертому підрозділі підсилюємо нижню межу

з використанням максимуму функції кількості розв'язків діофантового рівняння, а в п'ятому – з використанням оцінки знизу для кількості розбиттів.

У **п'ятому розділі** розглянуто побудову елементів великого порядку в розширеннях вигляду $F_p[x]/(x^p - x - a)$ (на основі поліномів Артіна-Шраєра). У першому підрозділі в теоремі 5.1 явно будуємо елементи великого порядку. У другому підрозділі розглядаємо з використанням комп'ютерних обчислень явну побудову деяких примітивних елементів. У третьому підрозділі даємо нижню межу для добутку біноміальних коефіцієнтів, пов'язаному з тестуванням простоти або побудовою елементів великого порядку в розширеннях Куммера та Артіна-Шраєра.

У **шостому розділі** даємо нижню межу для порядку деяких елементів у рекурсивних розширеннях скінченних полів характеристики два, визначених Конвеєм та Відеманом, а також у рекурсивних розширеннях полів характеристики більшої від двох. У першому підрозділі в наслідку 6.2 даємо нижню межу для порядку деяких елементів у розширеннях, визначених Конвеєм. В другому підрозділі описуємо деякі примітивні елементи для перших дванадцяти полів у вежах Конвея. Також формулюємо в наслідку 6.3 умову, при якій розглянуті в першому підрозділі елементи є примітивними. У третьому підрозділі даємо в теоремі 6.9 нижню межу для порядку деяких елементів у розширеннях, визначених Відеманом. Четвертий та п'ятий підрозділи присвячено отриманню нижніх меж для порядку елементів у вежах скінченних полів характеристики більшої, ніж два.

У **сьомому розділі в** першому підрозділі розглянуто побудову елементів великого порядку в загальних скінченних полях на основі гіпотези Гао. У другому підрозділі побудовано елементи великого порядку в цих полях без використання гіпотези Гао. Для отримання нижніх меж застосовуємо наслідок із ABC теореми Стовера–Мейсона для поліномів. У третьому підрозділі вивчаємо зв'язок між елементами великого порядку та доведенням простоти великих натуральних чисел.

РОЗДІЛ 1

Огляд літератури

1.1. Мультиплікативна структура скінченного поля

Через F_q будемо позначати скінченне поле з q елементів, де q – степінь деякого простого числа p.

1893 року І. Х. Мур довів класифікаційну теорему [1, 97, 102] для скінченних полів. Вона формулюється наступним чином:

Теорема 1.1. *Порядок скінченного поля є натуральним степенем простого числа. Для довільного* $q = p^n$ *існують скінченні поля з* q *елементами і всі вони ізоморфні. В цих полях кожен елемент задовольняє рівняння* $x^q = x$ *та поліном* $x^q - x$ *розкладається на лінійні множники* $x^q - x = \prod_{a \in F_q} (x - a)$.

Множина ненульових елементів в F_q є абелевою групою відносно множення, порядку $q-1$. За теоремою Лагранжа для скінченних груп [1], існує дільник k числа $q-1$ такий, що $x^k = 1$ для будь-якого ненульового елемента x з F_q. Так як рівняння $X^k = 1$ має щонайбільше k розв'язків у будь-якому полі, то $q-1$ є найменшим можливим значенням для k. Структурна теорема для скінченних абелевих груп дає, що ця мультиплікативна група є циклічною, тобто всі ненульові елементи є степенями одного елемента. Підсумовуючи сказане, отримуємо наступну теорему.

Теорема 1.2. [97] *Мультиплікативна група ненульових елементів поля* F_q *є циклічною, й існує такий елемент* a, *що* $q-1$ *ненульові елементи поля* F_q *є* a, a^2, ..., a^{q-2}, $a^{q-1}=1$.

Твірний елемент групи називають примітивним. За винятком випадків $q=2,3$ примітивний елемент не єдиний. Кількість примітивних елементів [97, 102] дорівнює $\varphi(q-1)$, де φ – функція Ейлера. Із наведеного випливає, що $x^q = x$ для кожного x в F_q. Частковий випадок, коли q – просте число, є малою теоремою Ферма.

(Абсолютний) степінь елемента α скінченого поля характеристики p визначаємо так: $\deg\alpha = [F_p(\alpha) : F_p]$. Мультиплікативний порядок $\operatorname{ord}\beta$ елемента $\beta \in F_q^*$ – це найменше натуральне число u таке, що $\beta^u = 1$.

Зауваження 1.1. Якщо $\alpha \neq 0,1$ є елементом скінченого поля характеристики p, то $\deg\alpha < \operatorname{ord}\alpha \leq p^{\deg\alpha} - 1$.

Якщо елемент a - примітивний в F_q, то для кожного ненульового елемента x з F_q існує єдине ціле число n з умовою $0 \leq n \leq q-2$ таке, що $x = a^n$. Це ціле n називають дискретним логарифмом [97, 102] для x за основою a.

Зауваження 1.2. Описану задачу знаходження дискретного логарифма в скінченому полі можна узагальнити [97] для будь-якої скінченої циклічної групи $G = \langle a \rangle$ порядку $q-1$, операцію в якій позначимо як звичайне множення. Тоді для кожного елемента x з G існує єдине ціле число n з умовою $0 \leq n \leq q-2$ таке, що $x = a^n$. Це ціле n 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 [97]. Це використано в низці криптографічних протоколів [99].

Коли ненульові елементи поля F_q зображаємо їх дискретними логарифмами, то операції їх множення й ділення є простими, оскільки вони зводяться до додавання та віднімання за модулем числа $q-1$. Проте, додавання полягає в обчисленні дискретного логарифма елемента $a^m + a^n$. Наступна рівність

$$a^m + a^n = a^n(a^{m-n} + 1)$$

дозволяє вирішити цю трудність, будуючи таблицю дискретних логарифмів для $a^n + 1$, які називають логарифмами Зеха, при $n = 0,...,q-2$ (звичайно визначають дискретний логарифм нуля як рівний $-\infty$). Логарифми Зеха корисні для великих обчислень, таких як лінійна алгебра над полями середнього розміру, тобто, полями, що є достатньо великими щоб зробити натуральні логарифми неефективними, але не занадто великими, оскільки треба попередньо обчислити таблицю того самого розміру, що й порядок поля.

Для поля F_q характеристики p, автоморфізм Фробеніуса – це відображення $\varphi: F_q \to F_q$, яке кожному елементу α з F_q ставить у відповідність елемент α^p [97, 102]. Два елементи α, β із розширеного поля F_q називаємо спряженими (над початковим простим полем F_p), якщо виконується рівність $\alpha = \varphi^t(\beta)$ для деякого степеня φ^t автоморфізму Фробеніуса.

Лема 1.1. [97] *Всі спряжені елементи мають однаковий мультиплікативний порядок.*

Норма [97, 102] елемента $\alpha \in F_{q^n}$ відносно розширення F_{q^n} поля F_q дорівнює $N_{F_{q^n}/F_q}(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i}$. Вона витримує всі степені g^t, $t = 0,..., p-1$ автоморфізму Фробеніуса. Тому норма елемента належить до основного поля. Тобто норма – це відображення з F_{q^n} в F_q. Ядром цього відображення є циклічна підгрупа порядку $(q^n - 1)/(q-1)$.

1.2. Примітивні елементи та їх пошук

З підрозділу 1.1 відомо, що мультиплікативна група скінченного поля є циклічна. Твірну цієї групи називають примітивним елементом. Алгоритм ефективний (швидкий, поліноміальний), якщо його час виконання дорівнює $\log(q^n)^{O(1)}$ арифметичних операцій в F_{q^n}.

Однією з найбільш важливих нерозв'язаних задач в обчислювальній теорії скінченних полів є створити швидкий алгоритм побудови примітивного елемента в скінченому полі F_q. Основні відомі стратегії пошуку [75, 76] примітивного елемента складаються з двох етапів:

1. Знайти " невелику " множину $A \subseteq F_q$, яка гарантовано містить примітивний елемент F_q.

2. Випробовувати всі елементи множини A на примітивність.

У багатьох випадках, маємо поліноміальні алгоритми для першого етапу, зокрема, якщо припускаємо виконання розширеної гіпотези Рімана (Extended Riemann Hypothesis або скорочено ERH) ([76]).

Слід розділити задачу побудови невеликої множини, яка містить примітивний елемент: окремо для простих полів та окремо для розширених полів. Звичайно розпочинаємо з простих полів і з невеликих чисел. Визначення верхньої межі для найменшого примітивного елемента завжди було важливою проблемою в алгебрі й теорії чисел. Ванг показав у своїй класичній праці [147], що найменший примітивний елемент для простого поля F_p обмежений величиною $p^{1/4+\varepsilon}$. Припускаючи ERH, Ванг [147] показав , що найменший примітивний елемент у простому полі F_p обмежений величиною $O(\omega^6(p-1)\log^2 p)$, де ω є відображенням, яке переводить натуральне число в кількість його різних простих дільників. Можна довести, що $\omega(n) = O(\log n / \log\log n)$. Шоуп [129] покращив цю межу до $\tilde{O}(\omega^4(p-1)\log^2 p)$. Тут $\tilde{O}(f(n))$ означає $O(f(n)\log^c f(n))$.

Таким чином, якщо ERH справедлива, то можна утворити множину, що містить примітивний елемент, виписуючи всі числа, менші, ніж межа Шоупа, яка є поліноміальною від розміру входу. Бах [27] показав, припускаючи ERH, як збудувати множину потужності $O(\log^4 p)$, що містить принаймні один примітивний елемент. Замість використання лише малих чисел, його множина складається з великих чисел, які є добутком малих простих чисел.

Випадок розширених полів малої характеристики виглядає простішим. Шоуп [129], і незалежно Шпарлінскі [131, теорема 2.4] показали, не спираючись ні на які припущення, що можна детерміновано збудувати множину розміру $(np)^{O(1)}$, яка містить принаймні один примітивний елемент поля F_{p^n}.

На жаль, при сьогоднішньому стані знань, другий етап вимагає розкладу $q-1$ на прості множники (α примітивний тоді і тільки тоді, коли $\alpha^{(q-1)/d} \neq 1$ для кожного простого $d \mid q-1$), для чого невідомий

поліноміальний алгоритм. Проблема не в тому, що примітивні елементи зустрічаються рідко. Насправді, доведено, що справедлива така теорема.

Теорема 1.3. ([125, розділ 1, теорема 5.1]) *Нехай q – степінь простого числа і нехай F_q – скінченне поле з q елементів. Кількість примітивних елементів у F_q, тобто величина $\varphi(q-1)$, більша, ніж $cq/\log\log q$, де $c>0$ – абсолютна константа, а φ є функцією Ейлера.*

Функція $1/\log\log q$ є оберненою до логарифмічної функції від розміру входу і вона дуже повільно прямує до нуля при збільшенні q. З цього випливає, що коли ми випадковим чином виберемо елемент, то з великою ймовірністю отримаємо примітивний елемент. Рівносильно, якщо виберемо список із $(\log\log q)^{1+\varepsilon}$ випадкових елементів, то з імовірністю $1+o(1)$ в ньому є примітивний елемент. Проте, дуже важко вирішити, який з елементів примітивний. Єдиний відомий загальний метод спирається на такий факт.

Теорема 1.4. ([44]) *Нехай $q-1=p_1^{e_1}p_2^{e_2}...p_m^{e_m}$, де $p_1,...,p_m$ – різні прості числа. Елемент α є примітивним в полі F_q тоді і тільки тоді, коли для кожного p_i, $1\le i\le m$, $\alpha^{(q-1)/p_i}\neq 1$.*

Ці твердження дають нам імовірнісний алгоритм побудови примітивного елемента з гіпотетичною часовою складністю $e^{O(\log^{1/3} q(\log\log q)^{2/3})}$, яка дорівнює складності найшвидшого універсального алгоритму розкладу на множники числа $q-1$, і є непрактичною при зростанні q.

Шпарлінскі [130] показав, що в полі F_q, де q є степенем простого числа, примітивний елемент можна знайти з часовою складністю $O(q^{1/4+\varepsilon})$ для будь-якого $\varepsilon>0$. Навіть ERH не може тут суттєво допомогти.

Зауважимо, що найкращий детермінований алгоритм розкладу числа N вимагає час $N^{1/4+\varepsilon}$.

Поліноміальний алгоритм, який знаходить примітивний елемент у скінченному полі малої характеристики, описано в праці [85]. Проте алгоритм спирається на два недоведених припущення та не підкріплений жодним обчислювальним прикладом. Перше з припущень подібне до гіпотези, висловленої Гао [73].

Також слід згадати результати про існування примітивних елементів певного (досить простого) вигляду. Для випадку простих полів F_q ($q = p$ – довільне просте число) Давенпорт [66] довів, що коли беремо q достатньо великим ($q > q_0(n)$), то існує такий елемент $a \in F_q$, що в розширенні $F_{q^n} = F_q(\theta)$ елемент $\theta + a$ є примітивним. Карліц [40] узагальнив наведене твердження для будь-якого степеня q простого числа.

Низка авторів детально вивчала розширення степеня 2, 3 та 4 [52–56, 100]. Зокрема, показано [52], що в розширеннях $F_{q^2} = F_q(\theta)$ для довільного $\beta \in F_q^*$ існують примітивні елементи вигляду $\beta(\theta + a)$, $a \in F_q$. Цей результат підтвердив гіпотезу, наведену в праці [79]. Його отримано повністю на основі теоретичних міркувань, без використання комп'ютерних обчислень.

Також доведено [56, 100], що коли $q \notin \{3, 7, 9, 13, 37\}$, то для розширень $F_{q^3} = F_q(\theta)$ існують примітивні елементи вигляду $\theta + a$, $a \in F_q$. Остаточний результат, який підтвердив сформульовану в праці [100] гіпотезу, наведено в роботі [56].

Стосовно розширень степеня 4 на сьогодні відомо [56] таке. Для розширень $F_{q^4} = F_q(\theta)$ за довільного $\beta \in F_q^*$ існують примітивні елементи вигляду $\beta(\theta + a)$, $a \in F_q$ за винятком $q \le 25943$ та $\omega(q^4 - 1) \le 12$. Тут $\omega(m)$ позначає кількість різних простих дільників числа m.

Як бачимо, є низка результатів про існування примітивних елементів певного простого вигляду. Проте, як їх явно знайти (тобто знайти елементи a та β для розширень степеня 2 чи степеня 4 та знайти елемент a для розширень степеня 3) невідомо.

Отримано низку результатів про існування примітивних елементів із різними додатковими властивостями. Елемент $x \in F_{q^n}$ називають вільним чи нормальним, якщо множина $x, x^q, x^{q^2}, ..., x^{q^{n-1}}$ є F_q-базисом для векторного простору F_{q^n}. Такий базис називають нормальним. Загально відомо, що як примітивні, так і вільні елементи існують. Також відомо, що існують елементи, які є одночасно примітивними й вільними.

Теорема 1.5. (теорема про примітивний нормальний базис) *Нехай q – степінь простого числа, а m – натуральне число. Існує $x \in F_{q^n}$, який одночасно примітивний і вільний.*

Ленстра та Шуф [96] дали повне доведення теореми 1.5, завершуючи доведення Карліца [38, 39] та Давенпорта [67] у часткових випадках. Недоліком їх праці є те, що доведення використовує комп'ютерні обчислення. Пізніше Коен та Гучинска [59] опублікували доведення без використання комп'ютерних обчислень за допомогою техніки просіювання, раніше введеної Коеном у роботі [58]. Також, досліджено низку узагальнень теореми 1.5 [57, 84, 147]. Так, у праці [89] отримано наступний результат.

Теорема 1.6. (підсилена теорема про примітивну нормальну базу)
Нехай q – степінь простого числа, а n – натуральне число. Існує $x \in F_{q^n}$ таке, що елементи x та x^{-1} є обидва одночасно примітивні й вільні, за винятком випадків, коли пара (q,n) є однією з таких пар: (2; 3), (2; 4), (3; 4), (4; 3) *або* (5; 4).

Тіан і Кві [133] довели вказане формулювання для випадку $n \geq 32$, а Коен і Гучинска [60] узагальнили його до вказаного вигляду, знову ж за допомогою їх техніки просіювання.

В роботі [89] розглянуто також узагальнення обидвох останніх теорем:

Теорема 1.7. *Нехай* $q \geq 23$ *– степінь простого числа,* $n \geq 17$ *– натуральне число та* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(F_q)$ *така, що коли* A *має точно два ненульових елементи і* q *– непарне, то результат ділення цих елементів є квадратом в* F_{q^n} *. Існує* $x \in F_{q^n}$ *таке, що* елементи x *та* $\frac{ax+b}{cx+d}$ *є обидва одночасно примітивні й вільні.*

Очевидно, що теореми 1.5 та 1.6 є частковими випадками теореми 1.7 для матриць вигляду $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ та $\begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix}$, де $a \neq 0$, відповідно. Однак зрозуміло наступне: незважаючи на те , що теорема 1.7 є природним розширенням теорем 1.5 і 1.6, велика кількість можливих винятків залишає місце для вдосконалення. Варто відзначити, що оскільки в цій роботі було використано згадану техніку просіювання, не слід очікувати суттєвих покращень. З іншого боку, якщо опускаємо у теоремі 1.7 умову для елемента $\frac{ax+b}{cx+d}$ бути примітивним, то отримана задача все ще буде узагальненням теорем 1.5 та 1.6 (щоб це було зрозумілим, зауважимо, що дві умови для x *та* x^{-1} бути примітивними в теоремі 1.6 накладаються, тобто остання задача насправді має власне три умови) і також буде порівнювана за складністю з теоремою 1.7, а сподівання повністю розв’язати цю задачу буде більш реалістичним.

Власне в роботі [90] автор опустив у теоремі 1.7 умову для елемента $\frac{ax+b}{cx+d}$ бути примітивним та повністю розв'язав задачу, яка виникла. А саме доведено наступне:

Теорема 1.8. *Нехай* q *– степінь простого числа,* $n \geq 2$ *– натуральне число та* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(F_q)$, *де* $A \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, *якщо* $q = 2$ *та* n *– непарне .*

Існує примітивний $x \in F_{q^n}$ *такий, що* x *та* $\frac{ax+b}{cx+d}$ *обидва утворюють нормальний базис для* F_{q^n} *над* F_q, *за винятком наступних випадків:*

1. $q = 2$, $n = 3$ *та* $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *або* $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$,

2. $q = 3$, $n = 4$ *та* A *є антидіагональною або*

3. (q, m) *дорівнює* (2,4), (4,3) *або* (5,4) *та* $d = 0$.

Слід зауважити, що не лише не маємо нових винятків, ніж ті, які з'явилися в теоремі 1.6, але зовсім не маємо винятків, якщо всі елементи матриці A є ненульовими. Це трохи несподівано, якщо розглядаємо велику кількість різних перетворень, що задають різні матриці A. Також, зауважимо, що нескінченна сім'я $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $q = 2$ та n – непарне, складається виключно із дійсних винятків.

Праця [90] доповнює результати із [89]. Оцінювання сум характерів [41, 51, 106] відіграє вирішальну роль у доведеннях в праці [90]. Більш того, вказана стаття продовжує роботи Коена і Гучинскої [59, 60] й використовує видозмінену техніку із них.

Слід також згадати праці, пов'язані з поняттям нормального базису над певним підполем скінченного поля [34, 57, 67, 68, 69, 71, 107], поняттям

само-дуального нормального базису [25, 88] та поняттям оптимального нормального базису [26, 31, 33, 48, 49, 70, 72, 104].

1.3 Елементи великого порядку та їх явна побудова

Як описано в попередньому підрозділі, ефективно побудувати примітивний елемент для заданого скінченного поля в обчислювальній теорії скінченних полів важко – проблема залишається відкритою.Ось чому розглядають менш обмежувальне питання: знайти елемент великого мультиплікативного порядку [102]. Цього достатньо для деяких застосувань. У цьому випадку не вимагають обчислити точний порядок елемента: достатньо отримати нижню межу для порядку. Переважно ця межа є значно меншою, ніж очікуваний фактичний порядок. Елементи великого порядку потрібні для низки застосувань, які, зокрема, охоплюють криптографію, теорію кодування, генератори псевдовипадкових чисел та комбінаторику. Як специфічний приклад застосування елементів великого порядку, слід виділити алгоритми [50, 149] інтерполяції розріджених (sparce) поліномів, де замість примітивного кореня якраз використовують елемент великого порядку (після деяких простих узгоджень параметрів).

С. Гао спробував формалізувати поняття елементів “великого порядку“ даючи наступне визначення [73]. Під “великим порядком” (англ. термін high order) елемента у скінченому полі F_{q^n} , ми розуміємо, що порядок елемента повинен бути більший, ніж кожен поліном від $\log(q^n)$, коли $q^n \to \infty$. Можна провести паралель між поділом алгоритмів стосовно оцінки їх обчислювальної складності та поділом елементів скінченного поля на елементи великого порядку та порядку, який 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 F_p при такій постановці задачі переважно не розглядають. Як виняток, можна вказати на дві роботи М.-С. Чанга. В одній із них [43] розглянуто побудову елементів великого порядку в простих скінченних полях. Друга з них [42] розглядає побудову елементів великого порядку (йдеться про так звані гауссові періоди) для випадку, коли зафіксовано великий степінь розширення, а характеристика початкового поля набагато більша від вказаного степеня.

Питання побудови елементів великого мультиплікативного порядку розглядають як для загальних, так і для спеціальних скінченних полів. Для часткових випадків скінченних полів можна збудувати елементи, що мають набагато більші порядки. Огляд отриманих у цій області результатів станом на 2005 рік написаний Ченгом [44]. Огляд отриманих результатів станом на початок 2012 року наведений в [102 , розділ 4.4] (розділ написаний Волохом). Перший приклад елемента великого порядку збудували Гатен та Шпарлінскі [75-78].

Таким чином, поки не буде знайдено новий шлях доведення примітивності елемента, мусимо відмовитися від мети знаходження примітивного елемента для загальних скінченних полів. На щастя, деколи достатньо елемента великого порядку. Наприклад, у криптології [99], якщо твірний елемент підгрупи має великий порядок, то це робить нездійсненною

атаку Шенкса та Полларда на задачу дискретного логарифма у цій підгрупі. Більш того, знаходження примітивного елемента є крайнім випадком знаходження елемента великого порядку. На практиці, поля малої характеристики є зокрема корисними. Якщо характеристики полів малі, то це навіть важча задача: знайти розклад на прості множники відповідного порядку, ніж порядку випадкових простих полів. У цьому контексті, задача елемента великого порядку може бути перефразована так: для q – фіксованого степеня простого числа, знайти елемент великого порядку в F_{q^n} за час поліноміальний від n. Інше важливе, але більш просте запитання вимагає знайти число n більше від заданого числа N, та елемент порядку принаймні q^{n^c} в F_{q^n} для деякої константи c. Логічне обґрунтування такого запитання, яке називають проблема знаходження елемента великого порядку для часткових скінченних полів, в тому, щоб спочатку розправитися з частковими скінченними полями, а потім постаратися збільшити щільність послідовності чисел n так, що зрештою можемо знайти елементи великого порядку для всіх розширень скінченних полів. Зауважимо, що не вимагається обчислити точний порядок елемента. Замість цього, лише треба дати доведення, що елемент має порядок більштй, ніж певна межа. Слід наголосити, що оскільки задача примітивного елемента є складною, то в більшості випадків криптологічних застосувань, скінченні поля вибирають так, що повні розклади порядків полів відомі, а значить є ефективний імовірнісний алгоритм побудови твірних цих полів.

1.3.1. Загальна схема й конструкція Гао

Явні побудови елементів великого порядку звичайно спираються на комбінаторні прийоми, які можуть надати доказову нижню межу для порядку. Вони не обчислюють точний порядок. Це, як правило, передбачає

знання розкладу порядку на множники. З обчислювальної точки зору, розширення скінченого поля це не що інше, як поліноміальне кільце над простим скінченним полем за модулем деякого нерозкладного полінома. Припустимо, що поле задається $F_q[x]/(f(x))$, де $f(x)$ – нерозкладний поліном над F_q. Нехай $\alpha = x(\mathrm{mod}\, f(x))$. Два різних поліноми можуть представляти той самий елемент поля. Наприклад, $x+1$ та $-x^3+1$ є в тому самому класі еквівалентності в полі $F_3[x]/(x^2+1)$. Проте, легко показати, що справедлива така лема.

Лема 1.2.1. *Нехай $f(x)$ – поліном степеня m над полем F_q. Якщо поліноми $g(x)$ та $h(x)$ з $F_q[x]$ степеня меншого за m різні, то класи цих поліномів у кільці $F_q[x]/(f(x))$ також є різними.*

Зокрема, беремо у розділі 3 нерозкладний поліном $f(x) = \Phi_r(x)$, у розділі 4 нерозкладний поліном $f(x) = x^m - a$, а у розділі 5 – поліном $f(x) = x^p - x - a$. У деяких випадках зручніше користуватися трошки видозміненим формулюванням леми 1.2.1, а саме наступною лемою.

Лема 1.2.2. *Якщо $g(x)$ та $h(x)$ не рівні в $F_q[x]$, а їх степені менші за m, то $g(\alpha) \neq h(\alpha)$.*

Усі побудови використовують подібну схему. Бажаний елемент β будують так, що можна знайти множину U великої потужності, яка складається з цілих чисел між 1 та $q^n - 1$ і яка задовольняє умови:

1. Для будь-якого $i \in U$, β^i має просте подання степеня меншого, ніж n, у $F_p[\alpha]$ (переважно отримуємо це подання використовуючи лінійність p-го степеня);

2. Для будь-яких $i, j \in U$, якщо $i \neq j$, то $\beta^i \neq \beta^j$. Оскільки степінь β має подання малого степеня, можемо підняти (англ. термін lift) цей елемент до

кільця поліномів $F_q[x]$, де простіше довести відмінність вказаних двох елементів.

Якщо можемо довести ці два твердження, то ми показали, що потужність множини U є нижньою межею для порядку елемента β.

Таким чином, при побудові елементів великого порядку домінує комбінаторний підхід. У цьому разі переважно беруть як елемент β деякий біном від змінної x (як правило, лінійний, тобто біном першого степеня) та будують добутки елементів, спряжених з елементом β. 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. Гао [73] дав алгоритм побудови елементів великого порядку для загальних розширень F_{q^m} скінченного поля F_q з нижньою межею для порядку $\exp((\log m)^2 / \log\log m)$. Його алгоритм припускає виконання певної правдоподібної, але досі не доведеної гіпотези. Більш точно підхід з праці [73] спирається на таке припущення.

Гіпотеза (Гао). Для довільного цілого числа n існує такий поліном $g(x) \in F_q[x]$ степеня d (який не перевищує $2\log_q n$), що $x^m - g(x)$ має нерозкладний дільник $f(x)$ степеня n.

Зауважимо, що наведені обчислювальні дані [73] підтверджують гіпотезу лише для полів характеристики два, а для більшої від двох такі дані в літературі відсутні. Конфлітті [61], спираючись на вказану гіпотезу, виконав точніший аналіз результатів з праці [73].

Застосовуючи описану на початку даного підрозділу схему, Гао [73] запропонував алгоритм із поліноміальною часовою складністю, який для

заданих степеня простого числа q та натурального числа n, видає елемент порядку принаймні

$$n^{\frac{\log_q n}{4\log_q(2\log_q n)}-\frac{1}{2}}.$$

Він не довів, що цей алгоритм завжди дає на виході якийсь елемент. Але є всі підстави зробити таке припущення.

Для полінома $g(x)\in F_q[x]$, означимо $g^{(i)}(x)$ як i-ту суперпозицію функції g. Формально

$$g^{(0)}(x)=x \text{ та } g^{(i)}(x)=g^{(i-1)}(g(x)) \text{ при } i\geq 1.$$

Нехай m – найменший степінь числа q, який більший або дорівнює n. Метод Гао просто перевіряє, чи $x^m-g(x)$ має нерозкладний дільник степеня n для всіх поліномів $g(x)$ степеня щонайбільше $2\log_q n$. Якщо так, то він видає на виході корінь цього полінома, позначений через β. Очевидно, що справедливе співідношення $F_q[\beta]=F_{q^n}$. Гао припускав, що такий поліном $g(x)$ існує.

Метод спирається на рівність $\beta^m=g(\beta)$ і дає як відповідь алгоритму елемент β. Оцінимо мультиплікативний порядок елемента β. Позначимо степінь $g(x)$ через ε. Степінь елемента β^{m^i} як полінома від β збільшується з швидкістю ε^i. Нехай $t=\left\lfloor \frac{\log_q n}{2\log_q \varepsilon} \right\rfloor$. Як описану раніше множину U, Гао розглядав наступну множину:

$$U=\left\{\sum_{i=0}^{t-1} a_i m^i \mid 0\leq a_i\leq \sqrt{n}\right\}.$$

Для будь-якого $u = \sum_{i=0}^{t-1} a_i m^i \in U$, $\beta^u = \prod_{i=0}^{t-1} (g^{(i)}(\beta))^{a_i}$. Зрозуміло, що поліном $\prod_{i=0}^{t-1} (g^{(i)}(x))^{a_i}$ має степінь менший, ніж n. Щоб показати, що для будь-яких $u, u' \in U$, $u \neq u'$, виконується $\beta^u \neq \beta^{u'}$, Гао спирався на доведене ним твердження про мультиплікативну незалежність поліномів $g^{(i)}(x)$.

Аналізуючи конструкцію Гао більш уважно, Конфлітті [61] отримав нижню межу для порядку у деяких випадках кращу, ніж отриману Гао. Оскільки степінь $g^{(i)}(x)$ росте експоненційно із збільшенням i, то обидва результати доводять лише слабо суперполіноміальні нижні межі. Таким чином, маємо не надто добрий результат, який ще й спирається на недоведене припущення.

Якщо поле володіє додатковими властивостями, то є два 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. Вони описані в підрозділах 1.3.2 та 1.3.3.

1.3.2. Гауссові періоди

Ґрунтуючись на властивостях гауссових періодів, Гатен і Шпарлінскі [75-78] запропонували алгоритм, який будує елемент субекспоненційного порядку в деяких часткових полях. Припустимодалі, що $r = 2n+1$ є простим числом, яке не ділить q, і q – примітивний елемент у F_r. Очевидно $r \mid q^{2n} - 1 = q^r - 1$. Нехай ξ – примітивний корінь степеня r з одиниці в $F_{q^{2n}}$. Розглянемо елемент $\beta = \xi + \xi^{-1}$, також відомий як гауссовий період типу $(n, 2)$. Легко показати, що $\beta \in F_{q^n}$.

Нехай $h = \lfloor \sqrt{r} \rfloor - 1$. Як множину U автори брали таку множину

$$U = \left\{ \sum_{i=0}^{h-1} a_i q^{s_i} \mid a_i \in \{0,1\} \right\},$$

де s_i є дискретний логарифм i за модулем r, а саме $q^{s_i} (\mathrm{mod}\, r) = i$, і, значить, $|U| = 2^h$.

Спираючись на цей результат, Гатен та Шпарлінскі [75-78] довели наступні теореми:

Теорема 1.9. *Нехай q – заданий степінь простого числа. Для будь-якого натурального числа N, натуральне число $n \geq N$ з умовою $n = O(N \log N)$ та елемент $\alpha \in F_{q^n}$ порядку принаймні $2^{(2n)^{1/2}-2}$ можна обчислити за час поліноміальний від N.*

Базово алгоритм шукає просте число r більше від $2N+1$ таке, що q є примітивним елементом в F_r. Цей алгоритм має ту перевагу, що утворюваний елемент є також нормальним елементом. Якщо вилучити цю вимогу, доведено результат із щільнішою послідовністю чисел n.

Теорема 1.10. *Нехай q заданий степінь простого числа. Для будь-якого натурального числа N, натуральне число $n \geq N$ з умовою $n = N + O(N/\log^c N)$ та елемент $\alpha \in F_{q^n}$ порядку принаймні $2^{10q^{-12}n^{1/2}-25}$ можна обчислити за час поліноміальний від N.*

Степінь полінома від ξ, який зображає $\xi^i \beta^{q^{s_i}}$ дорівнює $2i$, що росте лінійно із збільшенням i. Таким чином, досягнуто суперекспоненційну нижню межу $2^{O(\sqrt{n})}$. Далі розглянемо в підрозділі 1.3.3 результати із праці [44], в якій степінь полінома, що зображає $\beta^{q^{s_i}}$ незмінний і дорівнює одиниці, а як наслідок отримано нижню межу $2^{n^{1-\varepsilon}}$.

1.3.3. Елементи великого порядку в розширеннях Куммера

Сучасна техніка у знаменитому алгоритмі AKS тестування простоти та його подальших вдосконаленнях [23, 29, 30, 32, 145] полягає у використанні поліномів першого степеня для породження великої мультиплікативної групи за модулем натурального числа та полінома. Ченг [44-45] побачив зв'язок цієї задачі із проблемою знаходження елемента великого порядку для часткових скінченних полів та застосував цю ідею для отримання нового розв'язкувказаної задачі. Його результат характеризується щільнішою послідовністю чисел n та/або значно більшим порядком.

Розглянемо розширення Куммера F_{q^n}, $n \mid q-1$. Таке розширення можна записати у вигляді $F_{q^n} = F_q[x]/(x^n - b)$, де $x^n - b$ нерозкладний поліном над F_q. Як звичайно нехай $\alpha = x(\mathrm{mod}\, x^n - b)$ та нехай $\beta = \alpha + 1$. Використовуючи як додатні, так і від'ємні q-ті степені елемента β, отримано оцінку для порядку елемента β. Вона наближено дорівнює $5{,}8^n$. Використання від'ємних степенів запропоновано Волохом [145].

Тепер можна підсумувати результати попередніх розглядів.

Теорема 1.11. *Нехай q – степінь простого числа. Для достатньо великого натурального числа N можна обчислити за час поліноміальний від N натуральне число $n \in [N, 2qN]$ та елемент $\beta \in F_{q^n}$ порядку більшого, ніж* $5{,}8^{n/\log_q n}$.

У теоремі 1.11, використано послідовність $q-1$, $2(q^2-1),\ldots$, $i(q^i-1),\ldots$ У наступній теоремі, взято щільнішу послідовність 2, 6, 20,…, $p(p-1),\ldots$, де число p пробігає всі прості числа.

Теорема 1.12. *Нехай* q *– степінь простого числа*. М*ожна обчислити за час поліноміальний від* N *натуральне число* $n \in [N, N + O(N^{0,77})]$ *та елемент* $\beta \in F_{q^n}$ *порядку більшого, ніж* $5{,}8^{\sqrt{n}}$.

Ченг висловив гіпотезу, що β має порядок $q^{n/2}$ при $n \geq \log q$. Ця гіпотеза має важливий наслідок, що ймовірнісний алгоритм AKS доведення простоти має часову складність $\tilde{O}(\log^3 p)$, де p ціле число, чий сертифікат простоти шукаємо. Також Ченг висловив думку, що зв'язок [44] вказаної задачі із списком декодування кодів Ріда-Соломона дозволить обійти трудність. Проте остання ідея на сьогодні залишилася нереалізованою.

Близькими до розширень Куммера є розширення на основі підпросторових поліномів (англ. термін subspace polynomials). Також такі поліноми ще називають q–лінеаризованими поліномами. Елементи великого порядку в таких розширеннях збудовано в праці [47]: для будь-якого натурального числа c та числа q, яке є степенем деякого простого числа, збудовано елемент порядку принаймні $\exp(\sqrt{q^c})$ в скінченому полі з $q^{\frac{q^c-1}{q-1}}$ елементів.

1.3.4. Елементи великого порядку виходячи з елементів малих порядків

Волох у своїх працях [143, 144] та зробленому огляді [102] розглядав описані в підрозділах 1.3.1-1.3.3 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.

Теорема 1.13. *Існує абсолютна константа* $c > 0$ *та, для кожного* $\varepsilon > 0$, *існує* $\delta > 0$, *таке, що коли* $\alpha \neq 0,1$ *є елементом скінченого поля характеристики* p *з* $\deg \alpha = n$, *то*

1. [57, 59] *Якщо* $\operatorname{ord} \alpha = n+1$, *то* $\operatorname{ord}(1-\alpha) \geq \exp(c\sqrt{n})$.

2. [107] *Якщо* $\operatorname{ord} \alpha < n^{2-\varepsilon}$, *то* $\operatorname{ord}(1-\alpha) \geq \exp(cn^{\delta})$.

Зауваження 1.3. Якщо α таке як в теоремі 1.13, частина 1, то $n+1$ просте число, а p примітивний корінь за модулем $n+1$. Аналогічно, можливі значення для n в теоремі 1.13, частина 2 обмежені.

Зауваження 1.4. Аналогічні, але слабіші, результати можна довести про порядок $R(\alpha); R \in F_p[x]$ або навіть β; $T(\alpha, \beta) = 0$; $T(\alpha, \beta) \in F_p[x, y]$, із α як в попередній теоремі [143].

Таким чином, теорема 1.13, частина 2 та останнє зауваження вказують на такий загальний підхід, який розвинув у своїх роботах Волох. Слід розглядати пари координат точок x, y на плоских кривих. Якщо одна з кординат має малий порядок, то інша має великий мультиплікативний порядок. Зокрема, теорему 1.13, частину 2 можна витлумачити так. Покладаючи $x = \alpha$ та $y = 1-\alpha$, маємо координати точок на прямій на площині, заданій рівнянням $x + y = 1$. Координата $x = \alpha$ має малий порядок, а координата $y = 1-\alpha$ – великий порядок.

У [144], Волох показав, що при певних умовах, одна з координат точки на плоскій кривій повинна мати великий порядок. Волох [143, 144] також запропонував метод побудови елементів порядку принаймні $\exp(\Omega(\log m)^2))$ у скінченних полях на основі еліптичних кривих.

Зауваження 1.5. Поонен припустив (як частина більш загальної гіпотези, див. [143]) що, з позначеннями як у попередній теоремі,

$\max\{\mathrm{ord}\alpha, \mathrm{ord}\,(1-\alpha)\} \geq \exp(cn)$. У частковому випадку припущення також зроблене Ченгом [44].

Теорема 1.14. [73] *Нехай* α *задовольняє* $\alpha^m = g$, *де* $m \mid q-1$ *і нехай* g *примітивний елемент в* F_q. *Тоді,* $\deg\alpha = m\deg g$ *та* $\mathrm{ord}\,(1-\alpha) \geq \exp(cm)$.

1.3.5. Ітеративні побудови

Особливий інтерес становить побудова елементів у рекурсивних розширеннях скінченних полів – вежах скінченних полів характеристики два або більшої від двох. З прикладної точки зору такі побудови дуже привабливі, оскільки операції над елементами скінченого поля можна виконувати рекурсивно, а тому ефективно. Такі розширення, зокрема, розглядалися в роботах [87, 150]. Для даних класів полів є висловлені, проте не доведені гіпотези, про явну форму примітивних елементів (зокрема, гіпотеза Відемана [150]).

Волох також виділяє як окремий прийом при побудові елементів великого порядку використання ітеративних побудов. Такі результати отримані ним в роботах [143, 144], а також колективом авторів у роботі [36].

Теорема 1.15. [144] *Нехай* $\alpha_0 = 1 \in F_2$, α_k *є коренем полінома* $x^2 + \alpha_{k-1}x + 1$, $k > 0$. *Тоді* $F_{2^{2^k}} = F_2(\alpha_k)$; $n = \deg\alpha_k = 2^k$ *та* $\mathrm{ord}\alpha_k \geq \exp(n^\delta)$, *для деякої абсолютної константи* $\delta > 0$.

Недоліком наведеного в теоремі 1.15 результату є те, що значення абсолютної константи δ невідоме.

Теорема 1.16. [36] *Визначимо* $f(x,y) = y^2 + (6-8x^2)y + (9-8x^2)$. *Якщо* $q = p^m$ *є натуральним степенем простого числа* $p \neq 2$ *таким, що*

$q \equiv 1 (\mathrm{mod}\, 4)$, $\alpha_0 \in F_q$ *є таким, що* $\alpha_0^2 - 1$ *не є квадратом в* F_q, *визначимо* α_k *так:* $f(\alpha_{k-1}, \alpha_k) = 0$; $k > 0$. *Нехай* $\delta_k = \alpha_k^2 - 1$. *Тоді* $n = \deg \delta_k = m2^k$ *та* $\mathrm{ord}\, \delta_k \geq \exp(c(\log n)^2)$ *для деякої константи* $c > 0$.

Останню теорему можна проінтерпретувати й по-іншому. Розглянуті в ній розширення – це розширення на основі поліномів Куммера, які мають вигляд $F_q[x]/(x^m - a)$, де $m = 2^t$. Дійсно, якщо q такий степінь простого числа, що $q \equiv 1 (\mathrm{mod}\, 4)$, то існує наступне розширення $F_{q^{2^t}} = F_q[x]/(x^{2^t} - a)$.

Теорема 1.17. [36] *Визначимо*

$$g(x, y) = y^3 + (6 - 9x^3)y^2 + (12 - 9x^3)y + (8 - 9x^3).$$

Якщо $q = p^m$ *є натуральним степенем простого числа* $p \neq 3$ *таким, що* $q \equiv 1 (\mathrm{mod}\, 3)$, $q \neq 4$, $\beta_0 \in F_q$ *є таким, що* $\beta_0^3 - 1$ *не є кубом в* F_q, *визначимо* β_k *так* $f(\beta_{k-1}, \beta_k) = 0$; $k > 0$. *Нехай* $\gamma_k = \beta_k^2 - 1$. *Тоді* $n = \deg \gamma_k = m3^k$ *та* $\mathrm{ord}\, \gamma_k \geq \exp(c(\log n)^2)$ *для деякої константи* $c > 0$.

Останню теорему можна проінтерпретувати й по-іншому. Розглянуті в ній розширення – це розширення на основі поліномів Куммера, які мають вигляд $F_q[x]/(x^m - a)$, де $m = 3^t$. Дійсно, якщо q – такий степінь простого числа, що $q \equiv 1 (\mathrm{mod}\, 3)$, то існує наступне розширення $F_{q^{3^t}} = F_q[x]/(x^{3^t} - a)$.

1.4. Області застосування елементів великого порядку в скінченних полях

Можливими областями застосування елементів великого мультиплікативного порядку в скінченних полях є, зокрема, такі [97, 99]:

- криптографія (протокол Діффі-Хелмана, криптосистема Ель-Гамаля з відкритим ключем);

- завадостійке кодування (зокрема, при побудові кодів Боуза-Чодхурі-Хоквінгема або скорочено БЧХ-кодів);

- генератори псевдовипадкових чисел (різні степені елемента великого порядку можна розглядати як послідовність псевдовипадкових чисел);

- доведення простоти чисел. Елементи великого порядку використовують в алгоритмі AKS доведення простоти чисел, запропонованому Агравалом, Кайалом та Саксеною [23].

Застосування елементів великого мультиплікативного поряку в криптографії грунтується на так званій задачі дискретного логарифмування в будь-якій скінченній циклічній групі (див. зауваження 1.1).

Дискретні логарифми – це логарифми, визначені стосовно мультиплікативних циклічних груп. Якщо G – мультиплікативна циклічна група, а g – твірний елемент групи G, то визначення циклічних груп дає, що кожен елемент h в G можна записати як g^x для деякого x. Дискретний логарифм за основою g елемента h в циклічній групі G визначаємо рівним числу x. Наприклад, якщо як групу беремо Z_5^*, а твірний елемент дорівнює 2, то дискретний логарифм елемента 1 рівний 4, бо $2^4 \equiv 1 \bmod 5$.

Задачу дискретного логарифма формулюємо так: маючи групу G, твірний елемент g цієї групи та елемент h групи G, знайти дискретний елемент за основою g елемента h групи G.

Нехай G – скінченна циклічна група, яка має q елементів, з твірним елементом g. Використовуючи послідовні піднесення до квадрату, можна швидко (за поліноміальний час) обчислити $h = g^X$ для будь-якого додатного цілого числа $1 \le x \le q-1$. Вважається, що маючи якийсь h, обчислювально складно знайти дискретний логарифм від нього за основою g, тобто число x.

Іншими словами, функція $f(x) = g^x$ є однонапрямленою. Проте, доведення цього на сьогодні немає.

Виходячи із задачі дискретного логарифмування переважно розглядають такі дві криптографічні схеми.

1) Протокол Діффі-Хелмана

Як можуть два користувачі узгодити таємний ключ (можливо, для криптосистеми з таємним ключем) через відкритий канал зв'язку ?

Користувачі погоджують G –скінченну циклічну групу, яка має q елементів, та її твірний елемент g. Як G, так і g, є відкритими.

Користувач A: вибирає випадкове число $1 \le a \le q-1$, обчислює g^a та пересилає значення g^a користувачу B.

Користувач B: вибирає випадкове число $1 \le b \le q-1$, обчислює g^b та пересилає значення g^b користувачу A.

Користувач A обчислює $(g^b)^a$.

Користувач B обчислює $(g^a)^b$.

Тепер як користувач A, так і користувач B мають елемент групи G рівний g^{ab}, який може слугувати як узгоджений таємний ключ.

2) Криптосистема Ель-Гамаля (криптосистема з відкритим ключем)

Нехай G – скінченна циклічна група, яка має q елементів, з твірним елементом g. Як G, так і g, є відкритими.

Кожен користувач U: вибирає випадкове число $1 \le a \le q-1$ – секретний ключ для дешифрування. Тоді обчислює g^a і виставляє його – це публічний ключ цього користувача.

Щоб переслати таємне повідомлення P користувачу U,: слід вибрати випадкове число k, тоді обчислити та переслати пару значень $\beta_1 = g^k, \beta_2 = P(g^a)^k$.

Користувач U виконує дешифрування згідно з таким виразом $P = \beta_2(\beta_1)^{-a}$.

Зауважимо, що не обов'язково g мусить бути твірним елементом групи G. Перша та друга описані криптографічні схеми працюють для будь-якого випадкового елемента g. Разом з тим їх стійкість до зламування залежить від мультиплікативного порядку елемента g. Цей порядок елемента у вибраній скінченній циклічній групі мусить бути достатньо великим.

У криптографії можливе застосування як G таких скінченних циклічних груп:

1) Мультиплікативна група простого поля $F_p^* = \{1,..., p-1\}$, яка співпадає із $Z_p^* = \{1,..., p-1\}$ – множиною ненульових цілих чисел відносно множення за модулем великого простого числа p.

2) Еліптична крива $E(F_q)$ над скінченним полем F_q. Її переважно записують не в мультиплікативній, а в адитивній формі. Така крива – це множина пар (x, y) елементів вибраного поля, що задовольняють афінне рівняння еліптичної кривої в нормальній формі Веєрштраса

$$y^2 + xy = x^3 + Ax^2 + B,$$

де $A, B \in F_q$, $B \neq 0$, разом із приєднаною нескінченною віддаленою точкою O. Пара (x, y) елементів основного поля називається афінними координатами точки еліптичної кривої. Нескінченно віддалена точка O не має афінних координат. Елементи A, B основного поля називаються коефіцієнтами рівняння еліптичної кривої. Число точок еліптичної кривої разом з нескінченною точкою називається порядком еліптичної кривої.

3) Мультиплікативна група розширеного скінченного поля $F_{q^n}^*$.

Цю групу описано в підрозділі 1.1. Явній побудові елементів великого мультиплікативного порядку в ній присвячено дану дисертаційну роботу.

Задача дискретного логарифма не завжди є важкою. Складність знаходження дискретного логарифма залежить від вибраної групи. Наприклад, популярним вибором групи для криптосистем на основі дискретного логарифма є Z_p^* , де p – просте число. Проте, якщо $p-1$ є добутком малих простих чисел, то алгоритм Поліга-Хелмана [99] може розв'язати задачу дискретного логарифма у цій групі дуже ефективно. Ось чому ми завжди хочемо, щоб p було безпечним простим числом, коли використовуємо Z_p^* як основу криптосистем, заснованих на дискретному логарифмі. Безпечне просте число – це просте число, яке дорівнює $2q+1$, де q – велике просте число. Це гарантує, що $p-1=2q$ має великий простий множник, а, значить, вже згаданий алгоритм Поліга-Хелмана не може легко розв'язати задачу дискретного логарифма. Якщо p – безпечне просте число, то є субекспоненційний алгоритм, який називають обчислення індекса [99]. Це означає, що p повинне бути дуже великим (звичайно принаймні 1024-біт), щоб зробити криптосистему безпечною.

Крім атаки Поліга-Хелмана на задачу дискретного логарифма та атаки обчислення індекса, в літературі також описано [99] атаку Шенкса, алгоритм малого-великого кроку, алгоритм Полларда Rho.

Відомі алгоритми знаходження дискретного логарифма [99] можна класифікувати наступним чином:

1. алгоритми, які працюють в довільних групах, наприклад, повне перебирання, алгоритм Шенкса великих та малих кроків, ρ-алгоритм Полларда.
2. алгоритми, які працюють в довільних групах, але особливо ефективні, якщо порядок групи має лише малі прості дільники, наприклад алгоритм Поліга-Хелмана

3. метод обчислення індексів, який є ефективним лише для певних груп.

Алгоритм обчислення індексів є найпотужнішим методом, відомим для обчислення дискретних логарифмів. Ця техніка незастосовна для будь-яких груп. Проте, якщо її можна застосувати, вона завжди дає субекспоненційний за часом виконання алгоритм.

Опишемо спочатку цей алгоритм для довільної циклічної групи G. Алгоритм вимагає вибору відносно малої підмножини S елементів із G, яку називають базою розкладу, в такий спосіб, що значна частина елементів з G може бути ефективно виражена як добутки елементів з S. Наведений далі опис алгоритму попередньо обчислює базу даних логарифмів всіх елементів з S, а потім використовує цю базу даних кожен раз, коли потрібний логарифм певного елемента групи.

Опис алгоритму неповний з двох причин. По-перше, не визначена техніка вибору бази розкладу. По-друге, метод для ефективного утворення співвідношень вигляду (1.1) та (1.3) не визначений.

Опис алгоритму

ВХІД: твірний елемент α циклічної групи G порядку n та елемент $\beta \in G$.

ВИХІД: дискретний логарифм $y = \log_\alpha \beta$.

1. (*Вибір бази розкладу* S) Вибрати під множину $S = \{p_1, p_2, ..., p_t\}$ в G таку, що значна частка від всіх елементів у групі G може бути ефективно записана як добуток елементів з S.

2. (*Збирання лінійних співвідношень, у яких задіяні логарифми елементів з* S)

2.1 Вибрати випадкове число k, $0 \le k \le n-1$, та обчислити α^k.

2.2. Спробувати записати α^k як добуток елементів із S:

$$\alpha^k = \prod_{i=1}^{t} p_i^{c_i}, (c_i \ge 0). \qquad (1.1)$$

Якщо спроба успішна, то взяти логарифми від обидвох частин рівняння (1.1), щоб отримати лінійне співвідношення

$$k \equiv \sum_{i=1}^{t} c_i \log_\alpha p_i \pmod{n}. \qquad (1.2)$$

2.3. Повторювати кроки 2.1 та 2.2 поки не буде отримано $t+c$ співвідношень вигляду (1.2) (c – найменше натуральне число таке, що система рівнянь із $t+c$ співвідношень з високою ймовірністю має єдиний розв'язок).

3. (*Знаходження логарифмів елементів з* S) Виконуючи обчислення за модулем числа n, розв'язати систему $t+c$ лінійних рівнянь (з t невідомими) вигляду (1.2), назбираних на кроці 2, щоб отримати значення $\log_\alpha p_i$, $1 \le i \le t$.

4. (Обчислення y)

4.1 Вибрати випадкове число k, $0 \le k \le n-1$, та обчислити $\beta \cdot \alpha^k$.

4.2. Спробувати записати $\beta \cdot \alpha^k$ як добуток елементів із S:

$$\alpha^k = \prod_{i=1}^{t} p_i^{d_i}, (d_i \ge 0). \qquad (1.3)$$

Якщо спроба невдала, то повторити крок 4.1. В іншому разі, беручи логарифми від обидвох частин рівняння (1.3), знайти $\log_\alpha \beta \equiv \left(\sum_{i=1}^{t} d_i \log_\alpha p_i - k \right) \bmod n$. Повернути $y = \log_\alpha \beta$.

Для поля Z_p^*, де $p-$ просте число, база розкладу S може бути вибрана як перші t простих чисел. Наведений далі приклад ілюструє алгоритм обчислення індексів у Z_p^* із штучно вибраними невеликими параметрами.

Нехай $p = 229$. Елемент $\alpha = 6$ є твірним елементом для Z_{229}^* порядку $n = 228$. Розглянемо $\beta = 13$. Тоді $\log_6 13$ обчислємо наступним чином, використовуючи техніку обчислення індексів.

1. Як базу розкладу вибираємо перші п'ять простих чисел: $S = \{2,3,5,7,11\}$.

2. Отримуємо наступні шість співвідношень, які включають елементи із бази розкладу (невдалі спроби не показано):

$$6^{100} \bmod 229 = 180 = 2^2 \cdot 3^2 \cdot 5$$

$$6^{18} \bmod 229 = 176 = 2^4 \cdot 11$$

$$6^{12} \bmod 229 = 165 = 3 \cdot 5 \cdot 11$$

$$6^{62} \bmod 229 = 154 = 2 \cdot 7 \cdot 11$$

$$6^{143} \bmod 229 = 198 = 2 \cdot 3^2 \cdot 11$$

$$6^{206} \bmod 229 = 210 = 2 \cdot 3 \cdot 5 \cdot 7$$

Ці співвідношення породжують такі шість рівнянь, які включають логарифми елементів з бази розкладу:

$$100 \equiv 2\log_6 2 + 2\log_6 3 + 2\log_6 5 \pmod{228}$$

$$18 \equiv 4\log_6 2 + \log_6 11 \pmod{228}$$

$$12 \equiv \log_6 3 + \log_6 5 + \log_6 11 \pmod{228}$$

$$62 \equiv \log_6 2 + \log_6 7 + \log_6 11 \pmod{228}$$

$$143 \equiv \log_6 2 + 2\log_6 3 + \log_6 11 \pmod{228}$$

$$206 \equiv \log_6 2 + \log_6 3 + \log_6 5 + \log_6 7 \pmod{228}$$

3. Розв'язуючи лінійну систему шести рівнянь з п'ятьма невідомими, отримуємо розв'язки $\log_6 2 = 21$, $\log_6 3 = 208$, $\log_6 5 = 98$, $\log_6 7 = 107$, $\log_6 11 = 162$.

4. Припустимо, що вибрано натуральне число $k = 77$. Оскільки

$$\beta \cdot \alpha^k = 13 \cdot 6^{77} \bmod 229 = 147 = 3 \cdot 7^2,$$

то з цього випливає, що

$$\log_6 13 = (\log_6 3 + 2\log_6 7 - 77) \bmod 228 = 117.$$

Для поля $F_{2^m} = F_2[x]/(f(x))$, де $f(x)$ – нерозкладний поліном степеня m над F_2, база розкладу S може бути вибрана як множина всіх нерозкладних поліномів над початковим полем степеня щонайбільше деяка задана межа b. Наведений далі приклад ілюструє алгоритм обчислення індексів у F_{2^m} із штучно вибраними невеликими параметрами.

Нехай $f(x)=x^7+x+1$. Елемент $\alpha=x$ є твірним елементом для групи $F_{2^7}^*$ порядку $n=127$. Розглянемо $\beta=x^4+x^3+x^2+x+1$. Тоді $\log_x\beta$ обчислємо наступним чином, використовуючи техніку обчислення індексів.

1. Як базу розкладу вибираємо множину нерозкладних поліномів степеня щонайбільше 3: $S=\{x,x+1,x^2+x+1,x^3+x+1,x^3+x^2+1\}$.

2. Отримуємо наступні п'ять співвідношень, які включають елементи із бази розкладу (невдалі спроби не відображено):

$$x^{18}\bmod f(x)=x^6+x^4=x^4(x+1)^2$$

$$x^{105}\bmod f(x)=x^6+x^5+x^4+x=x(x+1)^2(x^3+x^2+1)$$

$$x^{72}\bmod f(x)=x^6+x^5+x^3+x^2=x^2(x+1)^2(x^2+x+1)$$

$$x^{45}\bmod f(x)=x^5+x^2+x+1=(x+1)^2(x^3+x+1)$$

$$x^{121}\bmod f(x)=x^6+x^5+x^4+x^3+x^2+x+1=(x^3+x+1)(x^3+x^2+1)$$

Ці співвідношення породжують такі п'ять рівнянь, які включають логарифми елементів з бази розкладу (для зручності позначимо $p_1=\log_x x$, $p_2=\log_x(x+1)$, $p_3=\log_x(x^2+x+1)$, $p_4=\log_x(x^3+x+1)$, $p_5=\log_x(x^3+x^2+1)$):

$$18\equiv 4p_1+2p_2\ (\mathrm{mod}127)$$

$$105\equiv p_1+2p_2+p_5\ (\mathrm{mod}127)$$

$$72\equiv 2p_1+2p_2+p_3\ (\mathrm{mod}127)$$

$$45\equiv 2p_2+p_4\ (\mathrm{mod}127)$$

$$121\equiv p_4+p_5\ (\mathrm{mod}127)$$

3. Розв'язуючи лінійну систему п'яти рівнянь з п'ятьма невідомими, отримуємо розв'язки $p_1=1$, $p_2=7$, $p_3=56$, $p_4=31$, $p_5=90$.

4. Припустимо, що вибрано натуральне число $k=66$. Оскільки

$$\beta\cdot\alpha^k=(x^4+x^3+x^2+x+1)x^{66}\bmod f(x)=x^5+x^3+x=x(x^2+x+1)^2,$$

то з цього випливає, що

$$\log_x(x^4 + x^3 + x^2 + x + 1) = (p_1 + 2p_3 - 66) \bmod 127 = 47 .$$

1.5. Висновки до розділу

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 відповідному для цього вигляді. Проведено огляд відомих результатів, наведених у літературі.

РОЗДІЛ 2

Допоміжні факти, методи дослідження

2.1. Необхідні для подальшого викладу відомі результати

2.1.1. Гауссові періоди

К. Ф. Гаусс у 1801 році ввів своє поняття періоду наступним чином [1, 76]. Нехай n, k та r – натуральні числа, для яких виконуються умови r – просте число та

$$nk = \varphi(r) = r - 1.$$

Крім того, $\varsigma \in \mathrm{C}$ – примітивний корінь r-го степеня з одиниці, а $K \subseteq Z_r^* = \mathrm{Gal}(\mathrm{Q}(\varsigma) : \mathrm{Q})$ – єдина підгрупа порядку k циклічної групи Z_r^*. Тоді елемент вигляду

$$\eta = \sum_{i \in K} \varsigma^i = \mathrm{Q}(\varsigma).$$

є гауссовим періодом типу (n, K) над Q. З цією побудовою пов'язана така вежа полів характеристики ноль:

$$\mathrm{Q} \subset \mathrm{Q}(\eta) \subset \mathrm{Q}(\varsigma)$$

та відповідний ланцюг скінченних груп

$$\{1\} \subset K \subseteq Z_r^*.$$

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

Над скінченним полем F_q можна розглядати аналогічну ситуацію: маємо n, k, r та $K \subseteq Z_r^*$ як раніше, а також вимагаємо $\gcd(q,r)=1$. Також беремо $\theta \in F_{q^{r-1}}$ – примітивний корінь r–го степеня з одиниці та покладаємо

$$\beta = \sum_{i \in K} \theta^i = F_{q^n}.$$

Тоді елемент β є гауссовим періодом типу (n,K) над F_q. Зокрема, елемент $\beta = \theta + \theta^{-1}$ називають гауссовим періодом типу $(\frac{r-1}{2}, 2)$.

Певні гауссові періоди над скінченними полями породжують нормальні бази. Тоді можемо ефективно [76] виконувати операцію піднесення до степеня у відповідному скінченому полі.

2.1.2. Розбиття числа

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. $U(C)$ позначатиме число розбиттів числа C. $U(C,d)$ позначатиме число таких розбиттів C, для яких $u_1,\ldots,u_C \le d$, тобто кожна частина розбиття з'являється не більше, ніж d разів. $Q(C,d)$ позначатиме число таких розбиттів C, для яких $u_j = 0$, якщо $j \equiv 0 \bmod d$, тобто кожна частина не ділиться на d.

Згідно з [24, наслідок 1.3], кількість розбиттів числа n, які не мають d однакових частин, дорівнює кількості розбиттів n, для яких ні одна частина не ділиться на d. Вказане формулювання можна записати у вигляді такої рівності:

$$U(n,d-1)=Q(n,d). \qquad (2.1)$$

Явна нижня межа для $Q(n,d)$ при $n \geq d^2$ наведена в [98]. Якщо $n<d$, то, зрозуміло, що $U(n,d-1)=U(n)$. Явна нижня межа для $U(n)$ для всіх натуральних чисел n також наведена в [24].

Більш точно, згідно з [98, теорема 5.1], для $d>1$ та $n \geq d^2$ виконується така нерівність:

$$Q(n,d) > \left(\frac{d(d-1)}{160n}\right)^{\sqrt{d}} \exp\left(2.5\sqrt{(1-\frac{1}{d})n}\right). \qquad (2.2)$$

Згідно з [98, теорема 4.2], для всіх натуральних чисел n виконується наступна нерівність:

$$U(n) > \frac{\exp\left(2.5\sqrt{n}\right)}{13n}. \qquad (2.3)$$

2.1.3. Нижні оцінки для біноміальних коефіцієнтів

Далі даємо відомі результати [132], які дозволяють отримувати нижні оцінки для певних біноміальних коефіцієнтів.

Посилену нерівність для біноміальних коефіцієнтів було отримано в [132, наслідок 2.9, нерівність (2.13)]. Більш точно, отримано такий результат.

Лема 2.1. Нехай r,s,t такі натуральні числа, які задовольняють умови $s>r \geq 1$ та $t \geq 2$. Тоді

$$\binom{st}{rt} > (1/\sqrt{2\pi}) \cdot e^{r-1/(8t)} \cdot t^{-1/2} \frac{s^{s(t-1)+1}}{(s-r)^{(s-r)(t-1)-r+1} \cdot r^{rt+1/2}}. \qquad (2.4)$$

Виходячи з леми 2.1, можна отримати такий наслідок.

Наслідок 2.1. Для $s>1$ та $t\geq 2$ виконується нерівність

$$\binom{st}{t} > (1/\sqrt{2\pi})\cdot e^{1-1/(8t)}\cdot t^{-1/2}\,\frac{s^{s(t-1)+1}}{(s-1)^{(s-1)(t-1)}}. \qquad (2.5)$$

2.2. Задачі, які вирішуються в дисертаційній роботі

Початково ідея використання ABC теореми Стовера–Мейсона для підсилення оцінки для порядку певних мультиплікативних підгруп скінченних кілець висловлена в праці [145]. Далі цю думку розвинув Д. Бернштейн [29]. Пропозицію використати ABC теорему для поліпшення оцінки для порядку гауссового періоду навели як відкрите питання автори праці [22]. У дисертаційній роботі дається часткова відповідь на вказане відкрите питання.

Для довільних полів вигляду $F_q[x]/(x^m-a)$ не було оцінки порядку елементів. Для розширень Куммера не було точної нижньої оцінки порядку елементів, які є лінійними двочленами відносно елемента, що задають вказане розширення. Такі оцінки отримано в даній роботі.

Для полів на основі поліномів Артіна-Шраєра не було оцінки порядку елементів, які задають вказане розширення. Таку оцінку отримано в дисертаційній роботі.

Особливий інтерес становить побудова елементів у рекурсивних розширеннях скінченних полів – вежах скінченних полів характеристики два або більшої від двох. З прикладної точки зору такі побудови дуже привабливі, оскільки операції над елементами скінченого поля можна виконувати рекурсивно, а тому ефективно. Такі розширення, зокрема, розглядалися в роботах [86, 87, 150]. Для даних класів полів є висловлені,

проте не доведені гіпотези, про явну форму примітивних елементів (зокрема, гіпотеза Відемана [150]). Для веж скінченних полів не було оцінок знизу мультиплікативних порядків елементів. Низку таких оцінок для різних веж скінченних полів (як характеристики два, так і характеристики більшої від двох) отримано в даній роботі.

Для веж скінченних полів, визначених Конвеєм, не були відомі (крім кількох перших полів у вежі) ніякі примітивні елементи та їх форма. Форму певних примітивних елементів для вказаних веж полів отримано в дисертаційній роботі.

Для загальних розширень скінченних полів стояло питання підсилити нижню межу для мультиплікативного порядку деяких елементів на основі підходу Гао-Конфлітті. Це зроблено в даній роботі. Також стояла задача отримати нижні межі для порядків без використання гіпотези Гао. Такі оцінки виведено в дисертаційній роботі. Ще одним питанням, яке виникло, було вивчення зв'язку між елементами великого мультиплікативного порядку та доведенням простоти великих натуральних чисел. Вказане питання розглянуте в цій роботі.

2.3. Підходи, використані в дисертаційній роботі

У даній дисертаційній роботі, зокрема, використано такі описані далі підходи.

1) Заміна елемента на його автоморфний образ

Згідно з лемою 1.1, спряжені елементи над будь-яким підполем мають однаковий мультиплікативний порядок. Таким чином, при отриманні нижньої межі для мультиплікативного порядку якогось елемента скінченого

поля цей елемент можна замінити на спряжений йому. Далі вивести нижню межу для елемента-заміни.

Такий прийом неодноразово використовуємо в третьому розділі. Зокрема, елемент $\theta^e(\theta^f + a)$ заміняємо на $\theta^g(\theta + a)$, де e – довільне натуральне число, f – довільне натуральне число взаємно просте з r, a – будь-який ненульовий елемент скінченого поля F_q. $g \equiv ef^{-1} \bmod r$. За рахунок цього зменшуємо степінь елемента як полінома від змінної θ і можемо показати, що цей елемент має більше різних степенів. У частковому випадку заміняємо гауссовий період $\beta = \theta + \theta^{-1} = \theta^{-1}(\theta^2 + 1)$ на його автоморфний образ. Це дає змогу підсилити відому оцінку порядку з роботи [22] та дати відповідь на наведене в даній роботі відкрите питання.

2) Комбінування двох варіантів оцінювання порядку

У четвертому розділі комбінуємо два варіанти явної побудови елемента великого мультиплікативного порядку в розширеннях скінченних полів на основі поліномів Куммера. Вибір варіанту спирається на аналізі величини певного параметра. Цей параметр отримуємо в результаті розкладу степеня m розширення початкового поля F_q на два множники $m = m_1 m_2$. При цьому m_1 є дільником $q - 1$. Перший із множників m_1 і є вказаним параметром. Якщо цей параметр великий, то елемент великого порядку будуємо так, як це роблять для розширень Куммера і описано в підрозділі 4.1. Якщо ж параметр m_1 – малий, то тоді другий множник m_2 є великим. Тоді будуємо елемент великого мультиплікативного порядку аналогічно до того, як це роблять для циклотомічних розширень і описано в розділі 3. Оскільки добуток $m = m_1 m_2$ – це задана величина, то обов'язково спрацьовує один із двох варіантів.

3) Використання різних відповідних понять

а) поняття розбиття натурального числа

Початково всі нижні межі у випадку циклотомічних розширень скінченних полів сформульовано у термінах розбиття. Це викликане тим, що для оцінки кількості розбиттів заданого числа існує добре розвинута теорія, зокрема монографія [24] Ендрюса “Теорія розбиттів”. Проте з точки зору прикладних застосувань найцікавішими є явні нижні межі. Тому нами додатково використано маловідому роботу [98] Мароті “Про елементарні нижні межі для функції розбиття”, де є наведено явні нижні межі для кількості розбиттів.

Розбиття фігурують і в четвертому розділі роботи.

б) діофантові нерівності та оптимізація кількості їх розв’язків

Використання діофантових нерівностей означає, що порівняно з використанням поняття розбиття знак дорівнює заміняємо на знак менше-дорівнює. Зрозуміло, що кількість варіантів збільшується, і їх власне підраховуємо. Оскільки ця кількість залежить від певного параметра, то його підбираємо так, щоб зробити кількість розв’язків максимальною. Для цього знаходимо максимум відповідної функції. Цей прийом використано в третьому та четвертому розділах.

4) Використання ABC-теореми для поліномів.

Згідно з працею [29] для поліномів справедлива теорема, яку часто називають ABC теоремою Стовера–Мейсона. З цієї теореми як наслідок отримано теорему 7.6, формулювання якої наведене в сьомому розділі. Це формулювання означає, що коли степені трьох поліномів обмежені величиною степеня полінома, який задає розширене поле, то вони одночасно не можуть бути рівними за модулем цього полінома. Застосовуючи вказаний результат, можна отримати кращу нижню оцінку для мультиплікативного порядку елемента, який задає розширення скінченого поля.

5) Комп’ютерні обчислення

У випадках, коли не можемо отримати бажаний результат теоретично, застосовуємо комп’ютерні обчислення. Їх використано в четвертому, п’ятому, шостому та сьомому розділах. Обчислення виконано з використанням як середовища Maple, так і власних програм, написаних з використанням середовища візуального програмування Delphi.

У п’ятому розділі комп’ютерні обчислення дозволили перевірити, що певні елементи є примітивними для обмеженої кількості значень простого числа p, яке задає скінченне поле. Також отримано часткові результати для трохи більших значень даного простого числа. В підрозділі 5.3 комп’ютерні обчислення використано, щоб показати, що значення з роботи [30] не є нижньою межею для добутку біноміальних коефіцієнтів, а лише певним наближеним значенням.

У шостому розділі знайдено певні примітивні елементи для перших одинадцяти полів у вежах скінченних полів, визначених Конвеєм. Виходячи з цих результатів, маємо припущення про вигляд примітивних елементів у цих вежах в загальному.

У сьомому розділі частково перевірено гіпотезу Аггравала, пов’язану з тестуванням великих натуральних чисел на простоту. Крім власного коду тут також використано певні бібліотечні модулі для роботи з великими числами.

Звичайно, у майбутньому бажано було б комп’ютерні обчислення при отриманні певних результатів по можливості замінити на строгі математичні доведення.

Суть інших методів, використаних в дисертаційній роботі, наводиться безпосередньо при доведенні основних результатів роботи.

2.4. Висновки до розділу

У першому підрозділі даного розділу наведено необхідні для подальшого викладу відомі результати (поняття гауссових періодів; розбиття числа; нижні оцінки для величин біноміальних коефіцієнтів).

У другому підрозділі розглянуто, які задачі вирішуються в дисертаційній роботі. Це задачі отримання нижніх меж для мультиплікативних порядків елементів як у часткових, так і в загальних розширеннях скінченнях полів.

У третьому підрозділі описано, які підходи використано при розв’язанні поставлених задач.

РОЗДІЛ 3

Елементи великого порядку в скінченних полях на основі циклотомічних поліномів

У даному розділі розглядаємо розширення скінченних полів, які пов'язані з поняттям гауссового періоду. Нагадаємо, що вказане поняття визначене в розділі 2. Нехай $r = 2s + 1$ – просте число, яке взаємно просте з q. Нехай q є примітивним коренем за модулем r, тобто мультиплікативний порядок числа q за модулем r дорівнює $r - 1$. Для r-го циклотомічного полінома $x^{r-1} + x^{r-2} + ... + x + 1$ будемо використовувати позначення $\Phi_r(x)$.

Теорема 2.47, частина (ii), із роботи [97] дає змогу отримати необхідну і достатню умову нерозкладності циклотомічного полінома $\Phi_r(x)$ над полем F_q. Згідно з цією теоремою поліном $\Phi_r(x)$ розкладається над полем F_q в добуток $\frac{\varphi(r)}{d}$ різних унітарних нерозкладних поліномів однакового степеня d, де число d – найменше натуральне число таке, що $q^d \equiv 1 \pmod r$. Тому в даному випадку поліном $\Phi_r(x)$ – нерозкладний над F_q, і фактор-кільце $F_q[x]/\Phi_r(x)$ є полем.

Будемо надалі використовувати наступні позначення:

$$F_q(\theta) = F_{q^{r-1}} = F_q[x]/\Phi_r(x),$$

де $\theta = x \pmod{\Phi_r(x)}$ – суміжний клас елемента x за модулем циклотомічного полінома $\Phi_r(x)$.

Очевидно, що виконується рівність $\theta^r = 1$. Елемент $\beta = \theta + \theta^{-1}$ називають гауссовим періодом типу $\left(\frac{r-1}{2}, 2\right)$. Він породжує нормальний базис над полем F_q. Розширення, пов'язані з поняттям гауссового періоду, розглянуті в роботах [22, 75–78]. Нижня границя на порядок дорівнює $\exp(\sqrt{r})$. Ці розширення існують для нескінченної кількості чисел r, якщо для числа q виконується гіпотеза Артіна (див. [82, 83]). У теорії чисел, гіпотеза Артіна про примітивні корені стверджує, що задане ціле число q , яке не є квадратом іншого цілого числа або числом -1, є примітивним коренем за модулем нескінченної кількості простих чисел p. Гіпотеза також описує асимптотичну щільність цих простих чисел.

У праці [22] показано, що порядок елемента β є принаймні $U((r-3)/2, p-1)$. У підрозділі 3.1, ми узагальнюємо цей результат на елементи більш загального вигляду, ніж β, та показуємо, що для для будь-якого натурального числа e, будь-якого натурального числа f взаємно простого з r, будь-якого ненульового елемента a з поля F_q, порядок елемента $\theta^e(\theta^f + a)$ в полі $F_q(\theta)$ є принаймні $U(r-2, p-1)$. Зокрема, мультиплікативний порядок гауссового періоду

$$\beta = \theta + \theta^{-1} = \theta^{-1}(\theta^2 + 1)$$

є принаймні $U(r-2, p-1)$. Ця межа покращує попередню межу $U((r-3)/2, p-1)$ Ахмаді, Шпарлінского та Волоха [22]. Показуємо, що порядок елемента $\theta^e(\theta^f + a)$ при умові $a^2 \neq \pm 1$ є принаймні $[U((r-3)/2, p-1)]^2/2$. Використовуючи елементи β та $(\theta^{-1} + a)(\theta + a)^{-1}$, ми також будуємо елемент порядку принаймні

$$[U(r-2, p-1)\cdot U((r-3)/2, p-1)]/2.$$

В другому підрозділі, отримуємо, використовуючи результати з [24, 98], явні нижні межі для мультиплікативних порядків в термінах характеристики поля p та степеня розширення r. У третьому підрозділі, даємо низку числових прикладів для отриманих раніше результатів. В четвертому підрозділі наведено модифікацію нижніх меж для порядків на основі кількості розв'язків лінійної діофантової нерівності. У п'ятому підрозділі отримано асимптотичні нижні межі для мультиплікативних порядків елементів. В останньому підрозділі зроблено висновки до третього розділу.

3.1. Нижні межі для порядків на основі поняття розбиття натурального числа

У даному підрозділі, доводимо далі теорему 3.1. яка дає нижню межу для мультиплікативних порядків певних елементів скінченого поля. Елементи з пункту (a) теореми 3.1 мають більш загальний вигляд, ніж гауссовий період типу $\left(\frac{r-1}{2}, 2\right)$. Пункти (b), (c) та (d) додані до формулювання теореми, бо мультиплікативна група $F_{q^{r-1}}^{*}$ містить внутрішній прямий добуток двох груп. Елементи з пункту (b) використовуємо для побудови підгрупи першої групи. Елементи з пункту (c) використовуємо для побудови підгрупи другої групи. Елементи з пункту (d) є твірними прямого добутку цих двох груп. Обчислення, зроблені далі в третьому підрозділі показують, що нижня межа для порядків цих елементів є кращою, ніж порядки елементів з пункту (a). Проте, елементи з пункту (d), на відміну від елементів із пункту (a), не є узагальненням гауссового періоду.

Елементи з наслідку 3.2 є твірними аналогічного до випадку теореми 3.1 прямого добутку двох підгруп. Перша із вказаних підгруп збудована з використанням гауссового періоду. Друга підгрупа будується, використовуючи елементи з пункту (c). Обчислення показують, що нижня межа для порядків цих елементів краща, ніж для порядків елементів із пункту (d).

Всі нижні межі в теоремі 3.1 використовують поняття розбиття натурального числа, де кожна частина з'являється не більше, ніж $p-1$ раз. Використовуємо для доведення пунктів (a), (b), (c) цієї теореми техніку, подібну до використаної в праці [22].

Якщо елемент $\alpha \in F$ є алгебраїчним над полем K, то однозначно визначений унітарний поліном $g \in K[x]$, який породжує ідеал $J = \{f \in K[x] \mid f(\alpha) = 0\}$ кільця $K[x]$ називають мінімальним поліномом (або визначальним поліномом, або нерозкладним поліномом) елемента α над K. Степенем α над K називаємо степінь полінома g. Поліном g є унітарним поліномом з кільця $K[x]$ найменшого степеня, для якого елемент α є коренем.

Нехай поле F_{q^m} є розширенням поля F_q і нехай $\alpha \in F_{q^m}$. Тоді елементи α, α^q, α^{q^2},..., $\alpha^{q^{m-1}}$ називають спряженими елемента α відносно поля F_q. Спряжені елемента α відносно поля F_q є різними тоді і тільки тоді, коли мінімальний поліном елемента α над полем F_q має степінь m. В іншому випадку, степінь d цього мінімального полінома є власним дільником числа m, і тоді спряжені елемента α відносно поля F_q є різними елементами α, α^q, ..., $\alpha^{q^{d-1}}$, причому кожен з них повторюється $\frac{m}{d}$ разів.

Припустимо, що $f \in K[x]$ є мінімальним поліномом елемента α над полем K, а степінь d цього полінома є дільником числа m. Тоді

$g(x) = f(x)^{\frac{m}{d}} \in K[x]$ називають характеристичним поліномом елемента α над полем K. Як було зауважено, корені полінома f виглядають так: α, α^q, …, $\alpha^{q^{d-1}}$, і тоді корені g в полі F є точно спряженими елемента α відносно поля K. Таким чином, маємо

$$g(x) = (x-\alpha)(x-\alpha^q)...(x-\alpha^{q^{m-1}}).$$

У випадку, якщо $d = m$ отримуємо $f = g$, тобто мінімальний та характеристичний поліноми елемента співпадають. Власне таку ситуацію маємо в даному розділі, бо $m = r-1$ та $d = \deg\Phi_r(x) = r-1$. Поняття мінімального полінома використовуємо при отриманні результатів, а саме: доведенні теореми 3.1, леми 3.1, леми 3.2 та леми 3.3. Виходячи з вище сказанного можна було б використовувати й рівносильне поняття характеристичного полінома, що роблять інші автори, зокрема в праці [22].

Теорема 3.1. *Нехай q – степінь простого числа p, $r = 2s+1$ – просте число взаємно просте з q, q – примітивний корінь за модулем r, елемент θ задає розширення $F_q(\theta) = F_{q^{r-1}}$, e – довільне цілее число, f – довільне ціле число взаємно просте з r, a – будь-який ненульовий елемент скінченого поля F_q. Тоді справедливі такі 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* $[U((r-3)/2, p-1)]^2/2$.

Доведення. (*a*) Очевидно, що відображення, яке переводить елемент θ в елемент θ^p, є автоморфізмом Фробеніуса поля $F_q(\theta)$. Оскільки число q – примітивне за модулем r, то знайдеться таке натуральне число m, для якого порівняння $f \equiv q^m \bmod r$ справедливе. Так як q є степенем p, то відображення, що переводить елемент θ в $\theta^f = \theta^{q^m}$, є степенем автоморфізму Фробеніуса і, тому, також є автоморфізмом поля $F_q(\theta)$. Оскільки останній розглянутий автоморфізм відображає елемент $\theta^g(\theta + a)$ в $\theta^e(\theta^f + a)$, де $g \equiv ef^{-1} \bmod r$, то мультиплікативні порядки цих елементів співпадають. Значить, достатньо довести, що елемент $\theta^g(\theta + a)$ для будь-якого натурального числа g має мультиплікативний порядок принаймні $U(r-2, p-1)$.

Так як q – примітивне за модулем r, то для кожного $j = 1,...,r-2$, існує таке натуральне число α_j, що $q^{\alpha_j} \equiv j \bmod r$. Степені

$$\left(\theta^g(\theta + a)\right)^{q^{\alpha_j}} = \theta^{gq^{\alpha_j}}(\theta^{q^{\alpha_j}} + \mathrm{a}) = \theta^{gj}(\theta^j + \mathrm{a})$$

належать до групи $<\theta^g(\theta + a)>$. Нехай S_1 – множина розбиттів $(u_1,...,u_{r-2})$ натурального числа $r-2$, де кожна частина з'являється не більше, ніж $p-1$ раз, тобто виконується умова

$$\sum_{j=1}^{r-2} ju_j = r-2,\ 0 \le u_1,...,u_{r-2} \le p-1.$$

Для кожного розбиття із визначеної множини S_1 ми будуємо наступний добуток

$$\prod_{j=1}^{r-2}[\theta^{gj}(\theta^j+a)]^{u_j}=\theta^{g\sum_{j=1}^{r-2}ju_j}\prod_{j=1}^{r-2}(\theta^j+a)^{u_j}=\theta^{g(r-2)}\prod_{j=1}^{r-2}(\theta^j+a)^{u_j},$$

який також належить до цієї групи. Показуємо, що коли два розбиття з S_1 різні, то відповідні їм добутки не однакові.

Доведення вказаного факту виконуємо методом від протилежного. Припустимо, що розбиття $(u_1,..,u_{r-2})$ та $(v_1,..,v_{r-2})$ з множини S_1 різні, а відповідні їм добутки однакові:

$$\theta^{g(r-2)}\prod_{j=1}^{r-2}(\theta^j+a)^{u_j}=\theta^{g(r-2)}\prod_{j=1}^{r-2}(\theta^j+a)^{v_j}.$$

Скорочуючи ліву та праву частини останньої рівності на однаковий множник $\theta^{g(r-2)}$, отримуємо співвідношення

$$\prod_{j=1}^{r-2}(\theta^j+a)^{u_j}-\prod_{j=1}^{r-2}(\theta^j+a)^{v_j}=0.$$

Таким чином, елемент θ – корінь полінома у лівій частині останньої рівності. Оскільки поліном $\Phi_r(x)$ є мінімальним поліномом для елемента θ, то поліном у лівій частині останньої рівності ділиться на $\Phi_r(x)$ без остачі. Тоді можна записати

$$\prod_{j=1}^{r-2}(x^j+a)^{u_j}=\prod_{j=1}^{r-2}(x^j+a)^{v_j}(\mathrm{mod}\,\Phi_r(x)).$$

Як бачимо, з лівого боку та правого боку в останній рівності є поліноми степеня $r-2$, строго меншого від степеня $\deg\Phi_r(x)$ циклотомічного полінома $\Phi_r(x)$. Тому ці поліноми рівні як поліноми над полем F_q, тобто маємо наступне співвідношення:

$$\prod_{j=1}^{r-2}(x^j+a)^{u_j}=\prod_{j=1}^{r-2}(x^j+a)^{v_j}. \qquad (3.1)$$

Нехай k – найменше натуральне число, для якого справедлива умова $u_k \neq v_k$. Не зменшуючи загальності міркувань, можемо взяти, скажімо $u_k > v_k$. Після скорочення однакових множників з обидвох боків рівності (3.1), отримуємо

$$(x^k+a)^{u_k-v_k}\prod_{j=k+1}^{r-2}(x^j+a)^{u_j}=\prod_{j=k+1}^{r-2}(x^j+a)^{v_j}. \qquad (3.2)$$

Позначимо вільний член полінома $\prod_{j=k+1}^{r-2}(x^j+a)^{u_j}$ через b. Тоді в лівій частині рівності (3.2) є доданок

$$(u_k-v_k)a^{u_k-v_k-1}bx^k$$

з мінімальним ненульовим степенем змінної x. Оскільки виконуються умови

$$0\le u_k, v_k \le p-1,\ u_k \neq v_k,\ a,b\neq 0,$$

то цей доданок ненульовий. Але такого доданка немає в правій частині, що робить рівність (3.2) неможливою. Таким чином, добутки, які відповідають різним розбиттям, не можуть бути однаковими, і отримуємо потрібний результат.

(*b*) Кількість елементів групи $F^*_{q^{r-1}}$ дорівнює

$$q^{r-1}-1=(q^{(r-1)/2}-1)(q^{(r-1)/2}+1).$$

Зауважимо, що оскільки число q – примітивне за модулем числа r, а r є простим числом, то виконуються такі порівняння за модулем числа r:

$q^{r-1} \equiv 1 \bmod r$ та $q^{(r-1)/2} \equiv -1 \bmod r$. Виходячи із сказаного, отримуємо наступне співвідношення:

$$[\theta^e(\theta^f + a)]^{q^{(r-1)/2}+1} = \theta^{e(q^{(r-1)/2}+1)}(\theta^{fq^{(r-1)/2}} + a)(\theta^f + a) = (\theta^{-f} + a)(\theta^f + a),$$

і отже, порядок елемента $(\theta^{-f} + a)(\theta^f + a)$ ділить число $q^{(r-1)/2} - 1$. Ми показуємо далі, що елемент $(\theta^{-f} + a)(\theta^f + a)$ породжує групу із кількістю елементів принаймні $U((r-3)/2, p-1)$. Справді, оскільки автоморфізм поля, що ставить у відповідність елементу θ елемент θ^f, переводить елемент $(\theta^{-1} + a)(\theta + a)$ в елемент $(\theta^{-f} + a)(\theta^f + a)$, то мультиплікативні порядки цих елементів співпадають. Отже, достатньо у цьому разі довести, що наступний елемент

$$(\theta^{-1} + a)(\theta + a) = \theta^{-1}(a\theta + 1)(\theta + a)$$

має мультиплікативний порядок принаймні $U((r-3)/2, p-1)$.

Оскільки q – примітивне за модулем r, то для $j = 1,...,(r-3)/2$, знайдеться таке натуральне число α_j, що виконується порівняння $q^{\alpha_j} \equiv j \bmod r$. Степені

$$[\theta^{-1}(a\theta + 1)(\theta + a)]^{q^{\alpha_j}} = \theta^{-j}(a\theta^j + 1)(\theta^j + a)$$

належать до групи $< \theta^{-1}(a\theta + 1)(\theta + a) >$. Для кожного розбиття з множини S_2, яка складається із розбиттів $(u_1,...,u_{(r-3)/2})$ числа $(r-3)/2$, для яких справедлива умова

$$\sum_{j=1}^{(r-3)/2} j u_j = (r-3)/2,\ 0 \le u_1,...,u_{(r-3)/2} \le p-1,$$

будуємо такий добуток:

$$\prod_{j=1}^{(r-3)/2}[\theta^{-j}(a\theta^j+1)(\theta^j+a)]^{u_j}=\theta^{-\sum_{j=1}^{(r-3)/2}ju_j}\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{u_j}=$$
$$=\theta^{-(r-3)/2}\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{u_j},$$

який також належить до вказаної групи. Покажемо, що коли два розбиття з S_2 різні, то відповідні їм добутки неоднакові.

Доведемо це методом від протилежного. Припустимо, що розбиття $(u_1,...,u_{(r-3)/2})$ та $(v_1,...,v_{(r-3)/2})$ з множини S_2 різні, а відповідні їм добутки співпадають:

$$\theta^{-(r-3)/2}\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{u_j}=\theta^{-(r-3)/2}\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{v_j}.$$

Тоді, аналогічно до доведення пункту (а), скорочуючи ліву та праву частини останньої рівності на однаковий множник $\theta^{-(r-3)/2}$ та враховуючи, що $\Phi_r(x)$ є мінімальним поліномом для елемента θ, отримуємо таку рівність для поліномів степеня $r-3<\deg\Phi_r(x)$:

$$\prod_{j=1}^{(r-3)/2}[(ax^j+1)(x^j+a)]^{u_j}=\prod_{j=1}^{(r-3)/2}[(ax^j+1)(x^j+a)]^{v_j}. \qquad (3.3)$$

Нехай k – найменше натуральне число, для якого $u_k\neq v_k$ та, скажімо, $u_k>v_k$. Після скорочення однакових множників з обидвох боків рівності (3.3), маємо співвідношення:

$$[ax^{2k}+(a^2+1)x^k+a]^{u_k-v_k}\prod_{j=k+1}^{(r-3)/2}[(ax^j+1)(x^j+a)]^{u_j}=\prod_{j=k+1}^{(r-3)/2}[(ax^j+1)(x^j+a)]^{v_j}.$$

(3.4)

Позначимо вільний член полінома $\prod_{j=k+1}^{(r-3)/2}[(ax^j+1)(x^j+a)]^{u_j}$ через b. Застосовуючи мультиноміальну формулу до множника $[ax^{2k}+(a^2+1)x^k+a]^{u_k-v_k}$, отримуємо, що в поліномі з лівого боку рівності (3.4) є наступний доданок

$$(u_k-v_k)(a^2+1)a^{u_k-v_k-1}bx^k$$

з мінімальним ненульовим степенем змінної x. Оскільки справедливі умови $0\le u_k,v_k\le p-1$, $u_k\ne v_k$, $a^2\ne -1$ та $a,b\ne 0$, то цей доданок ненульовий. Разом з тим такого доданка немає з правого боку рівності, що приводить до суперечності.

(*c*) Так як

$$[\theta^e(\theta^f+a)]^{q^{(r-1)/2}-1}=\theta^{e(q^{(r-1)/2}-1)}(\theta^{fq^{(r-1)/2}}+a)(\theta^f+a)^{-1}=\theta^{-2e}(\theta^{-f}+a)(\theta^f+a)^{-1},$$

то порядок елемента $\theta^{-2e}(\theta^{-f}+a)(\theta^f+a)^{-1}$ є дільником числа $q^{(r-1)/2}+1$. Ми показуємо, що елемент $\theta^{-2e}(\theta^{-f}+a)(\theta^f+a)^{-1}$ породжує групу порядку принаймні $U((r-3)/2,p-1)$. Дійсно, оскільки автоморфізм поля, який відображає елемент θ в елемент θ^f, переводить елемент $\theta^{-2ef^{-1}}(\theta^{-1}+a)(\theta+a)^{-1}$ в елемент $\theta^{-2e}(\theta^{-f}+a)(\theta^f+a)^{-1}$, то мультиплікативні порядки цих елементів співпадають. Значить, достатньо довести, що наступний елемент:

$$\theta^{-2ef^{-1}}(\theta^{-1}+a)(\theta+a)^{-1}=\theta^t(a\theta+1)(\theta+a)^{-1},$$

де число t вибираємо із умови $t=-2ef^{-1}-1$, має мультиплікативний порядок принаймні величина $U((r-3)/2,p-1)$. При цьому запис f^{-1} означає обернений до елемента f за модулем числа r. Оскільки, за умовою цієї

теореми, число f взаємно просте з числом r, то вказаний обернений елемент f^{-1} існує.

Так як число q – примітивне за модулем r, то для кожного $j = 1,...,(r-3)/2$, існує таке натуральне число α_j, що $q^{\alpha_j} \equiv j \bmod r$. У цьому разі степені

$$[\theta^t(a\theta+1)(\theta+a)^{-1}]^{q^{\alpha_j}} = \theta^{jt}(a\theta^j+1)(\theta^j+a)^{-1}$$

належать до групи $<\theta^t(a\theta+1)(\theta+a)^{-1}>$. Для кожного розбиття з множини S_2, яка складається із розбиттів $(u_1,...,u_{(r-3)/2})$ числа $(r-3)/2$, для яких виконується наступна умова:

$$\sum_{j=1}^{(r-3)/2} ju_j = (r-3)/2,\ 0 \le u_1,...,u_{(r-3)/2} \le p-1,$$

утворюємо такий добуток

$$\prod_{j=1}^{(r-3)/2} [\theta^{jt}(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j} = \theta^{t\sum_{j=1}^{(r-3)/2} ju_j} \prod_{j=1}^{(r-3)/2} [(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j} =$$
$$= \theta^{t(r-3)/2} \prod_{j=1}^{(r-3)/2} [(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j},$$

який також належить до цієї групи. Покажемо, що коли два розбиття з S_2 різні, то відповідні їм добутки не рівні.

Для цього припустимо, що розбиття $(u_1,...,u_{(r-3)/2})$ та $(v_1,...,v_{(r-3)/2})$ з S_2 є різними, а відповідні їм добутки рівні:

$$\theta^{t(r-3)/2} \prod_{j=1}^{(r-3)/2} [\theta^{jt}(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j} = \theta^{t(r-3)/2} \prod_{j=1}^{(r-3)/2} [\theta^{jt}(a\theta^j+1)(\theta^j+a)^{-1}]^{v_j}.$$

Тоді, аналогічно до доведення пункту (a), скорочуючи ліву та праву частини останньої рівності на однаковий множник $\theta^{t(r-3)/2}$ та враховуючи, що $\Phi_r(x)$ є мінімальним поліномом для елемента θ, отримуємо наступну рівність для поліномів степеня $r-3<\deg\Phi_r(x)$:

$$\prod_{j=1}^{(r-3)/2}(ax^j+1)^{u_j}(x^j+a)^{v_j}=\prod_{j=1}^{(r-3)/2}[(ax^j+1)^{v_j}(x^j+a)^{u_j}. \qquad (3.5)$$

Нехай k – найменше натуральне число, для якого $u_k\neq v_k$ та, скажімо, виконується нерівність $u_k>v_k$. Після вилучення однакових множників з обидвох боків (3.5), отримуємо

$$(ax^k+1)^{u_k-v_k}\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{u_j}(x^j+a)^{v_j}==(x^k+a)^{u_k-v_k}\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{v_j}(x^j+a)^{u_j}. \qquad (3.6)$$

Позначимо вільний член полінома $\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{u_j}(x^j+a)^{v_j}$ через b. Вільний член полінома $\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{v_j}(x^j+a)^{u_j}$ позначимо через c. Зрозуміло, що елемент b та елемент c не дорівнюють нулю. Оскільки вільні члени з обидвох боків рівності (3.6) співпадають, то справедливе співідношення $b=a^{u_k-v_k}c$. Із рівності коефіцієнтів біля степеня x^k з лівого та правого боку рівності (6), отримуємо

$$(u_k-v_k)ab=(u_k-v_k)a^{u_k-v_k-1}c,$$

з чого випливає рівність $b=a^{u_k-v_k-2}c$. Порівнюючи дві рівності для вільного члена b, отримуємо $a^2=1$, що приводить до суперечності з умовою $a^2\neq 1$ у пункті (c).

(*d*) Нагадаємо, що порядок групи $F^*_{q^{r-1}}$ дорівнює

$$q^{r-1}-1=(q^{(r-1)/2}-1)(q^{(r-1)/2}+1).$$

Множники $q^{(r-1)/2}-1$ та $q^{(r-1)/2}+1$ мають найбільший спільний дільник 2, бо їх сума дорівнює $2q^{(r-1)/2}$. Розглянемо підгрупу групи $F^*_{q^{r-1}}$ породжену елементом $\theta^e(\theta^f+a)$ Ця підгрупа включає дві підгрупи: перша породжена елементом

$$w_1=[\theta^e(\theta^f+a)]^{q^{(r-1)/2}+1}=(\theta^{-f}+a)(\theta^f+a),$$

а друга – елементом

$$w_2=[\theta^e(\theta^f+a)]^{q^{(r-1)/2}-1}=\theta^{-2e}(\theta^{-f}+a)(\theta^f+a)^{-1}.$$

Згідно з пунктом (b), порядок елемента w_1 ділить $q^{(r-1)/2}-1$, а згідно з пунктом (c), порядок елемента w_2 ділить $q^{(r-1)/2}+1$.

Утворимо елемент

$$w=\begin{cases} w_1^2w_2, \text{ якщо } \rho_2(q^{(r-1)/2}-1)=2 \\ w_1w_2^2, \text{ якщо } \rho_2(q^{(r-1)/2}+1)=2 \end{cases}.$$

Якщо $\rho_2(q^{(r-1)/2}-1)=2$, то число $(q^{(r-1)/2}-1)/2$ – непарне і взаємно просте з $q^{(r-1)/2}+1$. Очевидно, що тоді порядок елемента w_1^2 є дільником $(q^{(r-1)/2}-1)/2$. Значить, у цьому випадку отримуємо рівність груп $<z>=<w_1^2>\times<w_2>$.

Аналогічно до попереднього розгляду, коли виконується співвідношення $\rho_2(q^{(r-1)/2}+1)=2$, то число $(q^{(r-1)/2}+1)/2$ непарне і взаємно просте з числом $q^{(r-1)/2}-1$. Зрозуміло, що тоді порядок елемента w_2^2 є

дільником числа $(q^{(r-1)/2}+1)/2$. Таким чином, у цьому випадку маємо рівність $<z>=<w_1>\times<w_2^2>$.

В обидвох розглянутих випадках, порядок елемента w є добутком порядку елемента w_1 та порядку елемента w_2, поділеним на число 2. Згідно з пунктом (b) та пунктом (c), порядок елемента w, а, таким чином, і порядок елемента $\theta^e(\theta+a)$ є принаймні величина $[U((r-3)/2, p-1)]^2/2$. Теорему доведено.

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

Доведення. Той факт, що мультиплікативний порядок елемента $\beta=\theta+\theta^{-1}=\theta^{-1}(\theta^2+1)$ є принаймні $U(r-2, p-1)$ випливає з теореми 3.1, пункт (a). Оскільки справедливе співвідношення

$$(\theta+\theta^{-1})^{q^{(r-1)/2}-1}=(\theta^{q^{(r-1)/2}}+\theta^{-q^{(r-1)/2}})(\theta+\theta^{-1})^{-1}=(\theta^{-1}+\theta)(\theta+\theta^{-1})^{-1}=1,$$

то мультиплікативний порядок елемента β ділить число $q^{(r-1)/2}-1$. Наслідок доведено.

Нижня межа $U(r-2, p-1)$ в наслідку 3.1 для мультиплікативного порядку гауссового періоду β покращує раніше відому межу $U((r-3)/2, p-1)$ Ахмаді, Шпарлінского і Волоха [22] і дає відповідь на відкрите питання, поставлене цими авторами.

Зауваження 3.1. Гауссовий період β належить до підполя $F_{q^{(r-1)/2}}$ поля $F_q(\theta)=F_{q^{r-1}}$.

Особливий інтерес до гауссових періодів пояснюється наступним чином. Загалом, багато аспектів вивчення різних типів базисів [102] для F_{q^n}

над F_q у значному степені мотивовані ефективною аппаратною реалізацією помножувачів для F_{q^n}. Одна з плідних ідей, яка спонукала вивчення нормальних базисів, що є оптимальними або мають малу складність, є в патенті США Мессі та Омури “Computational Method and Apparatus for Finite Field Arithmetic”, US Patent No. 4,587,627, 1986.

Нехай $\alpha \in F_{q^n}$ – нормальний елемент над F_q та нехай $N = (\alpha_0, \alpha_1, ..., \alpha_{n-1})$ – нормальний базис поля F_{q^n} над F_q, породжений елементом α, де

$$\alpha_i = \alpha^{q^i},\ 0 \le i \le n-1.$$

Позначимо через $T = (t_{ij})$ матрицю розміру $n \times n$ задану наступним чином:

$$\alpha \cdot \alpha_i = j = \sum_{j=0}^{n-1} t_{ij} \alpha_j,\ 0 \le i \le n-1,$$

де $t_{ij} \in F_q$. Матриця T є таблицею множення для базису N. Кількість C_N ненульових значень у матриці T описує складність (також називають щільністю) цього базису. Доведено [102], що складність C_N нормального базису N поля F_{q^n} над F_q задовольняє нерівність

$$2n-1 \le C_N \le n^2 - n + 1.$$

Нормальний базис є оптимальним нормальним, якщо його його складність дорівнює нижній межі $2n-1$. Відомо [102], що кожен оптимальний нормальний базис еквівалентний оптимальному нормальному базису типу I або оптимальному нормальному базису типу II, які описані далі.

1. (Оптимальний нормальний базис типу I) Припустимо, що $n+1$ – просте число та q – примітивний елемент у мультиплікативній групі Z_{n+1}^*. Нехай α є примітивним коренем з одиниці степеня $n+1$. Тоді елемент α породжує оптимальний нормальний базис поля F_{q^n} над F_q.

2. (Оптимальний нормальний базис типу II) Припустимо, що $2n+1$ – просте число та нехай γ – примітивний корінь з одиниці степеня $2n+1$. Вважатимемо, що виконується одна із двох умов:

а) мультиплікативна група Z^*_{2n+1} породжена елементом 2 (тобто 2 – примітивний елемент у Z^*_{2n+1}. У цьому разі порядок елемента 2 за модулем $2n+1$ дорівнює $2n$).

або

б) мультиплікативна група Z^*_{2n+1} породжена елементами 2 та -1 (тобто, $2n+1 \equiv 3 \pmod 4$ й 2 породжує квадратичні лишки у Z^*_{2n+1}. У цьому разі порядок елемента 2 за модулем $2n+1$ дорівнює n, а група Z^*_{2n+1} є внутрішнім прямим добутком двох підгруп: підгрупи, породженої елементом 2 та підгрупи, породженої елементом -1. Зауважимо, що порядок елемента -1 дорівнює 2).

Тоді $\alpha = \gamma + \gamma^{-1}$ породжує оптимальний нормальний базис поля F_{2^n} над F_2.

Як бачимо, гауссові періоди типу (n,1) визначають оптимальні нормальні базиси типу I, а гауссові періоди типу (n,2) визначають оптимальні нормальні базиси типу II при $q = 2$. Явні побудови оптимальних та малої складності нормальних базисів зустрічаються рідко. Власне гауссові періоди є узагальненням оптимальних нормальних базисів.

Нехай a – довільний ненульовий елемент поля F_q. Далі будемо використовувати такі позначення: $\gamma = (\theta^{-1} + a)(\theta + a)^{-1}$ та

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

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

Доведення. Виходячи з наслідку 3.1, гауссовий період β має мультиплікативний порядок, який ділить число $q^{(r-1)/2}-1$ і є принаймні $U(r-2,p-1)$. Згідно з теоремою 3.1, пункт (c), (якщо покласти в формулюванні цього пункту $e=2^{-1} \bmod r$ та $f=1$), елемент γ має порядок, який ділить число $q^{(r-1)/2}+1$ і є принаймні величина $U((r-3)/2,p-1)$. Аналогічно до доведення теореми 3.1, пункт (d), порядок елемента z є добутком порядку елемента β та порядку елемента γ, поділеним на число 2. Таким чином, отримуємо потрібний результат. Наслідок доведено.

Для покращення отриманих у цьому підрозділі нижніх меж можна було б додатково спробувати використати при формуванні добутків не тільки додатні, але й від'ємні степені співмножників. Цей прийом запропонував первісно Ж. Волох у праці [145]. Проте він ефективний лише у випадку, коли всі співмножники є поліномами першого степеня. Оскільки у нашому випадку поліноми нелінійні, то застосування згаданого прийому дасть незначне покращення.

3.2. Явні нижні межі для порядків в термінах характеристики поля та степеня розширення

Явні нижні межі для порядків елементів скінченних полів в термінах характеристики поля p та степеня розширення r становлять особливий інтерес з точки зору застосувань. Ось чому ми використовуємо в цьому підрозділі деякі відомі оцінки з робіт [24, 98], пов'язані з розбиттями натурального числа (див. підрозділ 2.1.2.), щоб вивести такі явні нижні межі для мультиплікативних порядків елемента $\theta^e(\theta^f+a)$ та елемента z. Беремо наближено $\pi\sqrt{2/3} \approx 2.5$, щоб спростити подальші отримувані формули.

Ми використовуємо вказані відомі результати, теорему 3.1 та наслідок 3.2, щоб отримати явні нижні межі для мультиплікативних порядків розглянутих елементів. Порівнюючи за величиною характеристику поля p та степінь розширення r, будемо розрізняти такі два принципово відмінних випадки.

Випадок 1. Число r велике порівняно з p.

У цьому випадку справедливий такий наслідок.

Наслідок 3.3. *Нехай e – довільне ціле число, f – довільне ціле число взаємно просте з r, a – довільний ненульовий елемент поля F_q.*

(a) *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*

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

Доведення. (a) З пункту (a) теореми 3.1, рівності (2.1) і нерівності (2.2) випливає, що при виконанні умови $r-2\geq p^2$ мультиплікативний порядок елемента $\theta^e(\theta^f+a)$ задовольняє наступну нерівність

$$\mathrm{ord}(\theta^e(\theta^f+a))\geq U(r-2,p-1)=Q(r-2,p)>$$

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

(b) Застосування пункту (d) теореми 3.1, рівності (2.1) та нерівності (2.2) дозволяє отримати, що при виконанні співвідношення $(r-3)/2\geq p^2$ мультиплікативний порядок елемента $\theta^e(\theta^f+a)$ при $a^2\neq\pm 1$ задовольняє наступну нерівність

$$\mathrm{ord}(\theta^e(\theta^f+a))\geq[U((r-3)/2,p-1)]^2/2=[Q((r-3)/2,p)]^2/2>$$

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

(c) Застосовуючи наслідок 3.2, рівність (2.1) та нерівність (2.2), отримуємо, що при виконанні співвідношення $(r-3)/2\geq p^2$ мультиплікативний порядок введеного раніше елемента z при $a^2\neq 1$ задовольняє наступну умову

$$\mathrm{ord}\ z\geq[U(r-2,p-1)\cdot U((r-3)/2,p-1)]/2=[Q(r-2,p)\cdot Q((r-3)/2,p)]/2>$$

$$>\frac{1}{2}\left(\frac{p(p-1)}{160(r-2)}\right)^{\sqrt{p}}\exp\left(2.5\sqrt{(1-\frac{1}{p})(r-2)}\right)\left(\frac{p(p-1)}{80(r-3)}\right)^{\sqrt{p}}\exp\left(2.5\sqrt{(1-\frac{1}{p})\frac{r-3}{2}}\right)>$$

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

Наслідок доведено.

Випадок 2. Число r є того самого порядку, що й число p або мале порівняно з p.

У цьому разі справедливий такий наслідок.

Наслідок 3.4. *Нехай e – довільне натуральне число, f – довільне натуральне число взаємно просте з числом r, a – довільний ненульовий елемент скінченого поля F_q.*

(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*

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

Доведення. (a) З пункту (a) теореми 3.1 і нерівності (2.3) випливає, що при $r-2<p$ мультиплікативний порядок $L_{r,1}$ елемента $\theta^e(\theta^f+a)$ задовольняє наступну умову:

$$\operatorname{ord}(\theta^e(\theta^f+a))\geq U(r-2,p-1)=U(r-2)>\frac{\exp\left(2.5\sqrt{r-2}\right)}{13(r-2)}.$$

(b) Пункт (d) теореми 3.1 та нерівність (2.3) дають, що для $(r-3)/2<p$ мультиплікативний порядок елемента $\theta^e(\theta^f+a)$ при $a^2\neq\pm1$ задовольняє умову

$$\operatorname{ord}(\theta^e(\theta^f+a))\geq[U((r-3)/2,p-1)]^2/2=[U((r-3)/2)]^2/2>\frac{2\exp\left(2.5\sqrt{2}\sqrt{r-3}\right)}{169(r-3)^2}.$$

(c) Застосовуючи наслідок 3.2 та нерівність (2.3), отримуємо при виконанні умови $(r-3)/2<p$, що мультиплікативний порядок елемента z для $a^2\neq1$ задовольняє нерівність

$$\operatorname{ord} z\geq[U(r-2,p-1)U((r-3)/2,p-1)]/2=$$

$$=[U(r-2)U((r-3)/2)]/2>\frac{\exp\left(2.5(1+\frac{\sqrt{2}}{2})\sqrt{r-3}\right)}{169(r-2)(r-3)}.$$

Наслідок доведено.

3.3. Приклади нижніх меж для мультиплікативних порядків елементів

У даному підрозділі ми наводимо числові приклади нижніх меж для мультиплікативних порядків розглянутих раніше елементів.

Позначимо нижні межі для порядків елемента $\theta^e(\theta^f + a)$, елемента $\theta^e(\theta^f + a)$ при $a^2 \neq \pm 1$ та елемента z при $a^2 \neq 1$ через b_1, b_2 та b_3 відповідно. Через те, що це великі числа, для зручності порівняння підраховуємо їх логарифми за основою два. Нагадаємо, що кількість елементів мультиплікативної групи $F^*_{q^{r-1}}$ дорівнює $q^{r-1}-1$. Логарифми чисел $q^{r-1}-1$, b_1, b_2 та b_3 в розглянутих прикладах наведені в табл. 3.1. У всіх прикладах число r є простим, число $q = p$ є простим і примітивним за модулем числа r. При цьому розглядаємо поле $F_{q^{r-1}}$. Маємо випадок 1 в прикладах 1-4, бо виконується умова $r \geq 2p^2 + 3$. Маємо випадок 2 в прикладі 5, бо справедлива нерівність $r < p + 2$. Інші наведені в цій таблиці приклади не потребують коментарів.

Для першого наведеного у вказаній таблиці прикладу, в полі F_3 немає елементів, для яких справедлива нерівність $a^2 \neq 1 \bmod 3$. Виходячи з цього, відповідні дві клітинки таблиці залишились не заповненими.

Для другого прикладу, немає елементів у полі F_5, для яких $a^2 \neq \pm 1 \bmod 5$. Тому, немає числа у відповідній клітинці таблиці. Очевидно, що справедлива умова $a^2 \neq 1 \bmod 5$ для $a = 2, 3$. Так як 5≡1 mod 4, то виконується порівняння $5^{128}+1 \equiv 2 \bmod 4$. У цьому разі число $(q^{(r-1)/2}+1)/2 = (5^{128}+1)/2$ є непарним і взаємно простим з числом $q^{(r-1)/2} - 1 = 5^{128} - 1$.

Для третього прикладу, зрозуміло, що $a^2 \neq \pm 1 \bmod 11$ та $a^2 \neq 1 \bmod 11$ для $a = 2,3,4,5,6,7,8,9$. Оскільки 11≡-1 mod 4, то справедливе порівняння $11^{209} - 1 \equiv -2 \bmod 4$. Тоді число $(q^{(r-1)/2} - 1)/2 = (11^{209} - 1)/2$ непарне і взаємно просте з $q^{(r-1)/2} + 1 = 11^{209} + 1$.

Для четвертого прикладу, так як має місце конгруенція 11≡-1 mod 4, то виконується порівняння $11^{504}+1\equiv 2 \bmod 4$. Тоді число $(q^{(r-1)/2}+1)/2=(11^{209}+1)/2$ є непарним і взаємно простим з $q^{(r-1)/2}-1=11^{504}-1$.

Для п'ятого прикладу, оскільки 107≡-1 mod 4, то справедливе порівняння $107^{48}+1\equiv 2 \bmod 4$. Тоді $(q^{(r-1)/2}+1)/2=(11^{48}+1)/2$ непарне і взаємно просте з $q^{(r-1)/2}-1=107^{48}-1$.

Таблиця 3.1

Приклади нижніх меж для порядків елементів

№	q	r	$\log_2(q^{r-1}-1)$	$\log_2 b_1$	$\log_2 b_2$	$\log_2 b_3$
1	3	401	633,99	35,65	-	-
2	5	257	594,41	26,93	-	39,85
3	11	419	1446,04	39,56	43,53	60,74
4	11	1009	3487,1	74,25	90,14	118,76
5	107	97	647,18	24,72	28,71	38,89
6	13	401	1480,18	37,93	41,43	58,06
7	7	547	1532,82	48,80	56,14	76,30
8	19	1187	5038,04	81,12	99,10	130,11
9	17	1163	4749,63	80,40	98,15	128,93
10	83	59	369,75	17,53	18,92	26,76
11	101	83	545,97	22,26	25,35	34,73
12	5	467	1082,02	43,04	48,71	66,82
13	7	1187	3329,52	82,83	102,55	133,55
14	13	1163	4299,91	81,23	99,45	130,41

3.4. Уточнення явних нижніх меж для порядків елементів на основі кількості розв'язків лінійної діофантової нерівності

В праці [76] показано, що гауссовий період β має великий мультиплікативний порядок, а саме: принаймні $2^{\sqrt{r-1}-2}$. Межі такого типу: явні й для будь-яких p та r, становлять особливий інтерес для прикладних застосувань (зокрема, криптографії). Ці межі дозволяють просто порівнювати різні розширення скінченних полів.

Оцінки, які використовують поняття розбиття натурального числа: $U((r-3)/2, p-1)$ [17], $U(r-2, p-1)$ (див. перший підрозділ), або асимптотичні оцінки: $\exp\left((\frac{2.5}{\sqrt{2}}\sqrt{1-\frac{1}{p}}+o(1))\sqrt{r-1}\right)$ [22], не дозволяють отримати межу для порядку елемента для заданого скінченого поля. Явні оцінки в термінах чисел p та r виведені в другому підрозділі з оцінок в термінах розбиттів. Проте, такі межі отримані лише для $r \geq p^2+2$ 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 порівняно з роботою [76] явні нижні межі для довільних p та r як для порядку елемента β, так і елементів подібного вигляду. Для отримання цих меж підраховуємо кількість розв'язків лінійної діофантової нерівності замість підрахунку кількості розбиттів, як у попередніх підрозділах. Основним результатом третього підрозділу є теорема 3.2.

3.4.1. Допоміжні результати

Нехай c, d – додатні цілі числа та $d \le c$. Позначимо через $L(c,d)$ множину розв'язків $(u_1,...,u_c)$ такої лінійної діофантової нерівності:

$$\sum_{j=1}^{c} ju_j \le c, \tag{3.7}$$

які задовольняють умову $0 \le u_1,...,u_c \le d$.

Для розширення $F_q(\theta)$ початкового скінченного поля F_q доводимо наступні три леми.

Лема 3.1. *Нехай a – довільний ненульовий елемент поля F_q. Якщо розв'язки $(u_1,...,u_{r-2})$ з $(v_1,...,v_{r-2})$ з множини $L(r-2,p-1)$ є різними, то добутки $\prod_{j=1}^{r-2}(\theta^j + a)^{u_j}$ та $\prod_{j=1}^{r-2}(\theta^j + a)^{v_j}$ не рівні.*

Доведення. Доводимо лему 3.1 методом від протилежного. Припустимо, що розв'язки $(u_1,...,u_{r-2})$ та $(v_1,...,v_{r-2})$ з $L(r-2,p-1)$ різні, а відповідні їм добутки рівні, тобто:

$$\prod_{j=1}^{r-2}(\theta^j + a)^{u_j} = \prod_{j=1}^{r-2}(\theta^j + a)^{v_j}.$$

Значить, маємо співвідношення

$$\prod_{j=1}^{r-2}(\theta^j + a)^{u_j} - \prod_{j=1}^{r-2}(\theta^j + a)^{v_j} = 0.$$

Таким чином, елемент θ – корінь полінома у лівій частині останньої рівності. Оскільки поліном $\Phi_r(x)$ є мінімальним поліномом для елемента θ, то поліном у лівій частині останньої рівності ділиться на $\Phi_r(x)$ без остачі. Тоді можна записати

$$\prod_{j=1}^{r-2}(x^j+a)^{u_j} = \prod_{j=1}^{r-2}(x^j+a)^{v_j} (\mathrm{mod}\, \Phi_r(x)).$$

Так як з лівого й правого боку останньої рівності є поліноми степеня $r-2 < \deg \Phi_r(x)$, то ці поліноми рівні як поліноми над початковим полем F_q, тобто справедлива рівність:

$$\prod_{j=1}^{r-2}(x^j+a)^{u_j} = \prod_{j=1}^{r-2}(x^j+a)^{v_j}. \qquad (3.8)$$

Нехай k – найменше натуральне число, для якого степені u_k та v_k не співпадають і, скажімо, не зменшуючи загальності, візьмемо $u_k > v_k$. Після вилучення однакових множників з обидвох боків рівності (3.8), отримуємо таке співвідношення:

$$(x^k+a)^{u_k-v_k} \prod_{j=k+1}^{r-2}(x^j+a)^{u_j} = \prod_{j=k+1}^{r-2}(x^j+a)^{v_j}. \qquad (3.9)$$

Позначимо абсолютний член полінома $\prod_{j=k+1}^{r-2}(x^j+a)^{u_j}$ через b. Очевидно, що вільний член b не дорівнює нулю. Тоді з лівого боку рівності (3.9) є доданок

$$(u_k - v_k)a^{u_k-v_k-1}bx^k$$

з найменшим ненульовим степенем змінної x. Оскільки $0 \le u_k, v_k \le p-1$, $u_k \ne v_k$, $a, b \ne 0$, то цей доданок ненульовий. Але такого доданка немає з

правого боку згаданої рівності, що робить рівність (3.9) неможливою. Лему доведено.

Лема 3.2. *Нехай* a *–такий ненульовий елемент скінченого поля* F_q, *що* $a^2 \neq -1$. *Якщо розв'язки* $(u_1,...,u_{(r-3)/2})$ *та* $(v_1,...,v_{(r-3)/2})$ *з* $L((r-3)/2, p-1)$ *різні, то добутки* $\prod_{j=1}^{(r-3)/2} [(a\theta^j+1)(\theta^j+a)]^{u_j}$ *та* $\prod_{j=1}^{(r-3)/2} [(a\theta^j+1)(\theta^j+a)]^{v_j}$ *не рівні.*

Доведення. Припустимо, що розв'язки $(u_1,...,u_{(r-3)/2})$ та $(v_1,...,v_{(r-3)/2})$ з множини $L((r-3)/2, p-1)$ різні, а відповідні їм добутки рівні:

$$\prod_{j=1}^{(r-3)/2} [(a\theta^j+1)(\theta^j+a)]^{u_j} = \prod_{j=1}^{(r-3)/2} [(a\theta^j+1)(\theta^j+a)]^{v_j}.$$

Тоді, аналогічно до доведення леми 3.1, враховуючи, що поліном $\Phi_r(x)$ є мінімальним поліномом для елемента θ, маємо наступне рівняння для поліномів степеня $r-3 < \deg \Phi_r(x)$:

$$\prod_{j=1}^{(r-3)/2} [(ax^j+1)(x^j+a)]^{u_j} = \prod_{j=1}^{(r-3)/2} [(ax^j+1)(x^j+a)]^{v_j}. \qquad (3.10)$$

Нехай k – найменше натуральне число, для якого степені u_k та v_k не співпадають і, скажімо, не зменшуючи загальності, візьмемо $u_k > v_k$. Після вилучення однакових множників з обидвох боків рівності (3.10), отримуємо таке співвідношення:

$$[ax^{2k}+(a^2+1)x^k+a]^{u_k-v_k} \prod_{j=k+1}^{(r-3)/2} [(ax^j+1)(x^j+a)]^{u_j} = \prod_{j=k+1}^{(r-3)/2} [(ax^j+1)(x^j+a)]^{v_j}. \qquad (3.11)$$

Позначимо вільний член полінома $\prod_{j=k+1}^{(r-3)/2}[(ax^j+1)(x^j+a)]^{u_j}$ через b. Зрозуміло, що $b\neq 0$. Застосовуючи мультиноміальну формулу до виразу $[ax^{2k}+(a^2+1)x^k+a]^{u_k-v_k}$, отримуємо, що з лівого боку рівності (3.11) є член вигляду

$$(u_k-v_k)(a^2+1)a^{u_k-v_k-1}bx^k$$

з мінімальним ненульовим степенем змінної x. Оскільки виконуються умови $0\le u_k,v_k\le p-1,\ u_k\neq v_k,\ a^2\neq -1,\ a,b\neq 0$, то цей член ненульовий. Разом з тим такого члена немає з правого боку рівності (3.11), що приводить до суперечності. Таким чином, добутки, які відповідають різним розв'язкам $(u_1,...,u_{(r-3)/2})$ та $(v_1,...,v_{(r-3)/2})$ з множини $L((r-3)/2,p-1)$, є різними. Лему доведено.

Лема 3.3. *Нехай a – такий ненульовий елемент скінченого поля F_q, що $a^2\neq 1$. Якщо розв'язки $(u_1,...,u_{r-2})$ та $(v_1,...,v_{r-2})$ з $L((r-3)/2,p-1)$ є різними, то добутки $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j}$ та $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{v_j}$ не рівні.*

Доведення. Припустимо, що розв'язки $(u_1,...,u_{(r-3)/2})$ та $(v_1,...,v_{(r-3)/2})$ з множини $L((r-3)/2,p-1)$ різні, а відповідні їм добутки рівні:

$$\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j}=\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{v_j}.$$

Тоді, аналогічно до доведення леми 3.1, враховуючи, що поліном $\Phi_r(x)$ є мінімальним поліномом для елемента θ, отримуємо наступну рівність для поліномів степеня $r-3<\deg\Phi_r(x)$:

$$\prod_{j=1}^{(r-3)/2}(ax^j+1)^{u_j}(x^j+a)^{v_j}=\prod_{j=1}^{(r-3)/2}[(ax^j+1)^{v_j}(x^j+a)^{u_j}\ . \quad (3.12)$$

Нехай k – найменше натуральне число, для якого $u_k \neq v_k$ та $u_k > v_k$. Після вилучення спільних множників з обидвох боків (3.12), отримуємо

$$(ax^k+1)^{u_k-v_k}\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{u_j}(x^j+a)^{v_j}=(x^k+a)^{u_k-v_k}\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{v_j}(x^j+a)^{u_j}\ . \quad (3.13)$$

Позначимо вільний член полінома $\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{u_j}(x^j+a)^{v_j}$ через b, а абсолютний член полінома $\prod_{j=k+1}^{(r-3)/2}(ax^j+1)^{v_j}(x^j+a)^{u_j}$ через c. Очевидно, що $b,c\neq 0$. Оскільки абсолютні члени з обидвох боків (3.13) рівні, то виконується рівність $b=a^{u_k-v_k}c$. Так як коефіцієнти біля x^k з обидвох боків (3.12) є рівними, то маємо

$$(u_k-v_k)ab=(u_k-v_k)a^{u_k-v_k-1}c\,,$$

з чого випливає рівність $b=a^{u_k-v_k-2}c$. Порівнюючи останні дві рівності, отримуємо, що $a^2=1$ – суперечність з припущенням леми $a^2\neq 1$. Лему доведено.

3.4.2. Нижні межі на основі кількості розв'язків лінійної діофантової нерівності

Усі нижні межі на порядки елементів у теоремі 3.2 далі залучають кількість розв'язків $(u_1,...,u_c)$ лінійної діофантової нерівності (3.7), де $0\le u_1,...,u_c\le p-1$. Використовуємо для доведення пунктів (a), (b), (c) вказаної

теореми техніку подібну до тієї, що в [22, 76] та підрозділі 3.1. Ідея була введена Гатеном та Шпарлінскім [76], і розвинута в [22] та в першому підрозділі цієї дисертаційної роботи. Беремо лінійний біном від деякого степеня θ та всі його спряжені елементи, які також належать до групи, породженої цим біномом, і будуємо їх різні добутки. У цьому випадку, спряжені елементи є нелінійними біномами. Для отримання нижніх меж для мультиплікативних порядків підраховуємо кількість розв'язків лінійної діофантової нерівності замість підрахунку кількості розбиттів натурального числа.

Теорема 3.2. *Нехай e – довільне натуральне число, f – довільне натуральне число взаємно просте з r, a – довільний ненульовий елемент скінченого поля F_q. Тоді*

(a) Елемент $\theta^e(\theta^f + a)$ має мультиплікативний порядок принаймні $\left|L(r-2, p-1)\right|$,

(b) Елемент $(\theta^{-f} + a)(\theta^f + a)$ при $a^2 \neq -1$ має мультиплікативний порядок принаймні $\left|L((r-3)/2, p-1)\right|$ і цей порядок ділить $q^{(r-1)/2} - 1$,

(c) Елемент $\theta^{-2e}(\theta^{-f} + a)(\theta^f + a)^{-1}$ при $a^2 \neq 1$ має мультиплікативний порядок принаймні $\left|L((r-3)/2, p-1)\right|$ і цей порядок ділить $q^{(r-1)/2} + 1$,

(d) Елемент $\theta^e(\theta^f + a)$ при $a^2 \neq \pm 1$ має мультиплікативний порядок принаймні $\left|L((r-3)/2, p-1)\right|^2 / 2$.

Доведення. (*a*) Спочатку покажемо: елемент $\theta^e(\theta^f + a)$ має той самий порядок, що й елемент $\theta^g(\theta + a)$, де $g \equiv e f^{-1} \bmod r$. Очевидно, що відображення, яке переводить елемент θ в елемент θ^p, є автоморфізмом Фробеніуса поля $F_q(\theta)$. Оскільки число q – примітивне за модулем r, то порівняння $f \equiv q^m \bmod r$ справедливе для деякого натурального числа m. Так

як q є певним степенем p, то відображення, що переводить θ в $\theta^f = \theta^{q^m}$, є степенем автоморфізму Фробеніуса і, тому, також є автоморфізмом поля $F_q(\theta)$. Оскільки останній розглянутий автоморфізм відображає елемент $\theta^g(\theta + a)$ в елемент $\theta^e(\theta^f + a)$, де $g \equiv ef^{-1} \bmod r$, то мультиплікативні порядки цих елементів співпадають.

Значить, щоб довести (а), достатньо довести, що $\theta^g(\theta + a)$ для будь-якого натурального числа g має мультиплікативний порядок принаймні $|L(r-2, p-1)|$.

Так як q примітивне за модулем r, для кожного $j = 1,..., r-2$, існує натуральне число $\alpha(j)$ таке, що $q^{\alpha(j)} \equiv j \bmod r$. Степені

$$\left(\theta^g(\theta + a)\right)^{q^{\alpha(j)}} = \theta^{gq^{\alpha(j)}}(\theta^{q^{\alpha(j)}} + \text{a}) = \theta^{gj}(\theta^j + \text{a})$$

належать до групи $<\theta^g(\theta + a)>$. Для кожного розв'язку із $L(r-2, p-1)$ будуємо наступний добуток

$$\prod_{j=1}^{r-2}[\theta^{gj}(\theta^j + a)]^{u_j} = \theta^{g\sum_{j=1}^{r-2} ju_j} \prod_{j=1}^{r-2}(\theta^j + a)^{u_j} = \theta^{g(r-2)} \prod_{j=1}^{r-2}(\theta^j + a)^{u_j},$$

який також належить до вказаної групи. Зауважимо, що всі добутки мають однаковий множник $\theta^{g(r-2)}$. Згідно з лемою 3.1, якщо два розв'язки $(u_1,..., u_{r-2})$ та $(v_1,..., v_{r-2})$ з $L(r-2, p-1)$ різні, то добутки $\prod_{j=1}^{r-2}(\theta^j + a)^{u_j}$ та $\prod_{j=1}^{r-2}(\theta^j + a)^{v_j}$ не рівні. Таким чином, добутки $\theta^{g(r-2)} \prod_{j=1}^{r-2}(\theta^j + a)^{u_j}$ та $\theta^{g(r-2)} \prod_{j=1}^{r-2}(\theta^j + a)^{v_j}$, які відповідають різним розв'язкам, не можуть бути рівними і отримуємо потрібний результат.

(*b*) Кількість елементів групи $F^*_{q^{r-1}}$ дорівнює

$$q^{r-1}-1=(q^{(r-1)/2}-1)(q^{(r-1)/2}+1).$$

Зауважимо, що оскільки q – примітивне за модулем r, а r – просте, то виконуються порівняння $q^{r-1}\equiv 1 \bmod r$ та $q^{(r-1)/2}\equiv -1 \bmod r$. Тоді

$$[\theta^e(\theta^f+a)]^{q^{(r-1)/2}+1}=\theta^{e(q^{(r-1)/2}+1)}(\theta^{fq^{(r-1)/2}}+a)(\theta^f+a)=(\theta^{-f}+a)(\theta^f+a),$$

І, значить, порядок елемента $(\theta^{-f}+a)(\theta^f+a)$ ділить $q^{(r-1)/2}-1$. Показуємо, що елемент $(\theta^{-f}+a)(\theta^f+a)$ породжує групу порядку принаймні $\left|L((r-3)/2, p-1)\right|$. Дійсно, так як автоморфізм поля, що ставить у відповідність елементу θ елемент θ^f, переводить $(\theta^{-1}+a)(\theta+a)$ в $(\theta^{-f}+a)(\theta^f+a)$, то мультиплікативні порядки цих елементів співпадають. Отже, достатньо довести, що елемент

$$(\theta^{-1}+a)(\theta+a)=\theta^{-1}(a\theta+1)(\theta+a)$$

має мультиплікативний порядок принаймні $\left|L((r-3)/2, p-1)\right|$.

Оскільки q – примітивне за модулем r, то для $j=1,...,(r-3)/2$, існує таке натуральне число $\alpha(j)$, що $q^{\alpha(j)}\equiv j \bmod r$. Степені

$$[\theta^{-1}(a\theta+1)(\theta+a)]^{q^{\alpha(j)}}=\theta^{-j}(a\theta^j+1)(\theta^j+a)$$

належать до групи $<\theta^{-1}(a\theta+1)(\theta+a)>$. Для кожного розв'язку з множини $L((r-3)/2, p-1)$, будуємо наступний добуток

$$\prod_{j=1}^{(r-3)/2}[\theta^{-j}(a\theta^j+1)(\theta^j+a)]^{u_j}=\theta^{-\sum_{j=1}^{(r-3)/2}ju_j}\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)]^{u_j}=$$

$$= \theta^{-(r-3)/2} \prod_{j=1}^{(r-3)/2} [(a\theta^j + 1)(\theta^j + a)]^{u_j},$$

який також належить до вказаної групи. Зауважимо, що всі добутки мають однаковий множник $\theta^{-(r-3)/2}$. Згідно з лемою 3.2, якщо два розв'язки з $L((r-3)/2, p-1)$ різні, то добутки $\prod_{j=1}^{(r-3)/2} [(a\theta^j + 1)(\theta^j + a)]^{u_j}$ та $\prod_{j=1}^{(r-3)/2} [(a\theta^j + 1)(\theta^j + a)]^{v_j}$ не рівні. Таким чином, отримуємо потрібний результат.

(*c*) Так як

$$[\theta^e(\theta^f + a)]^{q^{(r-1)/2}-1} = \theta^{e(q^{(r-1)/2}-1)}(\theta^{fq^{(r-1)/2}} + a)(\theta^f + a)^{-1} = \theta^{-2e}(\theta^{-f} + a)(\theta^f + a)^{-1},$$

то порядок елемента $\theta^{-2e}(\theta^{-f} + a)(\theta^f + a)^{-1}$ є дільником числа $q^{(r-1)/2} + 1$. Ми показуємо, що $\theta^{-2e}(\theta^{-f} + a)(\theta^f + a)^{-1}$ породжує групу порядку принаймні $|L((r-3)/2, p-1)|$. Дійсно, оскільки автоморфізм поля, який відображає θ в θ^f, переводить елемент $\theta^{-2ef^{-1}}(\theta^{-1} + a)(\theta + a)^{-1}$ в елемент $\theta^{-2e}(\theta^{-f} + a)(\theta^f + a)^{-1}$, то мультиплікативні порядки цих елементів співпадають. Значить, достатньо довести, що елемент

$$\theta^{-2ef^{-1}}(\theta^{-1} + a)(\theta + a)^{-1} = \theta^t(a\theta + 1)(\theta + a)^{-1},$$

де $t = -2ef^{-1} - 1$, має мультиплікативний порядок принаймні $|L((r-3)/2, p-1)|$.

Так як q примітивне за модулем r, для $j = 1, ..., (r-3)/2$, існує натуральне число $\alpha(j)$ таке, що $q^{\alpha(j)} \equiv j \bmod r$. Степені

$$[\theta^t(a\theta + 1)(\theta + a)^{-1}]^{q^{\alpha(j)}} = \theta^{jt}(a\theta^j + 1)(\theta^j + a)^{-1}$$

належать до групи $<\theta^t(a\theta+1)(\theta+a)^{-1}>$. Для кожного розв'язку з множини $L((r-3)/2, p-1)$, будуємо такий добуток

$$\prod_{j=1}^{(r-3)/2}[\theta^{jt}(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j}=\theta^{t\sum_{j=1}^{(r-3)/2}ju_j}\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j}=$$

$$=\theta^{t(r-3)/2}\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j},$$

що також належить до цієї групи. Зауважимо, що всі добутки мають той самий множник $\theta^{t(r-3)/2}$. Згідно з лемою 3.3. якщо два розв'язки з $L((r-3)/2, p-1)$ різні, то добутки $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{u_j}$ та $\prod_{j=1}^{(r-3)/2}[(a\theta^j+1)(\theta^j+a)^{-1}]^{v_j}$ не рівні. Таким чином, отримуємо потрібний результат.

(*d*) Нагадаємо, що порядок групи $F^*_{q^{r-1}}$ дорівнює $q^{r-1}-1=(q^{(r-1)/2}-1)(q^{(r-1)/2}+1)$. Множники $q^{(r-1)/2}-1$ та $q^{(r-1)/2}+1$ мають найбільший спільний дільник 2, бо їх сума дорівнює $2q^{(r-1)/2}$. Розглянемо підгрупу групи $F^*_{q^{r-1}}$ породжену елементом $\theta^e(\theta^f+a)$. Ця підгрупа включає дві підгрупи: перша породжена елементом

$$w_1=[\theta^e(\theta^f+a)]^{q^{(r-1)/2}+1}=(\theta^{-f}+a)(\theta^f+a),$$

а друга – елементом

$$w_2=[\theta^e(\theta^f+a)]^{q^{(r-1)/2}-1}=\theta^{-2e}(\theta^{-f}+a)(\theta^f+a)^{-1}.$$

Згідно з пунктом (b), порядок елемента w_1 ділить $q^{(r-1)/2}-1$, а згідно з пунктом (c), порядок елемента w_2 ділить $q^{(r-1)/2}+1$.

Утворимо елемент

$$w=\begin{cases} w_1^2 w_2, \text{ якщо } \rho_2(q^{(r-1)/2}-1)=2 \\ w_1 w_2^2, \text{ якщо } \rho_2(q^{(r-1)/2}+1)=2 \end{cases}.$$

Якщо $\rho_2(q^{(r-1)/2}-1)=2$, то число $(q^{(r-1)/2}-1)/2$ є непарним і взаємно простим з $q^{(r-1)/2}+1$. Очевидно, що порядок елемента w_1^2 є дільником $(q^{(r-1)/2}-1)/2$. Значить, у цьому випадку, $<z>=<w_1^2>\times<w_2>$. Аналогічно до попереднього розгляду, коли $\rho_2(q^{(r-1)/2}+1)=2$, то $<z>=<w_1>\times<w_2^2>$. В обидвох випадках, порядок елемента w є добутком порядків елемента w_1 та елемента w_2, поділеним на 2. Згідно з пунктом (b) та пунктом (c), порядок елемента w, а отже, порядок елемента $\theta^e(\theta+a)$ є принаймні $\left|L((r-3)/2, p-1)\right|^2/2$.

Теорему доведено.

Наслідок 3.5. *Гауссовий період β має мультиплікативний порядок принаймні $\left|L(r-2, p-1)\right|$ і цей порядок ділить $q^{(r-1)/2}-1$.*

Доведення. З теореми 3.2, пункт (a), випливає, що мультиплікативний порядок елемента $\beta=\theta+\theta^{-1}=\theta^{-1}(\theta^2+1)$ є принаймні $\left|L(r-2, p-1)\right|$. Оскільки

$$(\theta+\theta^{-1})^{q^{(r-1)/2}-1}=(\theta^{q^{(r-1)/2}}+\theta^{-q^{(r-1)/2}})(\theta+\theta^{-1})^{-1}=(\theta^{-1}+\theta)(\theta+\theta^{-1})^{-1}=1,$$

то порядок елемента β ділить $q^{(r-1)/2}-1$. Наслідок доведено.

Нехай a ненульовий елемент скінченного поля F_q. Далі використовуємо ті ж самі позначення, що і в підрозділі 3.1: $\gamma=(\theta^{-1}+a)(\theta+a)^{-1}$ та

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

Наслідок 3.6. *Елемент* z *для* $a^2\neq 1$ *має мультиплікативний порядок принаймні* $\left|L(r-2,p-1)\right|\cdot\left|L((r-3)/2,p-1)\right|/2$.

Доведення. Згідно з наслідком 3**.5**, гауссовий період β має порядок, що ділить $q^{(r-1)/2}-1$, і вказаний порядок є принаймні величина $\left|L(r-2,p-1)\right|$. Згідно з теоремою 3.2, пункт (c) (якщо покласти $e=2^{-1}\bmod r$ та $f=1$), елемент γ має порядок, що ділить число $q^{(r-1)/2}+1$, і є принаймні величина $\left|L((r-3)/2,p-1)\right|$. Аналогічно до доведення теореми 3.2, пункт (d), порядок елемента z є добутком порядків елемента β та елемента γ, поділеним на число 2. Таким чином, отримуємо потрібну нижню межу для порядку. Наслідок доведено.

3.4.3. Явні нижні межі для порядків для довільних характеристики та степеня розширення

Як вже було сказано раніше, явні нижні межі для порядків елементів скінченних полів у термінах p та r представляють особливий інтерес для прикладних застосувань. Тому в цьому підрозділі підраховуємо кількість розв'язків лінійної діофантової нерівності, щоб отримати явні нижні межі для мультиплікативних порядків розглянутих раніше елемента $\theta^e(\theta^f+a)$ та елемента z.

Лема 3.4. *Кількість* $|L(c,d)|$ *розв'язків лінійної діофантової нерівності* (3.7)*, що задовольняють умову* $0 \le u_1,...,u_c \le d$*, є принаймні*

$$\begin{cases} (d+1)^{\sqrt{c/2}-2}, \text{ якщо } d = 1,2 \\ 5^{\sqrt{c/2}-2}, \text{ якщо } d \ge 4 \end{cases}.$$

Доведення. Нехай δ – натуральне число, яке задовольняє подвійну нерівність $1 \le \delta \le d$. Це число будемо вибирати із певних міркувань пізніше. Візьмемо найбільше натуральне число α таке, що справедлива умова $\sum_{i=1}^{\alpha} i \cdot \delta \le c$. Оскільки виконуються наступні співвідношення, в яких фігурують числа α та δ:

$$\sum_{i=1}^{\alpha} i \cdot \delta = \delta\alpha(\alpha+1)/2 < \delta(\alpha+1)^2/2,$$

то вибираємо число α з нерівності $\delta(\alpha+1)^2 \le 2c$, тобто маємо рівність $\alpha = \lfloor \sqrt{2c/\delta} \rfloor - 1$. Зрозуміло, що коли брати значення $u_i \in \{0,...,\delta-1\}$ при $i = 0,...,\alpha$ та значення $u_i = 0$ при $i = \alpha+1,...,c$, то отримаємо розв'язок нерівності (3.7). Кількість розв'язків цієї нерівності дорівнює наступній величині:

$$(\delta+1)^{\alpha} \ge (\delta+1)^{\sqrt{2c/\delta}-2} = (\delta+1)^{\sqrt{2c/\delta}} / (\delta+1)^2.$$

Щоб вибрати натуральне число δ, знаходимо максимум чисельника $f(\delta) = (\delta+1)^{\sqrt{2c/\delta}}$ останнього виразу. Очевидно, що $\delta = d$ у випадку $d = 1,2$. Тому далі припускаємо $d \ge 4$.

Запишемо вказаний чисельник у вигляді

$$f(\delta) = \exp\left(\ln(\delta+1) \cdot \sqrt{2c/\delta}\right).$$

Тоді матимемо співвідношення

$$f^{'}(\delta) = (\delta+1)^{\sqrt{2c/\delta}} \cdot \sqrt{2c/\delta} \cdot \left(\frac{1}{\delta+1} - \frac{\ln(\delta+1)}{2\delta} \right).$$

Прирівнюючи дану похідну до нуля $f^{'}(\delta) = 0$, отримуємо

$$\frac{1}{\delta+1} - \frac{\ln(\delta+1)}{2\delta} = 0.$$

Значення $3{,}92155 < \delta_0 < 3.921555$ є точкою максимуму для введеної функції $f(\delta)$. Найближчим цілим числом до максимуму є точка $\delta = 4$. Функція $f(\delta)$ монотонно спадає при $\delta \geq \delta_0$, а знаменник $(\delta+1)^2$ монотонно зростає. Тому, беремо $\delta = 4$ у цьому випадку, і отримуємо потрібний результат. Лему доведено.

Основним результатом цього підрозділу є наступна теорема, яка дає явні нижні межі для порядків елементів.

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

(а) 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*

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

Доведення. (a) Застосовуючи послідовно теорему 3.2, пункт (a), та лему 3.4, отримуємо потрібний результат.

(b) Бажаний результат отримуємо, застосовуючи послідовно теорему 3.2, пункт (d), та лему 3.4.

(c) Сформульований результат отримуємо, послідовно застосовуючи наслідок 3.7 та лему 3.4.

Теорему доведено.

Виходячи з доведеної теореми 3.3, ми отримуємо наступний наслідок.

Наслідок 3.7. *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 3.7 підсилює попередню відому межу $2^{\sqrt{r-1}-2}$ з праці [75] для мультиплікативного порядку елемента β.

3.5. Асимптотичні нижні оцінки для порядків

В даному підрозділі вивчаються асимптотичні оцінки для довільних характеристики початкового поля p та степеня розширення r. Такі дослідження розпочаті в роботі [22]. Так, згідно з працею [22, наслідок 2], рівномірно по q, при $r \to \infty$: мультиплікативний порядок гауссового періоду $\beta = \theta + \theta^{-1}$ задовольняє умову

$$\text{ord}\,\beta \geq \exp\left((\frac{\pi}{\sqrt{2}} \sqrt{\frac{2(p-1)}{3p}} + o(1))\sqrt{r-1} \right).$$

Можна вивести з доведеної в першому підрозділі теореми 3.1 аналогічні асимптотичні нижні границі для мультиплікативних порядків розглянутих у даній теоремі елемента $\theta^e(\theta^f + a)$ та елемента z. При цьому використовуємо деякі відомі оцінки з робіт [24, 81, 98]. Ці оцінки, зокрема рівність (2.1), нерівність (2.2) та нерівність (3.3), описані в підрозділі 2.3.

Лема 3.5. *Нехай s – натуральне число, l – просте число. Тоді при $s \to \infty$ виконується нерівність*

$$Q(s,l) \geq \exp\left((\pi \sqrt{\frac{2(l-1)}{3l}} + o(1))\sqrt{s} \right). \qquad (3.14)$$

Доведення. Для множини $V = \{v_1, ..., v_w\}$, $1 \leq v_i \leq \frac{l-1}{2}$, згідно з [81, лема 7.2] маємо при $s \to \infty$

$$p_V(s)=\frac{(6l)^{1/2}w^{1/4}}{2^r(12sl-A)^{3/4}}\left(\prod_{i=1}^{w}\csc(\pi v_i/l)\right)\exp(Tw^{1/2})[1+O(s^{-1/2})],$$

де $A=\sum_{i=1}^{w}(l^2-6v_il+6v_i^2)$, $T=\frac{\pi(12sl-A)^{1/2}}{3l}$.

Візьмемо як множину V таку множину $V=\{1,2,...,\frac{l-1}{2}\}$, тобто $v_i=i, i=1,...,\frac{l-1}{2}$. Тоді $w=\frac{l-1}{2}$ і згідно з працею [81, с.57] отримуємо $A=\frac{l-l^2}{2}$. Також маємо

$$2^{-r}\left(\prod_{i=1}^{w}\csc(\pi v_i/l)\right)=\left(\prod_{i=1}^{(l-1)/2}2\sin(\pi v_i/l)\right)^{-1}=l^{-1/2}.$$

У випадку вибраної раніше множини V виконується рівність

$$p_V(s)=U(s-1,l-1).$$

Оскільки

$$T=\left(\frac{2\pi}{\sqrt{3l}}+o(1)\right)\sqrt{s}\ \text{ та }\ w^{1/2}=\sqrt{\frac{l-1}{2}},$$

то отримуємо співвідношення

$$Tw^{1/2}=\left(\pi\sqrt{\frac{2(l-1)}{3l}}+o(1)\right)\sqrt{s}.$$

Таким чином, нерівність (3.14) виконується. Лему доведено.

Використовуючи лему 3.5, можемо отримати оцінки знизу для мультиплікативних порядків елементів $\theta^e(\theta^f+a)$ при довільному

ненульовому a і при виконанні умови $a^2 \neq \pm 1$ та для елемента z при справедливості умови $a^2 \neq 1$.

Наслідок 3.8. *Рівномірно по q, при $r \to \infty$: мультиплікативний порядок елемента $\theta^e(\theta^f + a)$ задовольняє умову*

$$\mathrm{ord}(\theta^e(\theta^f + a)) \geq \exp\left((\pi\sqrt{\frac{2(p-1)}{3p}} + o(1))\sqrt{r-2} \right).$$

Доведення. Введемо позначення $L_{r,1} = \mathrm{ord}(\theta^e(\theta^f + a))$. Використовуючи теорему 3.1, частину (a), маємо таку нерівність $L_{r,1} \geq U(r-2, p-1)$. Враховуючи рівність (2.1), одержуємо, що $L_{r,1} \geq Q(r-2, p)$. Далі застосовуємо лему 3.5 до $Q(r-2, p)$ і отримуємо оцінку в формулюванні цього наслідку. Наслідок доведено.

Наслідок 3.9. *Рівномірно по q, при $r \to \infty$: мультиплікативний порядок елемента $\theta^e(\theta^f + a)$ при $a^2 \neq \pm 1$ задовольняє умову*

$$ord(\theta^e(\theta^f + a)) \geq \frac{1}{2}\exp\left((\pi\sqrt{2}\sqrt{\frac{2(p-1)}{3p}} + o(1))\sqrt{r-3} \right).$$

Доведення. Позначимо $L_{r,2} = \mathrm{ord}(\theta^e(\theta^f + a))$. Використовуючи теорему 3.1, частину (d), маємо таку нерівність

$$L_{r,2} \geq \frac{1}{2}[U(\frac{r-3}{2}, p-1)]^2 .$$

Враховуючи нерівність (2.2), одержуємо, що виконується наступна нерівність:

$$L_{r,2} \geq \frac{1}{2}[Q(\frac{r-3}{2}, p)]^2 .$$

Згідно з лемою 2.5, застосованою до величини $Q(\frac{r-3}{2}, p)$, отримуємо таке співвідношення:

$$L_{r,2} \geq \frac{1}{2}\exp\left((\pi\sqrt{\frac{2(p-1)}{3p}} + o(1))2\sqrt{\frac{r-3}{2}} \right).$$

З останньої нерівності випливає оцінка порядку елемента $\theta^e(\theta^f + a)$ при виконанні умови $a^2 \neq \pm 1$, яка наведена в формулюванні даного наслідку. Наслідок доведено.

Наслідок 3.10. *Рівномірно по q, при $r \to \infty$: мультиплікативний порядок елемента z при $a^2 \neq 1$ задовольняє умову*

$$\text{ord } z \geq \frac{1}{2}\exp\left(\pi\left(1 + \frac{\sqrt{2}}{2}\right)\sqrt{\frac{2(p-1)}{3p}} + o(1))\sqrt{r-3} \right).$$

Доведення. Введемо позначення $L_{r,3} = \text{ord } z$. Використовуючи наслідок 3.2, маємо таку нерівність

$$L_{r,3} \geq \frac{1}{2}U(r-2, p-1)U(\frac{r-3}{2}, p-1).$$

Беручи до уваги рівність (2.1), одержуємо

$$L_{r,3} \geq \frac{1}{2}Q(r-2, p)Q(\frac{r-3}{2}, p).$$

Застосовуючи лему 3.5 до величини $Q(r-2, p)$ та до величини $Q(\frac{r-3}{2}, p)$, отримуємо наступне співвідношення:

$$L_{r,2} \geq \frac{1}{2}\exp\left((\pi\sqrt{\frac{2(p-1)}{3p}} + o(1))\left\{\sqrt{r-2} + \sqrt{\frac{r-3}{2}}\right\}\right).$$

З останньої нерівності випливає оцінка порядку елемента z при виконанні умови $a^2 \neq 1$, яка наведена в формулюванні даного наслідку. Наслідок доведено.

Далі в табл. 3.2 наводимо чисельне порівняння оцінок мультиплікативних порядків елементів скінченого поля, отриманих в наслідку 3.8, наслідку 3.9 та наслідку 3.10.

Наводимо залежну від характеристики p основу d, яку при оцінюванні порядку елемента підносимо до степеня, залежного від r. Тобто, порядок вказаного в таблиці елемента є принаймні $d^{\sqrt{r-3}}$, де значення d наведені у вказаній таблиці.

Таблиця 3.2

Чисельне порівняння оцінок порядків елементів

№	Елемент	Значення d	
		$p = 2$	$p \to \infty$
1	гауссовий період [22]	3,6058	6,1337
2	елемент $\theta^e(\theta^f + a)$, який узагальнює гауссовий період [108]	6,1337	13,0019
3	елемент $\theta^e(\theta^f + a)$, який узагальнює гауссовий період, при $a^2 \neq \pm 1$ [108]	13,0019	37,6223
4	елемент z при $a^2 \neq 1$ [108]	22,1170	79,7499

Слід зауважити, зокрема, до другого рядка наведеної таблиці, що в найгіршому випадку (коли $p = 2$)

$$d = \exp\left((\pi \sqrt{\frac{2(p-1)}{3p}} \right) = \exp\left((\pi \sqrt{\frac{2}{6}} \right) = 6{,}1337...$$

Якщо ж характеристика поля p стає дуже великою (тобто $p \to \infty$), то маємо наступну рівність:

$$d = \exp\left((\pi \sqrt{\frac{2}{3}} \right) = 13{,}0019....$$

3.6. Висновки до розділу

У даному 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.

У першому підрозділі підсилено та узагальнено результат з праці Ахмаді, Шпарлінского та Волоха [22] на елементи більш загального вигляду, ніж гауссовий період. Це дає відповідь на відкрите питання, поставлене цими авторами.

У другому підрозділі отримано, використовуючи відомі результати з теорії розбиттів, явні нижні межі для мультиплікативних порядків елементів у термінах p – характеристика початкового поля та r – степінь розширення початкового поля. При цьому розрізняємо два випадки: перший випадок – число r велике порівняно з характеристикою p та другий випадок – число r є того самого порядку, що й характеристика p, або мале порівняно з p.

В третьому підрозділі наведено низку числових прикладів для отриманих у двох попередніх підрозділах результатів. Через те, що мультиплікативні порядки елементів, які фігурують у цих прикладах, це великі числа, для зручності порівняння підраховуємо їх логарифми за основою два.

Четвертий підрозділ присвячено модифікації нижніх меж для мультиплікативних порядків елементів. Це зроблено на основі оптимізації та підрахунку кількості розв'язків лінійної діофантової нерівності замість підрахунку кількості розбиттів. Отриманий результат, зокрема, підсилює результат Ахмаді, Шпарлінскі та Волоха.

У п'ятому підрозділі підсилено відомі асимптотичні нижні межі для порядків елементів.

Результати цього розділу опубліковано у працях [10, 108, 111, 116, 120].

Розділ 4

Елементи великого порядку в скінченних полях на основі поліномів Куммера

У даному розділі розглядаємо явні нижні межі для мультиплікативного порядку елементів у розширеннях скінченних полів на основі поліномів Куммера. Поліномом Куммера називаємо поліном вигляду $x^m - a$, тобто поліном, який має лише два доданки (так званий двочлен або біном). Розширення на основі поліномів Куммера – це розширення вигляду $F_q[x]/(x^m - a)$. У загальному такі розширення описує теорія Куммера, яка забезпечує опис певних типів розширень полів (не обов'язково скінченних), беручи до уваги приєднання коренів m-го степеня з елементів основного поля. Теорія початково була розвинута Е. Куммером у 1840-х роках у його піонерській роботі, присвяченій останній теоремі Ферма.

В першому підрозділі висвітлюємо питання, при яких умовах такі розширення існують. У цьому підрозділі немає нових результатів – він носить технічний характер. У другому підрозділі розглядаємо частковий випадок розширення, коли виконується умова: m ділить $q-1$. Третій підрозділ присвячено розгляду випадку, коли знімаємо наведену умову подільності. Отримуємо нижню межу для порядку елементів в розширеннях на основі поліномів Куммера як результат комбінування двох різних підходів.

У наступному підрозділі підсилюємо нижню межу для порядку з використанням максимуму функції кількості розв'язків діофантового рівняння. В останньому підрозділі підсилюємо нижню межу для порядку елементів з використанням оцінки знизу для кількості розбиттів натурального числа.

4.1. Нерозкладність біномів над скінченними полями

У даному підрозділі описуємо, якими повинні бути числа q та m й елемент a початкового поля F_q, щоб розширення $F_q[x]/(x^m - a)$ на основі полінома Куммера $x^m - a$ існувало. Умова існування вказаного розширення зводиться до того, що біном $x^m - a$ має бути нерозкладним над початковим скінченним полем F_q.

У скінченних полях характеристики два є лише один нерозкладний біном, а саме поліном, що дорівнює $x+1$. Тому, до кінця цього розділу вважаємо, що число q – непарне. У випадку більшої характеристики в принципі можливе існування нерозкладних біномів. Для непарної характеристики, можемо перевіряти поліном $x^m - a$ на нерозкладність, використовуючи працю [97, теорема 3.75]. Ця теорема дає необхідну і достатню умову існування нерозкладних біномів у скінченних полях непарної характеристики.

Теорема 4.1. [97, теорема 3.75] *Нехай* $m \geq 2$ *натуральне число та* $a \in F_q^*$. *Тоді біном* $x^m - a$ *нерозкладний у* $F_q[x]$ *тоді і тільки тоді, коли виконуються наступні дві умови:*

1. *Кожен простий дільник числа* m *ділить порядок* e *елемента* $a \in F_q^*$, *але не ділить число* $(q-1)/e$;
2. *Якщо* $m \equiv 0 (\mathrm{mod}\ 4)$, *то* $q \equiv 1 (\mathrm{mod}\ 4)$.

Зрозуміло, що порядок e ненульового елемента a поля F_q у наведеній теоремі 4.1 ділить число $q-1$. Зауважимо, що нерозкладні біноми над початковим полем F_q можуть існувати лише для певних степенів

розширення m. Проілюструємо наведені в теоремі 4.1 поняття наступним прикладом.

Приклад 4.1. З'ясуємо, які є нерозкладні біноми $f(x) = x^m - a$, $m \geq 2$, над полем із трьох елементів F_3. Тоді $a \neq 1$, бо інакше елемент $x = 1$ є коренем $f(x)$. Тому застосовуємо теорему 4.1 при $q = 3$ та $a = 2$. Зрозуміло, що порядок елемента $a = 2$ дорівнює $e = 2$. Тоді умова (1) теореми 4.1 дає, що $m = 2$. Оскільки число m не ділиться на 4, то умова (2) теореми 4.1 також справедлива. Таким чином, існує лише один нерозкладний біном над полем F_3, а саме $x^2 - 2$.

Як розвиток теореми 4.1, маючи число $q \geq 5$, Панаріо й Томсон в роботі [105], точно описали для яких степенів розширення m початкового скінченного поля F_q існують нерозкладні поліноми. Результат цих авторів викладено в наступній теоремі.

Теорема 4.2. *Нехай F_q – скінченне поле непарної характеристики p, $p \geq 5$. Тоді над полем F_q існує нерозкладний біном степеня m, $m \neq 0 \pmod 4$ в тому і тільки в тому випадку, коли кожен простий дільник числа m є також простим дільником числа $q-1$. Якщо $m \equiv 0 \pmod 4$, то існує нерозкладний біном над полем F_q степеня m в тому і тільки в тому випадку, коли $q \equiv 1 \pmod 4$ і кожен простий дільник числа m є також простим дільником числа $q-1$.*

Виходячи із наведеного результату, можна зробити висновок, що коли $q \geq 5$, то можна збудувати розширення для нескінченної степенів розширення m. Це вигідно відрізняє дані розширення від розглянутих у третьому розділі розширень на основі циклотомічних поліномів, які існують

для нескінченної кількості степенів розширення лише при умові виконання для кількості q елементів початкового поля гіпотези Артіна.

Далі в табл. 4.1 наведено список кількості q елементів початкового поля й степенів розширення m та умови на ці степені, для яких існують нерозкладні біноми над початковим скінченним полем F_q, причому кількість елементів початкового поля задовольняє умову $q<102$.

Таблиця 4.1

Степені m, для яких існують нерозкладні біноми над F_q, $q<102$

№	q	m
1	3	2
2	5	2^{k_1}
3	7	$2^{k_1}3^{k_2}$, $m\neq 0(\mathrm{mod}\,4)$
4	9	2^{k_1}
5	11	$2^{k_1}5^{k_2}$, $m\neq 0(\mathrm{mod}\,4)$
6	13	$2^{k_1}3^{k_2}$
7	17	2^{k_1}
8	19	$2^{k_1}3^{k_2}$, $m\neq 0(\mathrm{mod}\,4)$
9	23	$2^{k_1}11^{k_2}$, $m\neq 0(\mathrm{mod}\,4)$
10	25	$2^{k_1}3^{k_2}$
11	27	$2^{k_1}13^{k_3}$, $m\neq 0(\mathrm{mod}\,4)$
12	29	$2^{k_1}7^{k_2}$
13	31	$2^{k_1}3^{k_2}5^{k_3}$, $m\neq 0(\mathrm{mod}\,4)$
14	37	$2^{k_1}3^{k_2}$
15	41	$2^{k_1}5^{k_2}$
16	43	$2^{k_1}3^{k_2}7^{k_3}$, $m\neq 0(\mathrm{mod}\,4)$
17	47	$2^{k_1}23^{k_2}$, $m\neq 0(\mathrm{mod}\,4)$
18	49	$2^{k_1}3^{k_2}$
19	53	$2^{k_1}13^{k_2}$
20	59	$2^{k_1}29^{k_2}$, $m\neq 0(\mathrm{mod}\,4)$
21	61	$2^{k_1}3^{k_2}5^{k_3}$
22	67	$2^{k_1}3^{k_2}11^{k_3}$, $m\neq 0(\mathrm{mod}\,4)$
23	71	$2^{k_1}5^{k_2}7^{k_3}$, $m\neq 0(\mathrm{mod}\,4)$
24	73	$2^{k_1}3^{k_2}$
25	79	$2^{k_1}3^{k_2}13^{k_3}$, $m\neq 0(\mathrm{mod}\,4)$
26	81	$2^{k_1}5^{k_2}$
27	83	$2^{k_1}41^{k_2}$, $m\neq 0(\mathrm{mod}\,4)$
28	89	$2^{k_1}11^{k_2}$
29	97	$2^{k_1}13^{k_2}$
30	101	$2^{k_1}5^{k_2}$

Прокоментуємо дані з цієї таблиці. Розглянемо спочатку рядок 19 наведеної таблиці. У цьому разі $q = 53$ – просте число, а $q - 1 = 52$ ділиться на 4 та 13.

Розглянемо рядок 26 наведеної таблиці. У цьому разі $q = 81$ – степінь простого числа 3, а $q - 1 = 80$ ділиться на 4 та 5.

Слід зауважити, що розглядаючи доведення теореми 4.2 отримуємо не лише можливі степені m, але й спосіб побудови елементів a. За теоремою 4.1, умова (1), кожен простий дільник числа m повинен ділити мультиплікативний порядок вільного члена $a \in F_q$, $a \neq 0$. Отже, нам треба розглядати лише степені m, чиї прості дільники ділять $q - 1$. Нехай $q - 1 = p_1^{e_1} \ldots p_r^{e_r}$, тоді $m = p_{s_1}^{l_1} \ldots p_{s_t}^{l_t}$, де $t \leq r$ та

$$\{p_{s_1} \ldots p_{s_t}\} \subseteq \{p_1 \ldots p_r\}.$$

Будуємо елемент a наступним чином:

$$a = \alpha^{\frac{q-1}{p_{s_1}^{e_{s_1}} \ldots p_{s_t}^{e_{s_t}}}},$$

де α – примітивний елемент F_q^*. Тоді збудований елемент a має порядок $e = p_{s_1}^{e_{s_1}} \ldots p_{s_t}^{e_{s_t}}$.

Проілюструємо побудову елементів a таким прикладом.

Приклад 4.2.

а) Нехай $q = 73$. Тоді $q - 1 = 2^3 \cdot 3^2$ і степінь m слід вибирати у вигляді $m = 2^{k_1} 3^{k_2}$. Візьмемо для прикладу $m = 2^2 3^2 = 36$. У даному випадку маємо $r = t = 2$, $s_1 = 1$, $s_2 = 2$, $e_{s_1} = 3$, $e_{s_2} = 2$. Тому елемент a вибираємо наступним чином:

$$a = \alpha^{\frac{72}{2^3 3^2}} = \alpha .$$

Таким чином, біном $x^{36} - \alpha$ – нерозкладний над полем F_{73}.

б) Нехай q та m ті ж самі, що й у пункті а). Візьмемо для прикладу $m = 3^2 = 9$. У даному випадку $r = 2$, $t = 1$, $s_1 = 2$, $e_{s_1} = 2$. Тому елемент a вибираємо наступним чином:

$$a = \alpha^{\frac{72}{3^2}} = \alpha^8 .$$

Значить, біном $x^9 - \alpha^8$ – нерозкладний над полем F_{73}.

Отже, у випадку $q = 3$ єдине можливе розширення існує для $m = 2$. Якщо ж $q \geq 5$, то можемо будувати розширення для нескінченної кількості чисел m. Проте, зауважуємо, що для будь-якої непарної характеристики p існує багато (власне, нескінченна кількість) степенів m, для яких немає нерозкладних біномів над F_q. Наприклад, у випадку $q = 101$ немає нерозкладних біномів степеня 7^{k_1}.

Крайнім випадком виконання умов теореми 4.1 або теореми 4.2 є умова, що число m ділить число $q - 1$. Очевидно, що у цьому разі число m менше або рівне, ніж величина $q - 1$. Якщо вимагаємо виконання умови: степінь розширення m ділить величину $q - 1$, то степінь розширення m може приймати лише скінченну кількість значень. У цьому випадку отримуємо розширення скінченних полів, які в загальній теорії полів називають розширеннями Куммера. Ці розширення детальніше розглядаємо в другому підрозділі.

З точки зору прикладних застосувань вказана умова подільності є досить жорсткою: для задано початкового скінченного поля можна утворити

лише скінченну кількість розширень бажаного вигляду. Разом з тим реалізація операцій у таких розширеннях є досить простою.

4.2 Нижня межа для порядку елементів у розширеннях Куммера

У даному підрозділі явно збудовано в розширеннях Куммера скінченних полів елементи мультиплікативного порядку більшого від 4^m.

Розширення на основі полінома Куммера мають вигляд $F_q[x]/(x^m - a)$. Їх зокрема застосовують в криптографії, що ґрунтується на спарюванні [28]. У праці [44] показано, як будувати елементи великого порядку в таких розширеннях при умові $q \equiv 1 (\mathrm{mod}\, m)$ – це власне розширення Куммера. У цьому разі отримано нижню границю $\exp(m)$. Проте вказана нижня межа є наближеною, а не точною. У даному підрозділі отримано нижню межу, яка є точною величиною. Це суттєво для низки прикладних застосувань (зокрема, криптології).

Ми беремо лінійний двочлен від елемента, який задає розширення, та всі його спряжені, що також належать до підгрупи, породженої цим двочленом, і будуємо їх різні добутки. Усі спряжені вказаного лінійного двочлена також є лінійними двочленами. Ідея запропонована Берізбейтіа [32] як вдосконалення алгоритму AKS [23] та розвинута в [44] для розширень Куммера.

Для будь-яких полів (не тільки скінченних) розширення Куммера – це розширення поля L / K, де для деякого заданого цілого числа $n > 1$ маємо:

- початкове поле K містить n різних коренів степеня n з одиниці (тобто, коренів полінома $x^n - 1$);
- L / K має абелеву групу Галуа порядку n.

Більш загально, справедливо таке: якщо K містить n різних коренів степеня n з одиниці, звідки випливає, що характеристика K не ділить n, то

приєднання до K кореня степеня n з будь-якого елемента $a \in K$ дає розширення Куммера (степеня m, де m ділить n).

Зокрема, для скінченних полів: розширення F_{q^m} поля F_q є розширенням Куммера тоді і лише тоді, коли ціле число m ділить $q-1$. У цьому разі $F_{q^m} = F_q[x]/(x^m - a)$. Нехай $\theta = x(\mathrm{mod}\,(x^m - a))$ - клас елемента x за модулем $x^m - a$. Зрозуміло, що

$$\theta^m = a \text{ та } \theta^{q-1} = (\theta^m)^{(q-1)/m} = a^{(q-1)/m}.$$

Наступна лема є очевидним наслідком леми 1.1 при $f(x) = x^m - a$.

Лема 4.1. *Якщо поліноми $g(x)$ та $h(x)$ з $F_q[x]$ степеня меншого за m різні, то класи цих поліномів в $F_q[x]/(x^m - a)$ також є різними.*

Лема 4.2. *Для будь-якого елемента b з поля F_q спряжені елемента $\theta + b$ над цим полем мають вигляд*

$$a^{i(q-1)/m}\theta + b \ (i = 0,...,m-1).$$

Доведення. Розглянемо спряжені елемента $\theta + b$, тобто елементи, в які він переходить при дії автоморфізму Фробеніуса.

Покажемо, що

$$(\theta + b)^{q^i} = a^{i(q-1)/m}\theta + b \qquad (4.1)$$

для будь-якого натурального i. Доведемо це індукцією по i.

Очевидно, що для $i = 0$ рівність (4.1) виконується. Припустимо, що вона виконується для деякого i. Тоді для $i+1$ маємо:

$$(\theta + b)^{q^{i+1}} = [(\theta + b)^{q^i}]^q = (a^{i(q-1)/m}\theta + b)^q = a^{i(q-1)/m}\theta^q + b =$$
$$= a^{i(q-1)/m}a^{(q-1)/m}\theta + b = a^{(i+1)(q-1)/m}\theta + b.$$

Отже, рівність (4.1) справедлива для будь-якого натурального i. Лему доведено.

Зауважимо, що елементи $a^{i(q-1)/m}\theta + b$ у формулюванні леми 4.2 є різними для $i = 0,...,m-1$, оскільки $a^{i(q-1)/m}\theta$ є різними.

Зафіксуємо цілі числа $0 \le k_{\_} \le k \le m-1$. Нехай $S(m, k_{\_}, k)$ множина таких відображень f з множини $\{0,...,m-1\}$ в множину цілих чисел, які мають наступні властивості:

$$\text{(V1)} \; |\{i \mid f(i) < 0\}| = k_{\_},$$

$$\text{(V2)} \; \sum_{i, f(i)<0} |f(i)| \le k,$$

$$\text{(V3)} \; \sum_{i, f(i)\ge 0} f(i) \le m-1-k.$$

Лема 4.3. *Кількість елементів множини* $S(m, k_{\_}, k)$ *дорівнює*

$$\binom{m}{k_{\_}}\binom{k}{k_{\_}}\binom{2m-k_{\_}-k-1}{m-k-1}.$$

Доведення. Щоб задати елемент множини $S(m, k_{\_}, k)$ спочатку вибираємо місця, на яких значення відображення від'ємні – це враховує множник $\binom{m}{k_{\_}}$. Далі вибираємо значення від'ємних елементів так, щоб сума їх абсолютних значень не перевищувала k – це враховує множник $\binom{k}{k_{\_}}$. Нарешті вибираємо невід'ємні значення відображення f на $m-k_{\_}$ місцях так, щоб їх сума не перевищувала $m-1-k$ – це враховує множник $\binom{2m-k_{\_}-k-1}{m-k-1}$. Лему доведено.

Лема 4.4. *Кількість елементів множини* $S(m,k_{\_},k)$ *більше від величини* 4^m *для* $m \geq 39$.

Доведення. Покладемо $k_{\_} = k = 2$. Тоді згідно з лемою 4.3 маємо такі співвідношення:

$$| S(m,k_{\_},k) | = \binom{m}{2}\binom{2m-5}{m-3} > \frac{m(m-1)}{2}\binom{2(m-3)}{m-3}.$$

Використовуючи лему 2.2, нерівність (2.4), (беремо $s=2$ та $t=m-3$), отримуємо

$$\binom{2(m-3)}{m-3} \geq 1{,}08444 \cdot e^{-\frac{1}{8(m-3)}} \cdot \frac{4^m}{128\sqrt{m-3}}.$$

Тоді справедливі такі співвідношення:

$$| S(m,k_{\_},k) | \geq 1{,}08444 \cdot m(m-1) \cdot e^{-\frac{1}{8(m-3)}} \cdot \frac{4^m}{256\sqrt{m-3}}.$$

Оскільки виконується нерівність

$$1{,}08444 \cdot m(m-1) \cdot e^{-\frac{1}{8(m-3)}} \geq 256\sqrt{m-3}$$

для $m \geq 39$, то маємо $| S(m,k_{\_},k) | > 4^m$. Лему доведено.

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

Доведення. Згідно з лемою 4.2 спряжені елемента $\theta + b$ (включаючи сам елемент $\theta + b$) мають вигляд $a^{i(q-1)/m}\theta + b$ *для* $i = 0,...,m-1$. Зрозуміло, що всі вони належать до підгрупи $\langle \theta + b \rangle$.

Нехай $S(m,k\_,k)$ - множина відображень f з множини $\{0,...,m-1\}$ в множину цілих чисел з описаними раніше властивостями V1, V2, V3. Для кожного елемента f з множини $S(m,k\_,k)$ утворюємо добуток $\prod_{0\le i\le m-1}(a^{i(q-1)/m}\theta+b)^{f(i)}$, який також належить до $\langle\theta+b\rangle$. Ми стверджуємо, що двом різним елементам f та g з множини $S(m,k\_,k)$ відповідають різні добутки.

Доведемо це методом від протилежного. Припустимо, що елементи f та g різні, але відповідні їм добутки однакові. У цьому разі справедлива наступна рівність:

$$\prod_{0\le i\le m-1}(a^{i(q-1)/m}\theta+b)^{f(i)}=\prod_{0\le i\le m-1}(a^{i(q-1)/m}\theta+b)^{g(i)} \tag{4.2}$$

Оскільки поліном x^m-a є мінімальним поліномом для елемента θ, то можемо записати

$$\prod_{0\le i\le m-1}(a^{i(q-1)/m}\theta+b)^{f(i)}=\prod_{0\le i\le m-1}(a^{i(q-1)/m}\theta+b)^{g(i)}(\mathrm{mod}(x^m-a)).$$

Тоді отримуємо наступну рівність для поліномів:

$$\begin{aligned}&\prod_{0\le i\le m-1,\, f(i)\ge 0}(a^{i(q-1)/m}x+b)^{f(i)}\prod_{0\le i\le m-1,\, g(i)<0}(a^{i(q-1)/m}x+b)^{-g(i)}=\\&\prod_{0\le i\le m-1,\, f(i)<0}(a^{i(q-1)/m}x+b)^{-f(i)}\prod_{0\le i\le m-1,\, g(i)\ge 0}(a^{i(q-1)/m}x+b)^{g(i)}(\mathrm{mod}(x^m-a))\end{aligned} \tag{4.3}$$

Так як маємо поліном степеня

$$\sum_{0\le i\le m-1,\, f(i)\ge 0}f(i)+\sum_{0\le i\le m-1,\, g(i)<0}(-g(i))\le m-1<\deg(x^m-a)$$

у лівій частині рівності (4.3) та поліном степеня

$$\sum_{0\le i\le m-1,\, f(i)<0} (-f(i)) + \sum_{0\le i\le m-1,\, g(i)\ge 0} g(i) \le m-1 < \deg(x^m - a)$$

у правій частині рівності (4.3), то за лемою 4.1 ці поліноми рівні як поліноми над полем F_q, тобто

$$\prod_{0\le i\le m-1,\, f(i)\ge 0} (a^{i(q-1)/m}x+b)^{f(i)} \prod_{0\le i\le m-1,\, g(i)<0} (a^{i(q-1)/m}x+b)^{-g(i)} = \prod_{0\le i\le m-1,\, f(i)<0} (a^{i(q-1)/m}x+b)^{-f(i)} \prod_{0\le i\le m-1,\, g(i)\ge 0} (a^{i(q-1)/m}x+b)^{g(i)} \qquad (4.4)$$

У рівності (4.4) маємо нерозкладні та попарно різні множники $a^{i(q-1)/m}x+b,\ i=0,...,m-1$. Ця рівність суперечить однозначності розкладу поліномів над полем F_q, що робить рівність (4.2) неможливою. Отже, добутки, які відповідають різним елементам множини $S(m,k\_,k)$, не можуть бути однаковими.

Таким чином, кількість різних розглянутих добутків, які належать до підгрупи $\langle\theta+b\rangle$, дорівнює кількості елементів у множині $S(m,c\_,c)$. Згідно з лемою 4.3 кількість елементів у множині $S(m,c\_,c)$ дорівнює

$$\binom{m}{k\_}\binom{k}{k\_}\binom{2m-k\_-k-1}{m-k-1}.$$

За лемою 4.4 маємо, що $|S(m,k\_,k)| > 4^m$ для $m \ge 39$. У результаті отримуємо твердження теореми. Теорему доведено.

Аналізуючи доведення теореми 4.3, можна також сформулювати такий наслідок.

Наслідок 4.1. *Припустимо, що* $m \geq 39$. *Для будь-якого ненульового елемента* b *поля* F_q *елемент* $\theta + b$ *розширення Куммера* F_{q^m} *має мультиплікативний порядок принаймні*

$$\operatorname{ord}(\theta + b) \geq \max_{0 \leq k_- \leq k \leq m} \binom{m}{k_-} \binom{k}{k_-} \binom{2m - k_- - k - 1}{m - k - 1}.$$

Зауважимо, що переважно розглядають розширення Куммера, для яких значення числа m набагато більше від q. Тому умова $m \geq 39$ не є надто обмежуючою. Разом з тим, при $m < 39$ для вказаних розширень слід виконувати окреме дослідження.

У підрозділі 3.1 нами пояснено особливий інтерес до циклотомічних розширень (і гауссових періодів) з точки зору ефективної аппаратної реалізації помножувачів для F_{q^n} та пов'язаних із цим нормальних базисів для поля F_{q^n} над F_q, що є є оптимальними або мають малу складність. Аналогічно в підрозділі 5.1 обгрунтувано підвищений інтерес до розширень Артіна-Шраєра. Так само можна, зокрема, обгрунтувати особливий інтерес до розширень Куммера й наступним чином. Згідно з [102, наслідок 5.3.10, пункт 2] вірне наступне формулювання: нехай n – довільний дільник числа $q-1$; нехай $\beta \in F_q$ має мультиплікативний порядок t такий, що $\gcd\left(n, \frac{q-1}{t}\right) = 1$ та $\alpha = \beta^{\frac{q-1}{n}}$. Тоді поліном

$$x^n - \beta(x - \alpha + 1)^n$$

є нерозкладним над F_q, а його корені утворюють нормальний базис поля F_{q^n} над F_q складності щонайбільше $3n - 2$. Оскільки у данному випадку степінь розширення n ділить величину $q-1$, то маємо розширення Куммера скінченого поля. Тобто, у цьому разі можна ствердити, що розширення

Куммера F_{q^n} ізоморфне полю, в якому існує нормальний базис малої складності. Власне йдеться про складність $3n-2$, яка близька до оптимальної.

4.3. Нижня межа в розширеннях на основі поліномів Куммера як результат комбінування двох підходів

Розширення на основі поліномів Куммера мають вигляд $F_q[x]/(x^m-a)$. Такі розширення зокрема використовують в криптографії, що ґрунтується на спарюванні [29]. У працях [44–46] показано, як збудувати елементи великого порядку в розширенні $F_q[x]/(x^m-a)$, якщо виконується умова $q \equiv 1 (\mathrm{mod}\, m)$. У цьому разі отримано межу $\exp(m)$. Елементи великого порядку сконструйовано в [25] 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 на для мультиплікативних порядків дорівнюють $\exp((\log m)^2)$, де $m=2^t$ та $m=3^t$ відповідно.

У даному підрозділі знімаємо умову $q \equiv 1 (\mathrm{mod}\, m)$ для будь-якого степеня розширення m. Числа q, m та елемент a припускаємо такими, що розширення $F_q[x]/(x^m-a)$ існує; m_2 є порядком q за модулем m. Далі показуємо в лемі 4.6, що $m=m_1 m_2$, де m_1 є дільником $q-1$. Беремо у даному підрозділі $m_1 > 2$. Покладемо $F_q(\theta) = F_{q^m} = F_q[x]/(x^m-a)$, де $\theta = x (\mathrm{mod}(x^m-a))$ є класом елемента x. Зрозуміло, що справедлива рівність $\theta^m = a$.

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 з роботи [44]; якщо ж $q-1$ не має великого дільника m_1, то число m_2 є великим, і використовуємо для побудови метод, аналогічний до методу з праць [22, 76]. 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. Власне у цій ситуації ефективним є запропонований метод комбінування двох описаних підходів.

Слід звернути увагу на різницю між ситуацією, коли для розширень вигляду $F_q[x]/(x^m-a)$ на основі поліномів Куммера виконується умова подільності числа $q-1$ на число m та ситуацією, коли ця умова не виконується.

Візьмемо для прикладу $q=101$. Якщо вимагаємо виконання умови m ділить $q-1$, то степінь розширення m може мати лише скінченну кількість значень $m=1,2,4,5,10,20,25,50,100$. Очевидно, що у цьому разі m не перевищує $q-1$. Тобто перша ситуація не є типовою для задачі побудови елементів великого мультиплікативного порядку. У випадку, коли умову $m \mid q-1$ знімаємо, то число m може набувати нескінченну кількість значень $m=2^{k_1}5^{k_2}$ $(k_1,k_2=0,1,2,...)$. Тоді m може бути набагато більшим від $q-1$, що власне є характерним для задачі конструювання елементів великого мультиплікативного порядку.

Основним результатом третього підрозділу є наведена далі теорема 4.4. Позначення $\lfloor\ \rfloor$ у ній означає заокруглення до найближчого меншого цілого числа.

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*

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

Ми беремо в обидвох випадках лінійний біном від деякого степеня змінної θ та всі його спряжені, які також належать до групи, породженої цим біномом, і будуємо їх різні добутки. У першому випадку, коли $q \equiv 1 (\mathrm{mod}\, m_1)$, спряжені є лінійними біномами. Ідея введена Берізбейтіа [32] як вдосконалення алгоритму AKS доведення простоти великих натуральних чисел [23] і розвинута в працях [44–46]. У другому випадку, спряжені є нелінійними біномами. Ідея запропонована Гатеном та Шпарлінскі [76], і розвинута в роботі [22]. Аналогічно до праці [47] наш підхід будує елементи великого порядку для нескінченної кількості чисел m, не припускаючи будь-яких гіпотез. Число m прямо не залежить від q, зокрема може бути меншим від числа q.

Нагадаємо, що для простого числа k, $\rho_k(l)$ позначає найбільший степінь k, який ділить натуральне число l.

Лема 4.5. *Нехай* u^s $(s \ge 1)$ *степінь простого числа. Покладемо* $\rho_u(q-1) = u^t$.

1. Якщо виконується одна з двох взаємовиключних умов:

(a) u *непарне та* $t \ge 1$

або

(b) $u = 2,\ s \ge 2$ *та* $t \ge 2,$

то порядок числа q *за модулем* u^s *дорівнює*

$$\tau(u^{s-t}) = \begin{cases} 1, \text{ якщо } s \le t \\ u^{s-t}, \text{ якщо } s > t \end{cases}.$$

2. Якщо ж виконується умова

(c) $u = 2$ *та* $s = 1$,

то порядок числа q *за модулем* u^s *дорівнює 1.*

Доведення. (1) Якщо $s \le t$, то зрозуміло u^s ділить $q-1$, порядок числа q за модулем s дорівнює 1. Отже, можемо брати $s > t$. Покажемо індукцією за $i \ge 0$, що $\rho_u(q^{u^i} - 1) = u^{t+i}$, тобто існує натуральне число α_i таке, що $q = 1 + \alpha_i u^{t+i}$ та $\gcd(\alpha_i, u) = 1$.

Оскільки $\rho_u(q-1) = u^t$, то твердження справедливе для $i = 0$. Припустимо, що твердження вірне для деякого $i \ge 0$. Тоді виконуються наступні співвідношення:

$$q^{u^{i+1}} = (1 + \alpha_i u^{t+i})^u = 1 + \alpha_i u^{t+i+1} + \sum_{k=2}^{u} \binom{u}{k} \alpha_i^k u^{k(t+i)}.$$

Так як $u \ge 3$ у випадку (a) або $t \ge 2$ у випадку (b), то маємо для $i \ge 0$, $k = u$, що $k(t+i) > t+i+1$. Значить, знайдеться таке натуральне число β_i, що

$$q^{u^{i+1}} = 1 + \alpha_i u^{t+i+1} + \beta_i u^{t+i+2} = 1 + u^{t+i+1}(\alpha_i + \beta_i u)$$

та $\gcd(\alpha_i + \beta_i u, u) = 1$. Отже, твердження виконується для всіх $i \ge 0$.

Тоді $\rho_u(q^{u^{s-t-1}} - 1) = u^{s-1}$, і $q^{u^{s-t-1}} \ne 1 (\mathrm{mod}\, u^s)$. З іншого боку, $\rho_u(q^{u^{s-t}} - 1) = u^s$, та $q^{u^{s-t}} = 1 (\mathrm{mod}\, u^s)$. Тому, порядок числа q за модулем u^s дорівнює u^{s-t}.

(2) Оскільки q непарне й $u^s = 2$, то отримуємо потрібний результат.

Лему доведено.

Зауважимо, що $s=1$, $t\geq 1$ у випадку (c) леми 4.5, і порядок числа q за модулем u^s дорівнює $\tau(u^{s-t})=1$.

Лема 4.6. *Нехай m_2 порядок числа q за модулем m. Тоді $m=m_1m_2$, де m_1 є дільником $q-1$, і підгрупа $\langle q\rangle$ групи Z_m^* може бути записана у вигляді $\langle q\rangle=\{i\cdot m_1+1\,|\,i=0,...,m_2-1\}$.*

Доведення. Нехай $m=\prod_{i=1}^{n}p_i^{s_i}$ – розклад числа m у добуток степенів попарно взаємно простих чисел p_i. Застосуємо лему 3.1 до $u=p_i$, $s=s_i$, $t=t_i$, $i=1,...,n$. Слід взяти до уваги, що коли $s_i\geq 1$, то $t_i\geq 1$ згідно з теоремою 4.1, пункт (1). Також слід взяти до уваги, що коли $p_i=2$ та $s_i\geq 2$, то $t_i\geq 2$ згідно з теоремою 4.1, пункт (2). Використовуючи китайську теорему про залишки [1], отримуємо, що порядок числа q у групі Z_m^* дорівнює $m_2=\prod_{i=1}^{n}\tau(p_i^{s_i-t_i})$. Тоді $m=m_1m_2$, де m_1 можна записати у вигляді

$$m_1=\prod_{i=1}^{n}p_i^{t_i}=\prod_{i=1}^{n}\rho_{p_i}(q-1).$$

Значить, m_1 ділить $q-1$, та $q=jm_1+1$ для деякого цілого числа j. Можемо взяти $0\leq j\leq m_2-1$ для Z_m^*. Тоді, $q\in G=\{i\cdot m_1+1\,|\,i=0,...,m_2-1\}$. Покажемо, що G є підгрупою групи Z_m^*.

Дійсно, множина G замкнена відносно множення, оскільки

$$(1+i_1\cdot m_1)(1+i_2\cdot m_1)=1+[(i_1+i_2+i_1\cdot i_2\cdot m_1)(\mathrm{mod}\,m_2)]\cdot m_1.$$

Беремо $i_1+i_2+i_1\cdot i_2\cdot m_1$ за модулем m_2, бо в іншому випадку його множення на m_1 дає число не менше від m. Очевидно, що $1\in G$. Для кожного

$1+i_1\cdot m_1\in G$, обернений елемент $1+i_2\cdot m_1$ існує, якщо взяти i_2 як розв'язок порівняння

$$i_1+i_2+i_1\cdot i_2\cdot m_1\equiv 0(\mathrm{mod}\, m_2),$$

тобто $i_2\equiv -i_1(1+i_1\cdot m_1)^{-1}(\mathrm{mod}\, m_2)$. Будь-який дільник m_2 ділиться на деяке просте число p_i, що ділить m_1, але не ділить $1+i_1\cdot m_1$. Отже, $\gcd(1+i_1\cdot m_1, m_2)=1$, і обернений елемент $(1+i_1\cdot m_1)^{-1}(\mathrm{mod}\, m_2)$ існує.

Так як порядок числа q за модулем m дорівнює m_2, то маємо, що $G=\langle q\rangle$. Лему доведено.

Лема 4.7. *Нехай b – ненульовий елемент скінченого поля F_q. Тоді елемент $\theta^{m_2}+b$ має мультиплікативний порядок принаймні*

$$\begin{cases} 2^{m_1}, \textit{якщо } 2\le m_1<869 \\ 4^{m_1}, \textit{якщо } m_1\ge 869 \end{cases}.$$

Доведення. Згідно з лемою 4.6, маємо $q\equiv 1\,(\mathrm{mod}\, m_1)$. Оскільки поліном $x^m-a=(x^{m_2})^{m_1}-a$ нерозкладний над скінченним полем F_q, то поліном $y^{m_1}-a$ також нерозкладний над F_q. Покладемо $\theta_1=\theta^{m_2}$ та розглянемо підполе $F_q(\theta_1)=F_q[y]/(y^{m_1}-a)$ поля $F_q(\theta)$. Візьмемо θ_1+b та його спряжені $a^i\theta_1+b$, $i=1,\ldots,m_1-1$. Збудуємо їх добутки $\prod_{i=0}^{m_1-1}(a^i\theta_1+b)^{\beta_i}$, де $\beta_i\in\{0,1\}$ та $\sum_{i=0}^{m_1-1}\beta_i\le m_1-1$. Очевидно, що всі ці добутки попарно різні, а їх кількість дорівнює $2^{m_1}-1$. Якщо $m_1>2$, ми також беремо добуток $(\theta_1+b)^2$, і отримуємо 2^{m_1} різних добутків.

Розглянемо випадок $m_1 = 2$. Зрозуміло, що 1, $\theta_1 + b$, $a\theta_1 + b$ – це три різних елементи. Доведемо, що $(\theta_1 + b)^2$ або $(a\theta_1 + b)^2$ є четвертим відмінним від них елементом. Ясно, що $(\theta_1 + b)^2$ відмінний від 1, $\theta_1 + b$. Якщо $(\theta_1 + b)^2 = a\theta_1 + b$, то $\theta_1^2 + (2b - a)\theta_1 + b(b-1) = 0$. Оскільки $y^2 - a$ є мінімальним поліномом для θ_1, то маємо $a = 2b$. Зауважимо, що поліном $(a\theta_1 + b)^2$ відмінний від 1, $a\theta_1 + b$. Якщо $(a\theta_1 + b)^2 = \theta_1 + b$, то $a^2\theta_1^2 + (2ab - 1)\theta_1 + b(b-1) = 0$, й $a^{-1} = 2b$. Таким чином, отримуємо $a = \pm 1$.

Оскільки $a \neq 1$, беремо $a = -1$ і будуємо добуток $(\theta_1 + b)(-\theta_1 + b) = -(\theta_1^2 + b)$. Так як $\theta_1^2 = -1$, то добуток дорівнює $b + 1$ і є четвертим відмінним елементом.

Припустимо тепер, що $m_1 \geq 869$. Згідно з наслідком 4.1, елемент $\theta_1 + b$ має мультиплікативний порядок $\mathrm{ord}(\theta_1 + b)$ принаймні величина

$$\mathrm{ord}(\theta_1 + b) \geq \max_{0 \leq d_- \leq d \leq m_1} \binom{m_1}{d_-} \binom{d-1}{d_- - 1} \binom{2m_1 - d - d_- - 2}{m_1 - d_- - 1}.$$

Покладемо $d_- = d = 1$. Тоді виконується наступна нерівність:

$$\mathrm{ord}(\theta_1 + b) \geq m_1 \binom{2(m_1 - 2)}{m_1 - 2}.$$

Використовуючи наслідок 2.1, нерівність (2.5) (беремо $s = 2$ та $t = m_1 - 2$), отримуємо таке співвідношення:

$$\binom{2(m_1 - 2)}{m_1 - 2} \geq 1{,}08444 \cdot e^{-\frac{1}{8(m_1 - 2)}} \cdot \frac{4^{m_1 - 2}}{2\sqrt{m_1 - 2}}.$$

У результаті маємо

$$\operatorname{ord}(\theta_1 + b) \geq 1{,}08444 \cdot e^{-\frac{1}{8(m_1-2)}} \cdot \frac{m_1}{32\sqrt{m_1-2}} 4^{m_1}.$$

Оскільки $1{,}08444 \cdot e^{-\frac{1}{8(m_1-2)}} \cdot m_1 \geq 32\sqrt{m_1-2}$ для $m_1 \geq 869$, то маємо $\operatorname{ord}(\theta_1 + b) \geq 4^{m_1}$. Лему доведено.

Далі явно будуємо в полі $F_q[x]/(x^m - a)$ елементи порядку принаймні величина $2^{\lfloor \sqrt[3]{2m} \rfloor}$.

Теорема 4.5. *Нехай b – довільний ненульовий елемент поля F_q. Тоді елемент $\theta + b$ має в полі $F_q(\theta) = F_q[x]/(x^m - a)$ мультиплікативний порядок принаймні кількість таких розв'язків $(e_1,...,e_{m_2-1})$ лінійної діофантової нерівності*

$$\sum_{i=0}^{m_2-1} (i \cdot m_1 + 1) e_i < m, \tag{4.5}$$

для яких $0 \leq e_1,...,e_{m_2-1} \leq p-1$.

Доведення. Згідно з лемою 4.6 для кожного $i = 0,1,...,m_2 - 1$, існує таке натуральне число α_i, що $q^{\alpha_i} \equiv (i \cdot m_1 + 1) \bmod m$, тобто $q^{\alpha_i} \equiv (i \cdot m_1 + 1) + j_i \cdot m$ для деякого цілого числа j_i. Степені

$$(\theta + b)^{q^\alpha} = \theta^{q^\alpha} + b = \theta^{i \cdot m_1 + 1} (\theta^m)^{j_i} + b = a^{j_i} \theta^{i \cdot m_1 + 1} + b$$

належать до групи $\langle \theta + b \rangle$. Нехай S множина таких розв'язків нерівності (4.5), для яких $0 \leq e_1,...,e_{m_2-1} \leq p-1$. Для кожного розв'язку з множини S будуємо наступний добуток

$$\prod_{i=0}^{m_2-1}(a^{j_i}\theta^{i\cdot m_1+1}+b)^{e_i},$$

що також належить до вказаної групи. Ми стверджуємо, що коли два розв'язки різні, то відповідні добутки не рівні.

Припустимо, що розв'язки $(e_1,...,e_{m_2-1})$ та $(e_1^{'},...,e_{m_2-1}^{'})$ з множини S, де $0\le e_1,...,e_{m_2-1}\le p-1$ та $0\le e_1^{'},...,e_{m_2-1}^{'}\le p-1$, є різними, а відповідні їм добутки є рівними:

$$\prod_{i=0}^{m_2-1}(a^{j_i}\theta^{i\cdot m_1+1}+b)^{e_i}=\prod_{i=0}^{m_2-1}(a^{j_i}\theta^{i\cdot m_1+1}+b)^{e_i^{'}}.$$

Оскільки поліном x^m-a є мінімальним поліномом для елемента θ, то записуємо

$$\prod_{i=0}^{m_2-1}(a^{j_i}x^{i\cdot m_1+1}+b)^{e_i}=\prod_{i=0}^{m_2-1}(a^{j_i}x^{i\cdot m_1+1}+b)^{e_i^{'}}(\mathrm{mod}(x^m-a). \qquad (4.6)$$

Так як маємо поліном степеня $\sum_{i=0}^{m_2-1}(im_1+1)e_i<m$ з лівого боку та поліном степеня $\sum_{i=0}^{m_2-1}(im_1+1)e_i^{'}<m$ з правого боку рівності (4.6), то ці поліноми співпадають як поліноми над полем F_q, тобто

$$\prod_{i=0}^{m_2-1}(a^{j_i}x^{i\cdot m_1+1}+b)^{e_i}=\prod_{i=0}^{m_2-1}(a^{j_i}x^{i\cdot m_1+1}+b)^{e_i^{'}}.$$

Нехай k – найменше натуральне число, для якого елементи e_k та $e_k^{'}$ не співпадають і, скажімо виконується нерівність $e_k>e_k^{'}$. Після вилучення однакових множників з лівого та правого боку рівності (4.6), отримуємо наступну рівність для поліномів.

$$(a^{j_k}x^{k\cdot m_1+1}+b)^{e_k-e_k^{'}}\prod_{i\geq k+1}^{m_2-1}(a^{j_i}x^{i\cdot m_1+1}+b)^{e_i}=\prod_{i\geq k+1}^{m_2-1}(a^{j_i}x^{i\cdot m_1+1}+b)^{e_i^{'}}. \qquad (4.7)$$

Позначимо вільний член полінома $\prod_{i\geq k+1}^{m_2-1}(a^{j_i}x^{i\cdot m_1+1}+b)^{e_i}$ через c. Тоді в поліномі з лівого боку рівності (4.7) є доданок

$$(e_k-e_k^{'})a^{j_k}b^{e_k-e_k^{'}-1}cx^{k\cdot m_1+1}$$

з ненульовим мінімальним степенем змінної x. Оскільки справедливі умови $0\leq e_k,e_k^{'}\leq p-1$, $e_k\neq e_k^{'}$, $a,b,c\neq 0$, то цей доданок ненульовий. Але такого доданка немає з правого боку, що робить рівність (4.7) неможливою. Значить, добутки, які відповідають різним розв'язкам, не можуть бути рівними, і отримуємо потрібний результат. Теорему доведено.

Лема 4.8. *Кількість розв'язків лінійної діофантової нерівності* (4.5)*, для яких* $0\leq e_1,...,e_{m_2-1}\leq p-1$*, є принаймні* $2^{\lfloor\sqrt{2m_2}\rfloor}$.

Доведення. Виберемо найбільше натуральне число α, таке, що $\sum_{i=0}^{\alpha}(i\cdot m_1+1)<m$. Нагадаємо, що $m_1>2$. Оскільки

$$\sum_{i=0}^{\alpha}(i\cdot m_1+1)=(\alpha m_1+2)(\alpha+1)/2<m_1(\alpha+1)^2/2,$$

то вибираємо значення числа α з нерівності $m_1(\alpha+1)^2\leq 2m$, тобто $\alpha=\lfloor\sqrt{2m_2}\rfloor-1$. Зрозуміло, що коли беремо значення $u_i\in\{0,1\}$ для $i=0,...,\alpha$ та значення $u_i=0$ для випадку $i=\alpha+1,...,m_2-1$, то отримуємо розв'язок нерівності (4.5). Кількість таких розв'язків дорівнює $2^{\alpha+1}=2^{\lfloor\sqrt{2m_2}\rfloor}$. Лему доведено.

Застосовуючи теорему 4.5 та лему 4.8, отримуємо в результаті наступну лему.

Лема 4.9. *Нехай* b *довільний ненульовий елемент поля* F_q. *Тоді* елемент $\theta+b$ *має в полі* $F_q(\theta)= F_q[x]/(x^m-a)$ *мультиплікативний порядок принаймні* $2^{\lfloor\sqrt{2m_2}\rfloor}$.

Тепер ми даємо доведення основного результату цього підрозділу, а власне доведення теореми 4.4.

Доведення теореми 4.4. Розіб'ємо доведення даної теореми на два випадки.

Розглянемо спочатку випадок $2\le m_1<869$. Якщо $2^{m_1}\le 2^{\lfloor\sqrt{2m_2}\rfloor}$, то будуємо згідно з лемою 4.9 елемент $\gamma=\theta+b$ з нижньою межею $2^{\lfloor\sqrt{2m_2}\rfloor}$ для його порядку. Якщо ж $2^{m_1}>2^{\lfloor\sqrt{2m_2}\rfloor}$, то будуємо згідно з лемою 4.7 елемент $\gamma=\theta^{m_2}+b$ з нижньою межею 2^{m_1} для його порядку. Таким чином, можна явно збудувати в полі $F_q[x]/(x^m-a)$ елемент мультиплікативного порядку принаймні максимум наступних двох нижніх меж: 2^{m_1} and $2^{\lfloor\sqrt{2m_2}\rfloor}$. У найгіршому випадку покладаємо ці межі рівними: $2^{m_1}=2^{\lfloor\sqrt{2m_2}\rfloor}$. Тоді отримуємо $m_2=\left\lfloor\sqrt[3]{m^2/2}\right\rfloor$, і порядок є принаймні $2^{\lfloor\sqrt[3]{2m}\rfloor}$.

Розглянемо тепер доведення для випадку $m_1\ge 869$. Якщо $2^{m_1}\le 2^{\lfloor\sqrt{2m_2}\rfloor}$, то будуємо згідно з лемою 4.9 елемент $\gamma=\theta+b$ з нижньою межею $2^{\lfloor\sqrt{2m_2}\rfloor}$ для його порядку. Якщо ж $2^{m_1}>2^{\lfloor\sqrt{2m_2}\rfloor}$, то будуємо згідно з лемою 4.7 елемент $\gamma=\theta^{m_2}+b$ з нижньою межею 4^{m_1} для його порядку. Таким чином, можна явно збудувати в полі $F_q[x]/(x^m-a)$ елемент мультиплікативного порядку принаймні максимум наступних нижніх меж: 4^{m_1} and $2^{\lfloor\sqrt{2m_2}\rfloor}$. У найгіршому

випадку ці межі є рівними: $4^{m_1} = 2^{\lfloor\sqrt{2m_2}\rfloor}$. Тоді $m_1 = \lfloor\sqrt[3]{m^2/2}\rfloor$, і порядок є принаймні $2^{\lfloor\sqrt[3]{4m}\rfloor}$.

Теорему доведено.

Далі розглядаємо кілька прикладів часткових розширень скінченних полів на основі поліномів Куммера.

Приклад 4.3. Нехай q – такий степінь простого числа, що $q \equiv 1 \pmod 4$. Тоді існує наступне розширення $F_{q^{2^t}} = F_q[x]/(x^{2^t} - a)$. Згідно з теоремою 4.4 елемент γ має мультиплікативний порядок принаймні $2^{\lfloor 2^{(t+1)/3}\rfloor}$. Ця межа є сильнішою для достатньо великих t від попередньо відомою межі, даної Буркхартом та ін. в праці [36]. Якщо $\rho_2(q-1)$ невелике, наприклад $q = 5$, то межа з [44] також є малою порівняно з отриманою.

Приклад 4.4. Нехай q – такий степінь простого числа, що $q \equiv 1 \pmod 3$. Тоді існує наступне розширення $F_{q^{3^t}} = F_q[x]/(x^{3^t} - a)$. Згідно з теоремою 4.4 елемент γ має мультиплікативний порядок принаймні $2^{\lfloor 2^{1/3}\cdot 3^{t/3}\rfloor}$. Ця межа підсилює попередню межу Буркхарта та ін., наведену в праці [36]. Якщо $\rho_3(q-1)$ мале, наприклад $q = 7$, то межа з роботи [44] також є малою порівняно з отриманою.

Приклад 4.5. Нехай p – просте число та $p \equiv 3 \pmod 4$. Виберемо такі елементи a, b із простого поля F_p, що $a^2 + b^2$ не є ані квадратом, ані кубом в F_p. Тоді існує наступне розширення:

$$F_{p^2}[x]/(x^m - (a \pm b\sqrt{-1}),\ m = \frac{k}{2},\ k = 2^i 3^j.$$

Такі розширення, як вже було сказано раніше, використовують у криптографії, що ґрунтується на спарюванні [29]. Застосовуючи теорему 4.4, отримуємо, що елемент γ має мультиплікативний порядок принаймні величина $2^{\lfloor 2^{i/3}3^{j/3}\rfloor}$.

4.4. Підсилення нижньої межі з використанням максимуму функції кількості розв'язків діофантового рівняння

У третьому підрозділі збудовано елементи великого порядку для розширень на основі поліномів Куммера без умови $q \equiv 1 (\mathrm{mod}\, m)$. Нижня границя на мультиплікативний порядок дорівнює $2^{\lfloor \sqrt[3]{2m}\rfloor}$. У даному підрозділі ми покращуємо отриману в попередньому підрозділі границю. Розглядаємо будь-яке розширення виду $F_q[x]/(x^m - a)$, і будуємо в ньому елементи мультиплікативного порядку принаймні величина

$$2^{\left\lfloor \sqrt[3]{\frac{(\log_2 5)^2}{2} m}\right\rfloor}.$$

Основна ідея така ж, як і в третьому підрозділі: якщо число $q-1$ має великий дільник m_1, то використовуємо для побудови метод, аналогічний методу для розширень Куммера; якщо ж число $q-1$ не має великого дільника m_1, то тоді дільник m_2 є великим, і ми використовуємо для побудови метод, аналогічний до методу для розширень на основі циклотомічних поліномів. Додаткова думка полягає в тому, щоб знайти максимум функції кількості розв'язків відповідного діофантового рівняння. Для досягнення цього власне користуємось лемою 4.10, аналогічною до доведеної в попередньому розділі леми 3.4.

Основний результат четвертого підрозділу – це наведена далі така теорема. Нагадаємо, що позначення $\lfloor w \rfloor$ у ній означає заокруглення натурального числа w у дужках до найближчого меншого натурального числа.

Теорема 4.6. *Нехай b - ненульовий елемент із F_q. Тоді елемент*

$$\gamma = \begin{cases} \theta + b, \text{якщо } m_1 \le \left\lfloor \log_2 5 \sqrt{\frac{m_2}{2}} \right\rfloor \\ \theta^{m_2} + b, \text{якщо } m_1 > \left\lfloor \log_2 5 \sqrt{\frac{m_2}{2}} \right\rfloor \end{cases}$$

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

$$\begin{cases} 2^{\left\lfloor \sqrt[3]{\frac{(\log_2 5)^2}{2} m} \right\rfloor}, \text{якщо } 2 \le m_1 < 869 \\ 2^{\left\lfloor \sqrt[3]{(\log_2 5)^2 \cdot m} \right\rfloor}, \text{якщо } m_1 \ge 869 \end{cases}.$$

Ми явно будуємо далі в полі $F_q[x]/(x^m - a)$ елементи порядку принаймні така величина: $2^{\left\lfloor \sqrt[3]{\frac{(\log_2 5)^2}{2} m} \right\rfloor}$.

Лема 4.10. *Число розв'язків лінійної діофантової нерівності* (4.5)*, для яких $0 \le e_1, ..., e_{m_2 - 1} \le p - 1$, є принаймні $5^{\left\lfloor \sqrt{\frac{m_2}{2}} \right\rfloor}$.*

Доведення. Нехай τ – натуральне число $(2 \le \tau \le p)$, яке виберемо пізніше. Візьмемо таке найбільше ціле число α, що

$$\sum_{i=0}^{\alpha} (i \cdot m_1 + 1)(\tau - 1) < m .$$

Нагадаємо, що $m_1 \geq 2$. Оскільки

$$\sum_{i=0}^{\alpha}(i \cdot m_1 + 1)(\tau - 1) = (\tau - 1)(\alpha m_1 + 2)(\alpha + 1)/2 < (\tau - 1)m_1(\alpha + 1)^2/2,$$

то ми вибираємо α з нерівності $(\tau - 1)m_1(\alpha + 1)^2 \leq 2m$, тобто $\alpha = \left\lfloor \sqrt{\frac{2m_2}{\tau - 1}} \right\rfloor - 1$.

Зрозуміло, що коли взяти $u_i \in \{0,..., p-1\}$ для $i = 0,..., \alpha$ та $u_i = 0$ для $i = \alpha + 1,..., m_2 - 1$, то отримуємо розв'язок нерівності (4.5). Число таких розв'язків дорівнює $\tau^{\alpha+1} = \tau^{\left\lfloor \sqrt{\frac{2m_2}{\tau-1}} \right\rfloor}$.

Для вибору τ дослідимо функцію $f(\tau) = \tau^{\sqrt{\frac{2m_2}{\tau-1}}}$ $(2 \leq \tau \leq p)$ на максимум. Запишемо з цією метою

$$f(\tau) = \exp\left(\ln \tau \cdot \sqrt{\frac{2m_2}{\tau - 1}} \right).$$

Тоді маємо такі співвідношення:

$$f'(\tau) = \tau^{\sqrt{\frac{2m_2}{\tau-1}}} \cdot \left(\frac{1}{\tau}\left(\frac{2m_2}{\tau - 1}\right)^{1/2} - \ln \tau \cdot \frac{1}{2} \cdot \left(\frac{2m_2}{\tau - 1}\right)^{-1/2} \cdot 2m_2 \frac{-1}{(\tau - 1)^2} \right) =$$

$$= \tau^{\sqrt{\frac{2m_2}{\tau-1}}} \cdot \frac{2m_2}{\tau - 1} \cdot \left(\frac{1}{\tau} - \frac{\ln \tau}{2(\tau - 1)} \right).$$

Якщо покладаємо $f'(\tau) = 0$, то $\left(\frac{1}{\tau} - \frac{\ln \tau}{2(\tau - 1)} \right) = 0$. Точка $4{,}92155 < \tau < 4.921555$ є точкою максимуму функції. Найближчим цілим числом до максимуму є $\tau = 5$.

Таким чином, число розв'язків нерівності (4.5) принаймні $5^{\left\lfloor\sqrt{\frac{m_2}{2}}\right\rfloor}$. Лему доведено.

Застосовуючи теорему 4.5 та лему 4.10, отримуємо таку лему.

Лема 4.11. *Нехай* b *довільний ненульовий елемент з* F_q. *Тоді* $\theta+b$ має в $F_q(\theta)= F_q[x]/(x^m-a)$ мультиплікативний порядок принаймні $5^{\left\lfloor\sqrt{\frac{m_2}{2}}\right\rfloor}$.

Тепер ми даємо доведення основного для четвертого підрозділу результату, а сааме доведення теоерми 4.6.

Доведення теореми 4.6. Розіб'ємо доведення теореми на два можливих випадки.

Розглянемо спочатку доведення для випадку $2 \le m_1 < 869$. Якщо $2^{m_1} \le 5^{\left\lfloor\sqrt{\frac{m_2}{2}}\right\rfloor}$, то будуємо згідно з лемою 4.11 елемент $\gamma = \theta + b$ з нижньою границею $5^{\left\lfloor\sqrt{\frac{m_2}{2}}\right\rfloor}$ на його порядок. Якщо $2^{m_1} > 5^{\left\lfloor\sqrt{\frac{m_2}{2}}\right\rfloor}$, то будуємо згідно з лемою 4.7 елемент $\gamma = \theta^{m_2} + b$ з нижньою границею 2^{m_1} на його порядок. Отже, можна явно збудувати в полі $F_q[x]/(x^m-a)$ елемент з мультиплікативним порядком принаймні максимум таких нижніх границь: 2^{m_1} та $5^{\left\lfloor\sqrt{\frac{m_2}{2}}\right\rfloor}$. У найгіршому випадку ці нижні границі співпадають: $2^{m_1} = 5^{\left\lfloor\sqrt{\frac{m_2}{2}}\right\rfloor}$. Тоді $m_1 = \left\lfloor \sqrt[3]{\frac{\log_2^2 5}{2} m} \right\rfloor$ і порядок є принаймні $2^{\left\lfloor\sqrt[3]{\frac{\log_2^2 5}{2} m}\right\rfloor}$.

Розглянемо тепер доведення для випадку $m_1 \ge 869$. Якщо $2^{m_1} \le 5^{\left\lfloor\sqrt{\frac{m_2}{2}}\right\rfloor}$, то будуємо згідно з лемою 4.11 елемент $\gamma = \theta + b$ з нижньою границею $5^{\left\lfloor\sqrt{\frac{m_2}{2}}\right\rfloor}$

на його порядок. Якщо $2^{m_1} > 5^{\left\lfloor \sqrt{\frac{m_2}{2}} \right\rfloor}$, то будуємо згідно з лемою 4.7 елемент $\gamma = \theta^{m_2} + b$ з нижньою границею 4^{m_1} на його порядок. Отже, можна явно збудувати в полі $F_q[x]/(x^m - a)$ елемент з мультиплікативним порядком принаймні максимум таких нижніх границь: 4^{m_1} та $5^{\left\lfloor \sqrt{\frac{m_2}{2}} \right\rfloor}$. У найгіршому випадку ці нижні границі співпадають: $4^{m_1} = 5^{\left\lfloor \sqrt{\frac{m_2}{2}} \right\rfloor}$. Тоді $m_1 = \left\lfloor \frac{\sqrt[3]{(\log_2 5)^2 m}}{2} \right\rfloor$ і порядок є принаймні $2^{\left\lfloor \sqrt[3]{(\log_2 5)^2 m} \right\rfloor}$.

Теорему доведено.

Далі розглядаємо приклади часткових розширень скінченних полів на основі поліномів Куммера.

Приклад 4.6. Нехай q – такий степінь простого числа, що $q \equiv 1 \pmod 4$. Тоді згідно з теоремою 4.2 існує таке розширення $F_{q^{2^t}} = F_q[x]/(x^{2^t} - a)$. Згідно з теоремою 4.6 елемент γ має мультиплікативний порядок принаймні $2^{\left\lfloor \sqrt[3]{(\log_2 5)^2 \cdot 2^{t-1}} \right\rfloor}$.

Приклад 4.7. Нехай q – такий степінь простого числа, що $q \equiv 1 \pmod 3$. Тоді згідно з теоремою 4.2 існує таке розширення $F_{q^{3^t}} = F_q[x]/(x^{3^t} - a)$. Згідно з теоремою 4.6 елемент γ має порядок принаймні $2^{\left\lfloor \sqrt[3]{\frac{(\log_2 5)^2}{2} \cdot 3^t} \right\rfloor}$.

Приклад 4.8. Нехай p – просте число та $p \equiv 3 \pmod 4$. Візьмемо такі елементи a, b з простого поля F_p, що $a^2 + b^2$ не є ні квадратом ні кубом у F_p. Тоді існує таке розширення

$$F_{p^2}[x]/(x^m-(a\pm b\sqrt{-1}),\ m=\frac{k}{2},\ k=2^i3^j.$$

Згідно з теоремою 4.6 елемент γ має мультиплікативний порядок принаймні $2^{\left\lfloor\sqrt[3]{(\log_2 5)^2\cdot 2^{i-2}3^j}\right\rfloor}$.

4.5. Підсилення нижньої межі з використанням оцінки знизу для кількості розбиттів

У третьому підрозділі явно збудовано елементи великого порядку для розширень на основі поліномів Куммера без виконання умови подільності величини $q-1$ на степінь розширеня m. Нижня межа для мультиплікативного порядку дорівнює $2^{\lfloor\sqrt[3]{2m}\rfloor}$. У даному підрозділі ми модифікуємо отриману в третьому підрозділі нижнюю межу. Розглядаємо будь-яке розширення вигляду $F_q[x]/(x^m-a)$, і будуємо в ньому елементи мультиплікативного порядку принаймні максимум двох чисел, які прямо залежать від степеня розширення m.

Більш точно, явно будуємо далі елементи в $F_q[x]/(x^m-a)$ мультиплікативного порядку принаймні максимум 2^{m_1} та величини $U\left(\lfloor m/(m_1+1)\rfloor, p-1\right)$. Застосовується така ж ідея, як і в третьому підрозділі: якщо число $q-1$ має великий дільник m_1, то використовуємо для побудови метод з праці [44]; якщо ж число $q-1$ не має великого дільника m_1, то тоді дільник m_2 є великим, і ми використовуємо для побудови метод, аналогічний до методу з робіт [22, 75]. Основний результат п’ятого підрозділу – це теорема 4.7.

Лема 4.12. *Кількість розв'язків* лінійної *діофантової нерівності (4.5), для яких виконується умова* $0 \le e_1,...,e_{m_2-1} \le p-1$, *є принаймні величина* $U\left(\lfloor m/(m_1+1)\rfloor, p-1\right)$.

Доведення. Нерівність (4.5) рівносильна такій нерівності:

$$m_1 \sum_{i=0}^{m_2-1} ie_i + \sum_{i=0}^{m_2-1} e_i < m, \tag{4.8}$$

Нехай $\sum_{i=0}^{m_2-1} ie_i$ – розбиття числа $m_2 - a$, де число a слід вибрати так, щоб нерівність (4.8) виконувалася; $e_i = 0$ для $m_2 - a \le i \le m_2 - 1$.

Зауважимо, що співвідношення $\sum_{i=0}^{m_2-1} e_i \le \sum_{i=0}^{m_2-1} ie_i$ справедливе для будь-яких $e_1,...,e_{m_2-1}$. Тоді маємо

$$m_1 \sum_{i=0}^{m_2-1} ie_i + \sum_{i=0}^{m_2-1} e_i \le m_1(m_2-a) + m_2 - a < m_1 m_2 = m.$$

Отримуємо $a > m_2/(m_1+1)$ та $m_2 - a < m/(m_1+1)$. Отже, можемо взяти $m_2 - a = \lfloor m/(m_1+1)\rfloor$. Лему доведено.

Застосовуючи теорему 4.5 та лему 4.12, отримуємо наведену далі таку лему.

Лема 4.13. *Нехай* b *– ненульовий елемент початкового поля* F_q. *Тоді елемент* $\theta + b$ має в *розширенні* $F_q(\theta) = F_q[x]/(x^m - a)$ *мультиплікативний порядок принаймні*

$$\frac{\exp\left\{2{,}5\sqrt{\left(m/(m_1+1)-p\right)(1-1/d)-(p-1)^2}\right\}}{\left\{13\left[(m/(m_1+1)-p)/(p(p-1))-1\right]\right\}^{p-1}}.$$

Доведення. Спочатку зауважимо, що згідно з теоремою 4.5 та лемою 4.12, елемент $\theta + b$ має в $F_q(\theta) = F_q[x]/(x^m - a)$ порядок принаймні $U(\lfloor m/(m_1+1) \rfloor, p-1)$.

Далі знаходимо явну нижню оцінку для $U(\lfloor m/(m_1+1) \rfloor, p-1)$. Нагадаємо, що згідно з (2.1) $U(n, d-1) = Q(n, d)$.

Виходячи з [98] (див. доведення теореми 5.1) для $Q(n,d)$ справедлива така нерівність:

$$Q(n,d) \geq \{U(\lfloor \lfloor n/d \rfloor/(d-1) \rfloor)\}^{d-1}. \qquad (4.9)$$

Підставляючи (2.3) (якщо взяти $\lfloor \lfloor n/d \rfloor/(d-1) \rfloor$ замість n) у формулу (4.9), отримуємо

$$Q(n,d) \geq \{U(\lfloor \lfloor n/d \rfloor/(d-1) \rfloor)\}^{d-1} = \frac{\exp\{2{,}5(d-1)\sqrt{\lfloor \lfloor n/d \rfloor/(d-1) \rfloor}\}}{\{13\lfloor \lfloor n/d \rfloor/(d-1) \rfloor\}^{d-1}}.$$

Оскільки $\lfloor a \rfloor > a - 1$, то маємо

$$Q(n,d) \geq \frac{\exp\{2{,}5(d-1)\sqrt{(n/d-1)/(d-1)-1}\}}{\{13((n/d-1)/(d-1)-1)\}^{d-1}} =$$
$$= \frac{\exp\{2{,}5\sqrt{(n-d)(1-1/d)-(d-1)^2}\}}{\{13((n-d)/(d(d-1))-1)\}^{d-1}}.$$

Приймаючи до уваги, що згідно з формулою (2.1) справедлива наступна рівність:

$$U(\lfloor m/(m_1+1) \rfloor, p-1) = Q(\lfloor m/(m_1+1) \rfloor, p)$$

та $n = m/(m_1+1)-1,\quad d = p$, отримуємо потрібну оцінку для $U(\lfloor m/(m_1+1)\rfloor, p-1)$. Лему доведено.

Основним результатом п'ятого підрозділу цього розділу є наведена далі теорема 4.7.

Теорема 4.7. *Можна явно збудувати в скінченому полі* $F_q(\theta)= F_q[x]/(x^m - a)$ *елемент з мультиплікативним порядком принаймні максимум таких двох чисел:* 2^{m_1} *та величина*

$$\frac{\exp\left\{2{,}5\sqrt{(m/(m_1+1)-p)(1-1/d)-(p-1)^2}\right\}}{\left\{13\left[(m/(m_1+1)-p)/(p(p-1))-1\right]\right\}^{p-1}}.$$

Доведення. Маємо такі дві нижні оцінки мультиплікативного порядку. Згідно з лемою 4.13 елемент $\gamma = \theta + b$ має мультиплікативний порядок принаймні наступна величина:

$$\frac{\exp\left\{2{,}5\sqrt{(m/(m_1+1)-p)(1-1/d)-(p-1)^2}\right\}}{\left\{13\left[(m/(m_1+1)-p)/(p(p-1))-1\right]\right\}^{p-1}}.$$

Згідно з лемою 4.7 елемент $\gamma = \theta^{m_2} + b$ має мультиплікативний порядок принаймні 2^{m_1}.

Таким чином, ми можемо явно збудувати (взявши залежно від співвідношення між наведеними раніше параметрами, елемент $\theta + b$ або елемент $\theta^{m_2} + b$) в розширеному скінченому полі $F_q[x]/(x^m - a)$ елемент, який має мультиплікативний порядок принаймні максимум двох вказаних нижніх оцінок. Теорему доведено.

Зауважимо, що оцінка з леми 4.13 є точною оцінкою знизу для мультиплікативного порядку елементів вигляду $\theta+b$ у заданому скінченному полі. Разом з тим, вона громіздка і її не завжди зручно використовувати для порівняння різних скінченних полів. Як наближену оцінку можна взяти наступну величину: $\exp\left(2{,}5\sqrt{\frac{m}{m_1}}\right)$. Тоді прирівнюємо, розраховуючи на найгірший можливий випадок, дві вказані нижні оцінки для мультиплікативних порядків:

$$2^{m_1}=\exp\left(2{,}5\sqrt{\frac{m}{m_1}}\right)$$

і отримуємо $m_1=\sqrt[3]{6{,}25(\log_2 e)^2 m}$. Як наслідок, можемо явно збудувати в розширенні $F_q(\theta)=F_q[x]/(x^m-a)$ скінченного поля F_q елемент з такою наближеною нижньою оцінкою на його мультиплікативний порядок: $2^{\sqrt[3]{6{,}25(\log_2 e)^2 m}}$.

4.6. Висновки до розділу

У даному розділі розглянуто явні нижні межі для мультиплікативного порядку елементів у розширеннях скінченних полів на основі поліномів Куммера. Це розширення, які мають вигляд $F_q[x]/(x^m-a)$ для деяких величин q, m та a.

У першому підрозділі описуємо, якими повинні бути перелічені величини, щоб вказане розширення існувало. Умова існування вказаного розширення зводиться до того, що біном x^m-a має бути нерозкладним над початковим скінченним полем F_q. У скінченних полях характеристики два є лише один нерозкладний біном, а саме $x+1$. Тому у четвертому розділі

вважаємо, що характеристика поля є непарною. У випадку $q=3$ єдине можливе розширення існує для степеня розширення рівного $m=2$. Якщо ж $q\geq 5$, то можемо будувати розширення для нескінченної кількості степенів розширення m. Проте, для будь-якої непарної характеристики існує нескінченна кількість степенів розширення, для яких немає нерозкладних біномів над початковим полем.

Другий підрозділ присвячений розгляду випадку, коли виконується умова: степінь розширення m ділить число $q-1$ ненульових елементів початкового поля. У цьому випадку отримуємо так звані розширення 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 третьому підрозділі у довільних розширеннях скінченних скінченних полів на основі поліномів Куммера 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.

У четвертому підрозділі підсилюємо нижню межу для мультиплікативного порядку елементів із використанням максимуму функції кількості розв’язків діофантового рівняння.

В п’ятому підрозділі підсилюємо нижню межу для мультиплікативного порядку елементів із залученням оцінки знизу для кількості розбиттів натурального числа.

Результати цього розділу опубліковано в роботах [8, 9, 18, 109, 117, 121, 122].

Розділ 5

Елементи великого порядку в скінченних полях на основі поліномів Артіна-Шраєра

У даному розділі явно будуємо елементи великого мультиплікативного порядку в розширеннях скінченних полів вигляду $F_p[x]/(x^p - x - a)$. Такі розширення існують для будь-якого простого числа p, що випливає із теорії Артіна-Шраєра для довільних полів ненульової характеристики.

Теорія Артіна-Шраєра [92] є частиною теорії Галуа для довільних полів. Також її можна розглядати у випадку ненульової характеристики поля як аналог теорії Куммера для розширень Галуа степеня, який дорівнює характеристиці поля p. Вказану теорію, названу пізніше їх іменами, запропонували для випадку розширень простого степеня p Артін та Шраєр у 1927 році, а Вітт у 1936 році узагальнив її на розширення степеня, який дорівнює степеню простого числа, тобто для випадку p^n.

Якщо поле K (не обов'язково скінченне) має характеристику p, де p – довільне просте число, то будь-який поліном вигляду $x^p - x - a$ для елемента a з поля K, називають поліномом Артіна-Шраєра. Коли a не належить до підмножини $\{y \mid y \in K, y = x^p - x \text{ для } x \in K\}$, цей поліном є нерозкладним в $K[x]$, а його поле розкладу над K є циклічним розширенням поля K степеня p. І навпаки, будь-яке розширення Галуа поля K степеня p, рівного характеристиці поля K, є полем розкладу якогось полінома Артіна-Шраєра. Це можна довести, використовуючи аналоги методів у теорії Куммера, такі як теорема Гілберта 90 та адитивні когомології Галуа.

Розглянуті розширення називають розширеннями Артіна-Шраєра. У тому випадку, коли степінь розширення дорівнює p^n, їх переважно називають розширеннямя Артіна-Шраєра-Вітта.

5.1. Нижня межа для порядку елементів

В першому підрозділі явно будуємо елементи великого порядку в розширеннях Артіна-Шраєра скінченних полів та даємо явну оцінку знизу на їх мультиплікативний порядок. Більш точно, явно будуємо в скінченних полях вигляду $F_{p^p} = F_p[x]/(x^p - x - a)$ елементи мультиплікативного порядку більшого від $(p-1)\cdot 4^p$.

Ми беремо лінійний двочлен від елемента, який задає розширення, та всі його спряжені, що також належать до підгрупи, породженої цим двочленом, і будуємо їх різні добутки. Усі спряжені вказаного лінійного двочлена над простим підполем F_p також є лінійними двочленами. Ідея запропонована Берізбейтіа в праці [32] як вдосконалення алгоритму AKS з роботи [23] та розвинута в праці [44] для розширень Куммера. Також в [46] без доведення та деталізації наведено зауваження про аналогію розширень Куммера та розширень Артіна-Шраєра.

Для будь-якого простого числа p розширенням Артіна-Шраєра скінченого поля F_p є поле F_{p^p}. Наслідок 3.79 з роботи [97] дає необхідну і достатню умову нерозкладності полінома $x^p - x - a$ над полем F_q, яке має характеристику p. Згідно з вказаним наслідком поліном $x^p - x - a$ є нерозкладним тоді і тільки тоді, коли слід елемента a над полем F_p не дорівнює нулю. Оскільки в даному випадку $q = p$, а степінь розширення

$m=1$, то слід елемента a над полем F_p дорівнює $Tr_{F_p}(a)=\sum_{i=0}^{m-1}a^{q^i}=a$, і поліном x^p-x-a є нерозкладним над F_p для будь-якого ненульового елемента a з F_p.

Тому з обчислювальної точки зору можна вважати, що наступні поля рівні: $F_{p^p}=F_p[x]/(x^p-x-a)$. Нехай $\theta=x\ (\mathrm{mod}\ x^p-x-a)$ – суміжний клас елемента x за ідеалом, породженим поліномом x^p-x-a. Зрозуміло, що справедлива рівність $\theta^p=\theta+a$. Наступна лема є очевидним наслідком леми 1.1 при $f(x)=x^p-x-a$.

Лема 5.1. *Якщо поліноми $g(x)$ та $h(x)$ з $F_p[x]$ степеня меншого за p різні, то класи цих поліномів в $F_{p^p}=F_p[x]/(x^p-x-a)$ також є різними.*

Лема 5.2. *Спряжені над полем F_p елемента $\theta+b$ ($b\in F_p$) мають вигляд $\theta+b+ia$ для $i=0,\ldots,p-1$.*

Доведення. Розглянемо спряжені над полем F_p елемента $\theta+b$, тобто елементи, в які він переходить при дії автоморфізму Фробеніуса.

Покажемо, що виконується співвідношення $(\theta+b)^{p^i}=\theta+b+ia$, що для будь-якого натурального числа i. Доведемо це індукцією за i.

Очевидно, що для $i=0$ рівність виконується. Припустимо, що вона виконується для деякого числа i. Тоді для $i+1$ маємо:

$$(\theta+b)^{p^{i+1}}=[(\theta+b)^{p^i}]^p=(\theta+b+ia)^p=\theta^p+b+ia=\theta+b+(i+1)a.$$

Отже, рівність справедлива для будь-якого натурального числа i. Лему доведено.

Зауважимо, що елементи $\theta+b+ia$, які фігурують у формулюванні леми 5.2 є попарно різними при $i=0,...,p-1$.

Зафіксуємо цілі числа $1\le c_-\le c\le p-1$. Аналогічно до підрозділу 4.2 розглянемо множину $S(p,c_-,c)$ таких відображень f з множини $\{0,...,p-1\}$ в множину цілих чисел, для яких виконуються наступні умови:

$$\text{I)}\ |\{i\mid f(i)<0\}|=c_-,$$

$$\text{II)}\ \sum_{i,f(i)<0}|f(i)|\le c,$$

$$\text{III)}\ \sum_{i,f(i)\ge 0}f(i)\le p-1-c.$$

Виконуючи доведення аналогічно до доведення леми 4.3, отримуємо таку лему.

Лема 5.3. *Число елементів множини* $S(p,c_-,c)$ *дорівнює*

$$\binom{p}{c_-}\binom{c}{c_-}\binom{2p-c_--c-1}{p-c-1}.$$

Лема 5.4. $|S(p,c_-,c)|>4^p$ *для* $p\ge 41$.

Доведення. Доведення майже точно повторює доведення леми 4.4. Слід лише зауважити, що число p є характеристикою скінченного поля і через це повинне бути простим числом. Тому беремо найближче більше від числа 39 просте число, яке дорівнює 41. Лему доведено.

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

Доведення. Згідно з лемою 5.2 спряжені елемента $\theta+b$ (включаючи сам елемент $\theta+b$) мають вигляд $\theta+b+ia$ для $i=0,...,p-1$. Зрозуміло, що всі вони належать до підгрупи $\langle\theta+b\rangle$.

Нехай $S(p,c\_,c)$ - множина відображень f з множини $\{0,...,p-1\}$ в множину цілих чисел з описаними раніше властивостями I, II, III. Для кожного елемента f з множини $S(p,c\_,c)$ утворюємо добуток $\prod_{0\le i\le p-1}(\theta+b+ia)^{f(i)}$, який також належить до $\langle\theta+b\rangle$. Ми стверджуємо, що двом різним елементам f та g з множини $S(p,c\_,c)$ відповідають різні добутки.

Доведемо це методом від протилежного. Припустимо, що елементи f та g різні, але відповідні їм добутки однакові:

$$\prod_{0\le i\le p-1}(\theta+b+ia)^{f(i)}=\prod_{0\le i\le p-1}(\theta+b+ia)^{g(i)}. \tag{5.1}$$

Таким чином, елемент θ є коренем полінома $\prod_{0\le i\le p-1}(x+b+ia)^{f(i)}-\prod_{0\le i\le p-1}(x+b+ia)^{g(i)}$. Оскільки поліном x^p-x-a є мінімальним поліномом для θ , то можемо записати наступну рівність:

$$\prod_{0\le i\le p-1}(x+b+ia)^{f(i)}=\prod_{0\le i\le p-1}(x+b+ia)^{g(i)}(\mathrm{mod}(x^p-x-a)).$$

Тоді справедливе таке співвідношення для поліномів:

$$\begin{gathered}\prod_{0\le i\le p-1,\,f(i)\ge 0}(x+b+ia)^{f(i)}\prod_{0\le i\le p-1,\,g(i)<0}(x+b+ia)^{-g(i)}=\\ \prod_{0\le i\le p-1,\,f(i)<0}(x+b+ia)^{-f(i)}\prod_{0\le i\le p-1,\,g(i)\ge 0}(x+b+ia)^{g(i)}(\mathrm{mod}(x^p-x-a))\end{gathered} \tag{5.2}$$

Так як маємо поліном степеня рівного величині

$$\sum_{0\le i\le p-1,\,f(i)\ge 0}f(i)+\sum_{0\le i\le p-1,\,g(i)<0}(-g(i))\le p-1<\deg(x^p-x-a)$$

у лівій частині та поліном степеня, який дорівнює

$$\sum_{0\le i\le p-1,\, f(i)<0} (-f(i)) + \sum_{0\le i\le p-1,\, g(i)\ge 0} g(i) \le p-1 < \deg(x^p - x - a)$$

у правій частині рівності (5.2), то згідно із лемою 5.1 вказані поліноми рівні як поліноми над початковим простим полем F_p , тобто справедлива наступна рівність:

$$\prod_{0\le i\le p-1,\, f(i)\ge 0} (x+b+ia)^{f(i)} \prod_{0\le i\le p-1,\, g(i)<0} (x+b+ia)^{-g(i)} = \prod_{0\le i\le p-1,\, f(i)<0} (x+b+ia)^{-f(i)} \prod_{0\le i\le p-1,\, g(i)\ge 0} (x+b+ia)^{g(i)}. \qquad (5.3)$$

У рівності (5.3) маємо нерозкладні та попарно різні множники $\theta + b + ia$, $i = 0,..., p-1$. Ця рівність суперечить однозначності розкладу поліномів над полем F_p, що робить рівність (5.1) неможливою. Отже, добутки, які відповідають різним елементам множини $S(p, c_-, c)$, не можуть бути однаковими.

Таким чином, кількість різних розглянутих добутків, які належать до циклічної підгрупи, породженої елементом $\theta + b$, дорівнює кількості елементів у множині $S(p, c_-, c)$. Згідно з лемою 5.3 кількість елементів у множині $S(p, c_-, c)$ дорівнює

$$\binom{p}{c_-}\binom{c}{c_-}\binom{2p-c_--c-1}{p-c-1}.$$

За лемою 5.4 маємо, що для випадку $p \ge 41$ справедлива нерівність $|S(p, c_-, c)| > 4^p$. Звідси випливає наведене в даній теоремі твердження. Теорему доведено.

Аналізуючи доведення теореми 5.1, можна також сформулювати такий наслідок, який аналогічний до наслідку 4.1.

Наслідок 5.1. *Припустимо, що* $p \geq 41$. *Для будь-якого ненульового елемента* b *поля* F_p *елемент* $\theta + b$ *розширення Артіна-Шраєра* F_{p^p} *має мультиплікативний порядок принаймні*

$$\operatorname{ord}(\theta + b) \geq \max_{0 \leq k_- \leq k \leq m} \binom{p}{c_-} \binom{c}{c_-} \binom{2p - c_- - c - 1}{p - c - 1}.$$

Зауважимо, що для випадку $2 \leq p < 41$ можна, використовуючи комп'ютерні обчислення, явно збудувати примітивні елементи поля F_{p^p}. Це зроблено в наступному другому підрозділі. Тому немає сенсу у цьому разі розглядати такі оцінки для мультиплікативних порядків елементів, які наведені у теоремі 5.1.

Лема 5.5. *Числа* $p-1$ *та* $N_p = p^{p-1} + \ldots + p + 1$ *є взаємно простими.*

Доведення. Припустимо, що число t є дільником числа $p-1$. Тоді маємо порівняння $p \equiv 1 \pmod{t}$, виходячи з якого отримуємо:

$$p^{p-1} + \ldots + p + 1 \equiv 1 + \ldots + 1 = p \equiv 1 \pmod{t}.$$

Це означає, що число t не є дільником числа $p^{p-1} + \ldots + p + 1$. Отже, числа $p-1$ та N_p – взаємно прості. Лему доведено.

Лема 5.6. *Елемент* θ *має в* F_{p^p} *мультиплікативний порядок, який є дільником числа* N_p.

Доведення. Зрозуміло, що $\beta = \theta^{N_p} = \prod_{i=0}^{p-1} \theta^{p^i}$ – це норма елемента $N_{F_{p^p}/F_p}(\theta)$, яка належить до F_p. Оскільки виконується співвідношення

$$\beta = \theta^p + \sum_{i=2}^{p-1} a_i \theta^i + (p-1)!\theta$$

та вірне порівняння $(p-1)!\equiv -1(\mathrm{mod}\, p)$ (за теоремою Вільсона), то, враховуючи $\theta^p - \theta = 1$ та $\sum_{i=2}^{p-1} a_i \theta^i = 0$, маємо $\beta = 1$. Лему доведено.

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

Доведення. Кількість елементів мультиплікативної групи $F_{p^p}^*$ дорівнює

$$p^p - 1 = (p-1)(p^{p-1} + \ldots + p + 1).$$

Згідно з лемою 5.5 числа $p-1$ та $N_p = p^{p-1} + \ldots + p + 1$ є взаємно простими. Таким чином, мультиплікативна група поля F_{p^p} є внутрішнім прямим добутком двох підгруп: з $p-1$ та з N_p елементів. Примітивний елемент a має мультиплікативний порядок $p-1$. Згідно з лемою 5.6 елемент θ має в F_{p^p} мультиплікативний порядок, який є дільником числа N_p. Тоді згідно з лемою 2.1 мультиплікативний порядок всіх елементів вигляду $\theta + b$ ($b \in F_p$) також є дільником числа N_p. Виходячи з теореми 5.1, порядок елемента $\theta + b$ більший від 4^p. Отже, порядок елемента $a(\theta + b)$ є більшим від $(p-1)\cdot 4^p$. Наслідок доведено.

У підрозділі 3.1 нами пояснено особливий інтерес до циклотомічних розширень (і гауссових періодів) з точки зору ефективної аппаратної реалізації помножувачів для F_{q^n} та пов'язаних із цим нормальних базисів для поля F_{q^n} над F_q, що є є оптимальними або мають малу складність. Аналогічно підвищений інтерес до розширень Артіна-Шраєра можна, зокрема, обгрунтувати й наступним чином. Згідно з [102, наслідок 5.3.10,

пункт 1] вірне наступне формулювання: для довільних елементів $\alpha, \beta \in F_q^*$ з умовою $Tr_{F_q / F_p}(\beta) = 1$ поліном

$$x^p - \frac{1}{\beta}\alpha x^{p-1} - \frac{1}{\beta}\alpha^p$$

є нерозкладним над F_q, а його корені утворюють нормальний базис над F_q складності щонайбільше $3p-2$. Тобто, якщо зупинитись на частковому випадку $q = p$, то можна ствердити, що розширення Артіна-Шраєра F_{p^p} ізоморфне полю, в якому існує нормальний базис малої складності. Власне йдеться про складність $3p-2$, яка близька до оптимальної.

5.2. Деякі примітивні елементи

Почнемо даний підрозділ з прикладу, в якому знайдено мультиплікативні порядки елементів для низки розширень Артіна-Шраєра. Наведений приклад показує, що отримана в першому підрозділі нижня межа для порядку є значно меншою від реальних мультиплікативних порядків елементів.

Приклад 5.1. У випадку поля F_{p^p} мультиплікативнй порядок всіх елементів вигляду $\theta + b$ ($b \in F_p$) дорівнює

$$\text{величині } \frac{2^2-1}{2-1} = 3 \text{ для випадку } p = 2,$$

$$\text{величині } \frac{3^3-1}{3-1} = 13 \text{ для випадку } p = 3,$$

$$\text{величині } \frac{5^5-1}{5-1} = 781 \text{ для випадку } p = 5,$$

величині $\frac{7^7-1}{7-1}=137257$ для випадку $p=7$,

величині $\frac{11^{11}-1}{11-1}=28531167061$ для випадку $p=11$.

Розглянемо відповідні скінченні поля та виконані в них комп'ютерні обчислення.

1. Випадок скінченного поля F_{2^2}.

Характеристика поля дорівнює $p=2$. Згідно з виконаними комп'ютерними обчисленнями кількість елементів мультиплікативної групи поля дорівнює 2^2-1=3 і мультиплікативнй порядок елемента θ дорівнює 3. Тоді згідно з лемою 2.1 мультиплікативний порядок всіх елементів вигляду $\theta+b$ ($b\in F_p$) також дорівнює 3.

2. Випадок скінченного поля F_{3^3}.

Характеристика поля дорівнює $p=3$. Згідно з виконаними комп'ютерними обчисленнями кількість елементів мультиплікативної групи поля дорівнює $3^3-1=26$, а мультиплікативнй порядок елемента θ дорівнює 13. Тоді згідно з лемою 2.1 мультиплікативний порядок всіх елементів вигляду $\theta+b$ ($b\in F_p$) також дорівнює 13.

3. Випадок скінченного поля F_{5^5}.

Характеристика поля дорівнює $p=5$. Згідно з виконаними комп'ютерними обчисленнями кількість елементів мультиплікативної групи поля дорівнює $55\text{-}1=3124$, а мультиплікативнй порядок елемента θ дорівнює 781. Тоді згідно з лемою 2.1 мультиплікативний порядок всіх елементів вигляду $\theta+b$ ($b\in F_p$) дорівнює 781.

4. Випадок скінченного поля F_{7^7}.

Характеристика поля дорівнює $p=7$. Згідно з виконаними комп'ютерними обчисленнями кількість елементів мультиплікативної групи поля дорівнює

$7^7 - 1 = 823542$, а мультиплікативнй порядок елемента θ дорівнює 137257. Тоді згідно з лемою 3 мультиплікативний порядок всіх елементів вигляду $\theta + b$ ($b \in F_p$) також дорівнює 137257.

5. Випадок скінченного поля $F_{11^{11}}$.

Характеристика поля дорівнює $p = 11$. Згідно з виконаними комп'ютерними обчисленнями кількість елементів мультиплікативної групи поля дорівнює $11^{11} = 1 = 285311670610$, а мультиплікативнй порядок елемента θ дорівнює 28531167061. Тоді згідно з лемою 2.1 мультиплікативний порядок всіх елементів вигляду $\theta + b$ ($b \in F_p$) дорівнює 28531167061.

Описані в даному прикладі комп'ютерні обчислення виконані на двоядерному процесорі Intel Pentium P6200 2,13 GHz у двох варіантах. У першому варіанті використана власна програма в середовищі Delphi. У другому варіанті для порівняння використано середовище Maple. В обидвох варіантах отримані однакові результати.

Оскільки не всі визнають доведення із застосуванням комп'ютерних обчислень, то даємо також доведення без комп'ютерних обчислень. Для цього досить взяти розклади відповідних порядків мультиплікативних груп скінченних полів на прості множники та обчислити степені елемента θ. Хоча ці результати отримані нами знову ж таки з використанням комп'ютерних обчислень, проте їх можна перевірити вручну. Зокрема, для піднесення до степеня можна використати відомий швидкий ("індійський") алгоритм послідовних піднесень до квадрату та множень. Він служить для виконання операцій піднесення чисел до великих степенів за певним модулем.

Власне для обчислення виразу $a^d \bmod n$ застосовують такий алгоритм:

- записують число d в двійковому вигляді: $d = d_0\ 2^r + ... + d_{r-1}\ 2 + d_r$, де d_i ($i = 1, 2, \ldots, r$) – числа, що дорівнюють 0 або 1, $d_0 = 1$;

- приймають $a_0 = a$ та для $i = 1, 2, ..., r$ обчислюють $a_i \equiv a_{i-1}^2 \cdot a^{d_i} \pmod{n}$.

Тоді число a_r є потрібним результатом.

Наведений алгоритм ґрунтується на порівнянні $a_i \equiv a^{d_0 2^i + ... + d_i} \pmod{n}$ і потребує близько $2 \log_2 d$ множень за модулем n.

Далі описуємо отримання результатів з прикладу 5.1 без застосування комп'ютерних обчислень. Розглянемо відповідні скінченні поля та порядки елементів в них.

1. Оскільки випадок скінченного поля F_{2^2} вимагає нескладних обчислень, то їх не наводимо.

2 Випадок скінченного поля F_{3^3}.

Кількість елементів мультиплікативної групи поля дорівнює 26=2·13. Можна безпосередньо перевірити, що $\theta^{13} = 1$. Таким чином, мультиплікативнй порядок елемента θ дорівнює 13. Тоді згідно з лемою 2.1 мультиплікативний порядок всіх елементів вигляду $\theta + b$ також дорівнює 13.

3. Випадок скінченного поля F_{5^5}.

Кількість елементів мультиплікативної групи поля дорівнює 3124=4·11·71. Можна безпосередньо перевірити, що справедливі такі співвідношення:

$$\theta^{11} = \theta^3 + 2\theta^2 + \theta \neq 1,$$
$$\theta^{71} = 4\theta^4 + 2\theta^3 + 4\theta^2 + 3\theta + 1 \neq 1,$$
$$(\theta^{71})^{11} = 1.$$

Таким чином, мультиплікативнй порядок елемента θ дорівнює 781=11·71. Тоді згідно з лемою 3 мультиплікативний порядок всіх елементів вигляду $\theta + b$ дорівнює 781.

4. Випадок скінченного поля F_{7^7}.

Кількість елементів мультиплікативної групи поля дорівнює 823542=2·3·29·4733. Можна безпосередньо перевірити, що виконуються наступні співвідношення:

$$\theta^{29} = \theta^5 + 4\theta^4 + 6\theta^3 + 4\theta^2 + \theta \neq 1,$$
$$\theta^{4733} = \theta^6 + 5\theta^5 + 2\theta^4 + 5\theta^3 + 4\theta^2 + 2\theta + 5 \neq 1,$$
$$(\theta^{4733})^{29} = 1.$$

Таким чином, мультиплікативнй порядок елемента θ дорівнює 137257=29·4733. Тоді згідно з лемою 2.1 мультиплікативний порядок всіх елементів вигляду $\theta + b$ також дорівнює 137257.

5. Випадок скінченного поля $F_{11^{11}}$.

Кількість елементів мультиплікативної групи поля дорівнює 285311670610=2·5·15797·1806113. Можна безпосередньо перевірити, що справедливі такі співвідношення:

$$\theta^{15797} = 2\theta^{10} + 3\theta^9 + 2\theta^8 + 3\theta^7 + 4\theta^6 + 8\theta^5 + 6\theta^4 + 4\theta^3 + 3\theta^2 + 8\theta \neq 1,$$
$$\theta^{18061137} = 3\theta^{10} + 4\theta^9 + 8\theta^8 + 8\theta^7 + 6\theta^6 + 7\theta^5 + \theta^4 + 5\theta^3 + 4\theta^2 + 6 \neq 1,$$
$$(\theta^{1806113})^{15797} = 1.$$

Таким чином, мультиплікативнй порядок елемента θ дорівнює 28531167061=15797·1806113. Тоді згідно з лемою 2.1 мультиплікативний порядок всіх елементів вигляду $\theta + b$ дорівнює 28531167061.

Далі у даному підрозділі розглядаємо явну побудову деяких елементів великого мультиплікативного порядку (зокрема, примітивних елементів) для розширень полів вигляду F_{p^p}, де p – просте число. При цьому використовуватимемо позначення:

$$N_p = (p^p - 1)/(p - 1) = \sum_{i=0}^{p-1} p^i .$$

Нагадаємо, що згідно з лемою 5.2 у полі F_{p^p} спряжені елемента θ мають вигляд $\theta + ia$ для $i = 0,..., p-1$. Слід зауважити, що елементи $\theta + ia$ є різними для $i = 0,..., p-1$. Згідно з лемою 2.1 всі елементи вигляду $\theta + ia$, $i = 0,..., p-1$, мають однаковий мультиплікативний порядок.

Лема 5.7. [37] *Кожен дільник числа* N_p *має вигляд* $2kp+1$, *де* k *– деяке натуральне число*.

Числа Белла $B(n)$, $n = 0,1,...$ [101, 146] виникають у низці комбінаторних задач. Наприклад, $B(n)$ дає кількість розбиттів множини з n елементів. Доведено, що послідовність цих чисел за модулем довільного простого числа p є періодичною, і мінімальний період b_p ділить N_p. Висловлено гіпотезу [146], що для будь-якого простого p виконується $b_p = N_p$, та виконано певні обчислення з перевірки гіпотези.

Позначаємо мультиплікативний порядок елемента θ в полі F_{p^p} через $\operatorname{ord}\theta$. У [37, твердження 1.2a] без доведення сформульовано таке твердження: для будь-якого простого p виконується $\operatorname{ord}\theta = b_p$. Виходячи з леми 1.2 та відомих формулювань [101, 146] маємо таку гіпотезу про мультиплікативний порядок елемента θ.

Гіпотеза. Елемент θ має в скінченному полі F_{p^p} мультиплікативний порядок, рівний числу N_p.

Гіпотезу перевірено нами для певних значень простого числа p у середовищі комп'ютерної алгебри Maple (пакети Galois Field та NumTheory) Для цього числа N_p розкладено на прості множники і потім обчислено відповідні степені елемента θ. Для піднесення до степеня використовували

описаний раніше відомий швидкий ("індійський") алгоритм послідовних піднесень до квадрата та множень. Для $p > 53$ розкласти N_p на прості множники не вдалося. У цьому разі брали відомі розклади числа N_p на прості множники, отримані в межах так званого Cunnigham проекту [101, 146].

Користуючись цими розкладами, обчислювали θ в степені N_p / q для будь-якого простого дільника q числа N_p. Дійсно, якщо елемент не дорівнює одиниці в степені N_p / q, то цей же елемент не дорівнює одиниці також у степені будь-якого дільника N_p / q.

Отримані чи взяті з літературних джерел прості множники для N_p / q наведені далі. $A(p,l)$ або $B(p,l)$ позначають прості дільники N_p з l десятковими розрядами. Якщо розряди дільника не поміщаються в одному рядку, то запис переносимо в наступні рядки.

Випадок p=2, для якого число $N_p = 3$ має один простий дільник $A(2,1)$=3 вже розглянуто в прикладі 5.1.

Випадок p=3, для якого число $N_p = 13$ має один простий дільник $A(2,1)$=13 раніше описано в прикладі 5.1.

Випадок p=5, для якого число $N_p = 781$ має два простих дільники $A(5,2)$=11, $B(5,2)$=71 раніше описано в прикладі 5.1.

Випадок p=7, для якого число $N_p = 137257$ має два простих дільники $A(7,2)$=29, $A(7,4)$=4733 було розглянуто в прикладі 5.1.

Випадок p=11, для якого число N_p=28531167061 має два простих дільники $A(11,5)$=15797, $A(11,7)$=1806113 вже розглянуто нами в прикладі 5.1.

Для випадку p=13 число N_p=25239592216021 має такі прості дільники: $A(13,2)$=53, $A(13,6)$=264031, $A(13,7)$=1803647. Обчислюючи відповідні степені елемента θ, ми отримали:

$$\theta^{\frac{25239592216021}{53}} = \theta^{476218721057} = 12\theta^{12} + 10\theta^{11} + 9\theta^{10} + 2\theta^9 + 2\theta^8 + 6\theta^7 +$$
$$+ 12\theta^6 + 6\theta^5 + 10\theta^4 + 5\theta^3 + 11\theta^2 + 4\theta + 10 \neq 1,$$

$$\theta^{\frac{25239592216021}{264031}} = \theta^{95593291} = 12\theta^{12} + 4\theta^{11} + 11\theta^{10} + 9\theta^8 + 2\theta^7 +$$
$$+ 10\theta^6 + 11\theta^5 + 2\theta^4 + 12\theta^3 + 2\theta^2 + 7\theta + 6 \neq 1,$$

$$\theta^{\frac{25239592216021}{1803647}} = \theta^{13993643} = 6\theta^{11} + 3\theta^{10} + 3\theta^9 + 5\theta^8 + 3\theta^7 +$$
$$+ 4\theta^6 + 9\theta^5 + 12\theta^3 + 9\theta^2 + \theta + 1 \neq 1.$$

Таким чином, мультиплікативнй порядок елемента θ дорівнює N_p=25239592216021=53·264031·1803647. Тоді згідно з лемою 2.1 мультиплікативний порядок всіх елементів вигляду $\theta + b$ дорівнює N_p=25239592216021.

Для випадку p=17 число N_p=51702516367896047761 має такі прості дільники: $A(17,5)$=10949, $A(17,7)$=1749233, $A(17,10)$=2699538733. Обчислюючи відповідні степені елемента θ, ми отримали:

$$\theta^{\frac{51702516367896047761}{10949}} = \theta^{4722122236541789} = \theta^{16} + 16\theta^{15} + 8\theta^{14} + \theta^{13} + 7\theta^{12} + 3\theta^{11} + \theta^{10} + 11\theta^9 +$$
$$+ 13\theta^8 + 5\theta^7 + 15\theta^6 + 14\theta^5 + 5\theta^4 + 4\theta^3 + 3\theta^2 + 13\theta + 9 \neq 1$$
,

$$\theta^{\frac{51702516367896047761}{1749233}} = \theta^{29557249587617} = \theta^{16} + 14\theta^{15} + 11\theta^{14} + 4\theta^{13} + 7\theta^{12} + 8\theta^{11} + 12\theta^{10} +$$
$$+ 5\theta^9 + 8\theta^8 + 10\theta^7 + 9\theta^6 + 7\theta^5 + 15\theta^4 + 8\theta^3 + 9\theta + 2 \neq 1,$$

$$\theta^{\frac{51702516367896047761}{2699538733}} = \theta^{19152352117} = 6\theta^{16} + 16\theta^{15} + 5\theta^{13} + 2\theta^{12} + 11\theta^{11} + \theta^{10} + 7\theta^9 +$$
$$+ 4\theta^8 + 13\theta^7 + 16\theta^6 + 6\theta^5 + 5\theta^4 + 6\theta^3 + 12\theta^2 + 9 \neq 1.$$

Як бачимо, мультиплікативнй порядок елемента θ дорівнює N_p=51702516367896047761=10949·1749233·269953873353. Тоді згідно з

лемою 2.1 мультиплікативний порядок всіх елементів вигляду $\theta+b$ дорівнює N_p=51702516367896047761.

Для випадку p=19 число N_p має такий простий дільник: $A(19,24)$=109912203092239643840221. Як бачимо, якщо p=19, то число N_p=109912203092239643840221 є простим, і тому без обчислень зрозуміло, що мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=23 число N_p має такі прості дільники: $A(23,3)$=461, $A(23,4)$=1289, $A(23,12)$=831603031789, $A(23,13)$= 1920647391913. Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=29 число N_p має такі прості дільники: $A(29,2)$=59, $A(29,5)$=16763, $B(29,5)$=84449, $A(29,7)$=2428577, $A(29,8)$= 14111459, $B(29,8)$=58320973, $A(29,9)$=549334763. Оскільки згідно з леммою 5.7 кожен дільник N_p (зокрема, простий дільник) має вигляд $2kp+1$, де k – деяке натуральне число, то цей дільник не менший від $2p+1$. У цьому випадку дільник $A(29,2)$=59 точно дорівнює $2p+1$. Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=31 число N_p має такий простий дільник: $A(31,45)$=5689724710241078652870214343019771585348244 81. Як бачимо, якщо p=31, то число N_p є простим, і тому без обчислень зрозуміло, що мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=37 число N_p має такі прості дільники: $A(37,3)$=149, $A(37,4)$=1999, $B(37,4)$=7993, $A(37,5)$=16651, $B(37,5)$=17317, $A(37,14)$=10192715656759, $A(37,26)$=41903425553544839998158239. Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=41 число N_p має такі прості дільники: $A(41,2)=83$, $A(41,7)=1752341$, $A(41,8)=20567159$, $A(41,19)=1876859311090803007$, $A(41,31)=592618758969149753779349775671 9$. Дільник $A(41,2)=83$ точно дорівнює $2p+1$. Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=43 число N_p має такі прості дільники: $A(43,3)=173$, $A(43,6)=120401$,$A(43,62)=19825223972382274003506149120708429799166030$ 881820329892377241. Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=47 число N_p має такі прості дільники: $A(47,4)=1693$, $A(47,36)=255742492896763511474638530188876017$, $A(47,39)=194707033016099228267068299180244011637$.
Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=53 число N_p має такі прості дільники: $A(53,3)=107$, $A(53,6)=141829$, $A(53,17)=16505521259654533$, $A(53,17)=143470720478589313288313473$, $A(53,41)=13033960579631324880455449881408994392143$.
Дільник $A(53,3)=107$ точно дорівнює $2p+1$. Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=59 число N_p має такі прості дільники: $A(59,3)=709$, $A(59,9)=141579233$, $A(59,92)=519032918545811732955628586329770548834605140850704525154528413772606533396805577108032429 13$. Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=61 число N_p має такі прості дільники: $A(61,3)$=977, $A(61,21)$=343625872243632312073,
$A(61,30)$=398853286456071792609917995907,
$A(61,55)$=1000403244183535565720394723140528028235711874491322863.
Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=67 число N_p має такі прості дільники:
$A(67,3)$=269, $A(67,4)$=4021, $A(67,6)$=730837, $A(67,8)$=10960933,
$A(67,34)$=151495488509660402356228791573004 9,
A(67,69)=256633734115152868342504983965010677873884920165866916224701215378677.
Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=71 число N_p має такі прості дільники:
$A(71,6)$=105649, $A(71,16)$=3388409395214741, $A(71,17)$=17882954877203881,
A(71,93)=613683109618829730126963701125307210322365580597593081378705115087489446138913203546134827149.
Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=73 число N_p має такі прості дільники:
$A(73,3)$=293, $B(73,3)$=439, $A(73,7)$=1414741, $A(73,8)$=25239167,
$B(73,8)$=56377463, $A(73,13)$=1295720382587, $A(73,16)$=3611379501352361,
$A(73,19)$=1192167517020392933,
$A(73,31)$=2026896285132395253381459595427,
$A(73,32)$=4996816900275650198711946923957 9.
Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=79 число N_p має такі прості дільники:

$A(79,3)=317$, $A(79,10)=1558537597$, $A(79,21)=171355071830508389477$,
$A(79,26)=54493132908043378263202913$,
$A(79,91)=22721150760046430236542239283038495399004182773576902092080250519046301344744302355875324 69$.

Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=83 число N_p має такі прості дільники:
$A(83,4)=2657$, $A(83,8)=11155201$, $A(83,28)=1008505707601323349156769489$,
$A(83,120)=7836470444281502295741301492530485608458896884973672654179464830453763633187875989865272866159794567160521003597813795 01$.

Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=89 число N_p має такі прості дільники:
$A(89,3)=179$, $A(89,16)=8009862103557709$,
$A(89,25)=5964844210432006407836201$,
$A(89,29)=37307598912253490893302199133$,
$A(89,43)=25754788912985389860028669118711095747052 71$,
$A(89,58)=43300753095996573226343710429674283735337995345667655225 17$.

Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=97 число N_p має такі прості дільники:
$A(97,3)=389$, $A(97,6)=363751$, $A(97,9)=684640163$,
$A(97,29)=11943728733741294764390602153$,
$A(97,51)=54918036119932472441837346627191293171027153407377 3$,
$A(97,95)=85411410016592864938535742262164288660754818699519364051241927961077872028620787589587608357877$.

Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=101 число N_p має такі прості дільники:
$A(101,3)$=607, $A(101,4)$=1213, $B(101,4)$=5657, $A(101,6)$=157561,
$A(101,13)$=9931988588681, $A(101,15)$=102208068907493,
$A(101,18)$=393101595766008847,
$A(101,53)$=126029656265361098723842162970857603088232945227460 17,
$A(101,89)$=827704658429408347048873899828426397792600825329983113733
42321923674635196667950706525429.
Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=103 число N_p має такі прості дільники:
$A(103,4)$=1237, $A(103,23)$=16706917226363953216841,
$A(103,29)$=66372424944116825940401913193,
$A(103,54)$=167321256949237716863040684441514323749790592645938001,
$A(103,98)$=89707581603220837495423746538342394651894047634741087988 2
39408988665008750471193666771965885841573.
Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=107 число N_p має такі прості дільники:
$A(107,9)$=137122213, $A(107,11)$=10508824813,
$A(107,33)$=847261197784821583381604854855693,
$A(107,165)$=10766612031801322134832621304679109736373060932198056581
05114560464119811777376359354144803060636615034532802355308395706 6
08732204196562982376620243300101549002437 21.
Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=109 число N_p має такі прості дільники:
$A(109,4)$=2617, $A(109,25)$=619609874313908289143863 1,
$A(109,49)$=708022605183994255434421517741836511379166407220 3,

$A(109,58)$=208713939295518862111380319002407112397476975917955337364
9,
$A(109,86)$=464027680737994183678386213462383636318527230770013415699
738962634317307438534121839 69.
Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=113 число N_p має такі прості дільники:
$A(113,3)$=227, $A(113,4)$=3391, $B(113,4)$=8363, $A(113,14)$=34314816732569,
$A(113,33)$=785192800256197898644431714786031,
$A(113,47)$=707392557690776166740660853180308116559329202 03,
$A(113,53)$=463619438165353893856898038800353703519601461561358 49,
$A(113,75)$=156188923624921598706429639869280783831517753126599083921
347225838874137507.
Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=137 число N_p має такі прості дільники: $A(137,4)$=1097,
$A(137,6)$=124123, $A(137,10)$=1918644449, $A(137,11)$=12779722229,
$A(137,12)$=574894288613, $A(137,15)$=271329112787027,
$A(137,26)$=54142883557383383180139791,
$A(137,34)$=175942946746093587991677561018 0659,
$A(137,35)$=145022309304806896114020754741 37987,
$A(137,59)$=588561079227779241809167742182641919130595839705607470527
99,
$A(137,85)$=934071232559400840093407339869879240982857127598597347315
693390678356749364687067 2273.
Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=163 число N_p має такі прості дільники:

$A(163,3)=653$, $A(163,4)=2609$, $A(163,5)=41729$, $A(163,8)=31943437$,
$A(163,13)=3727539197017$, $A(163,15)=391683908074297$,
$A(163,19)=8224734227858383253$,
$A(163,294)=873731113569196990890835986192129173409524886694447044065358806870119366079877919813141944527600064407189529943532765535798175050207126450306560075493806670103079302366087579963215445882957195132391218856978994664108287290309304544935690610282525263840051036346118706712633401272010470869112209.$

Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Для випадку p=167 число N_p має такі прості дільники:
$A(167,5)=16033$, $A(167,13)=1001953110409$,
$A(167,27)=669806250678629514045626189$,
$A(167,326)=87444239918513347200417206763885266878486592017697475452275492802524107648922764409669764005440339999576336174215277205753010755144944763014461751186508889382948378115745705303068042382156807989737803733695607334661762256376971899176736131531905948146589448742206136634050702146473811813798265772411904805657766572367475888549.$

Обчислюючи відповідні степені елемента θ, ми отримали, що у цьому випадку мультиплікативний порядок елемента θ дорівнює N_p.

Таким чином, у результаті виконаних обчислень з'ясовано, що наведена раніше гіпотеза справедлива для p<126 та для p=137, 163, 167. Тобто, з урахуванням леми 2.1, маємо такий результат.

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

Для наведених далі простих чисел p повні розклади N_p на прості множники знайдені [101, 146], але в літературі наведені не всі множники.

Для випадку p=149 число N_p має такі прості множники:
$A(149,4)$=1193, $A(149,8)$=51784951, $A(149,9)$=450090559, $B(149,9)$=465814231,
$A(149,44)$=14897084928588789671974072568141537826492971,
$A(149,53)$=24356237167368011037018270166971738740925336580189261,
$A(149,84)$, $A(149,115)$ – не наведені в літературі прості множники.

Для випадку p=157 число N_p має такі прості множники:
$A(157,5)$=86351, $A(157,13)$=1356984109417,
$A(157,61)$=269246276242763276898122337166239758557650345281852679342
0773,
$A(157,99)$, $A(157,167)$ – не наведені в літературі прості множники.

Для випадку p=173 число N_p має такі прості множники:
$A(173,3)$=347, $A(173,6)$=685081, $A(173,18)$=161297590410850151,
$A(173,176)$, $A(173,184)$ – не наведені в літературі прості множники.

Далі наведено прості числа p, для яких повні розклади N_p на прості множники на даний час невідомі. Позначення $C(p,l)$ означає складений дільник числа N_p з l десятковими розрядами, розклад якого невідомий.

Для випадку p=127 число N_p має такі прості множники:
$A(127,3)$=509, $A(127,5)$=22861,$A(127,25)$=1320675600886906675359917,
$C(127,234)$ – складений дільник з невідомим розкладом.

Для випадку p=131 число N_p має такі прості множники:
$A(131,4)$=1049, $A(131,18)$=1742643541410742623061,
$C(131,251)$ – складений дільник з невідомим розкладом.

Для випадку p=199 число N_p має такі прості множники:
$A(139,3)$=557, $A(139,12)$=119833345601,
$C(139,282)$ – складений дільник з невідомим розкладом.

Для випадку p=151 число N_p має такі прості множники:

$A(151,4)$=2417, $A(151,5)$=15101, $A(151,7)$=1234577,

$A(151,37)$=76065860958152040103022674017659073 53,

$C(151,277)$ – складений дільник з невідомим розкладом.

Для випадку p=179 число N_p має такі прості множники:

$A(179,33)$=6183119082113155839913145480811 49,

$C(179,369)$ – складений дільник з невідомим розкладом.

Використовуючи наведені часткові розклади (розклади з невідомими простими або зі складеними множниками), перевірили для всіх можливих випадків, що порядок елемента θ не є власним дільником N_p.

Таким чином, виконані обчислення показують, що наведена на початку гіпотеза, ймовірно, виконується для більшості простих чисел. Тоді елемент θ та спряжені з ним мають великий мультиплікативний порядок, рівний N_p. Виходячи з цього, можна явно збудувати деякі примітивні елементи в розширеннях Артіна-Шраєра.

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* $\mathrm{ord}(u) = N_p$.

Доведення. Кількість елементів мультиплікативної групи $F^*_{p^p}$ дорівнює наступній величині:

$$p^p - 1 = (p-1)(p^{p-1} + \ldots + p + 1).$$

Згідно з лемою 5.5 числа $p-1$ та $N_p = p^{p-1} + \ldots + p + 1$ є взаємно простими. Таким чином, мультиплікативна група розширеного поля F_{p^p} є внутрішнім прямим добутком двох підгруп: підгрупи з $p-1$ та підгрупи з N_p елементів. Тому примітивний елемент поля F_{p^p} є добутком твірного елемента групи з

$p-1$ елементів та твірного елемента групи з N_p елементів. Теорему доведено.

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

Доведення. Згідно з лемою 5.5 числа $p-1$ та $N_p = p^{p-1}+...+p+1$ взаємно прості. Таким чином, мультиплікативна група поля F_{p^p} є внутрішнім прямим добутком двох підгруп: з $p-1$ та з N_p елементів. Елемент α породжує підгрупу з $p-1$ елементів, а елемент $\theta+ia$ – підгрупу з N_p елементів. Значить, елемент $\alpha(\theta+ia)$ примітивний в F_{p^p}.

Згідно з лемою 5.7, кожен дільник числа N_p не менший від $2p+1$. Тоді найбільший спільний дільник числа від 2 до $p-1$ та N_p дорівнює 1. Отже, порядок елемента $(\theta+ia)^j$ ($j=2,...,p-1$) збігається з порядком $\theta+ia$ і дорівнює N_p. Елемент α породжує підгрупу з $p-1$ елементів, а $(\theta+ia)^j$ – підгрупу з N_p елементів. Таким чином, елемент $\alpha(\theta+ia)^j$ – примітивний в F_{p^p}. Наслідок доведено.

Як видно з наведених раніше розкладів, N_p може бути простим числом.

Теорема 5.4. *Якщо N_p – просте число, то всі примітивні елементи поля F_{p^p} мають вигляд $\alpha\cdot u$, де α – примітивний елемент в F_p, а u – неодиничний елемент поля F_{p^p} з нормою 1.*

Доведення. Мультиплікативна група $F^*_{p^p}$ розширення Артіна-Шраєра є внутрішнім прямим добутком підгрупи F^*_p та підгрупи з N_p елементів.

Елемент α породжує підгрупу F_p^*. Оскільки N_p – просте число, то в підгрупі A з N_p елементів кожен неодиничний елемент є твірним. Всі елементи з A (і тільки вони) мають норму 1. У результаті отримуємо твердження теореми. Теорему доведено.

Зауважимо, що крім примітивних елементів вигляду $\alpha(\theta+ia)^j$ (кількість яких дорівнює $(p-1)\cdot p\cdot\lambda(p-1)$, де λ позначає функцію Ейлера, в полі F_{p^p} є також інші примітивні елементи, оскільки їх загальна кількість дорівнює

$$\lambda(p^p-1)=\lambda(p-1)\cdot\lambda(N_p).$$

Теорема 5.5. *Множина примітивних елементів поля F_{p^p} розбивається на підмножини по p спряжених елементів у кожній.*

Доведення. Спочатку покажемо, що загальна кількість примітивних елементів $\lambda(p-1)\cdot\lambda(N_p)$ ділиться на p. Для цього досить показати, що на p ділиться співмножник $\lambda(N_p)$. Дійсно, функція Ейлера λ володіє властивістю мультиплікативності. Число N_p має хоча б один простий дільник і він записується як $2kp+1$ для деякого натурального k. Тоді $\lambda(N_p)$ ділиться на $\lambda(2kp+1)=2kp$.

Будь-який примітивний елемент поля F_{p^p} має p спряжених елементів над полем F_p [97]. Неважко перевірити, що спряженість елементів є відношенням еквівалентності. Тоді дві підмножини попарно спряжених елементів або не перетинаються або збігаються. Теорему доведено.

Приклад 5.2. Випишемо всі примітивні елементи у випадку $p=3$, тобто для поля F_{3^3}. Кількість елементів мультиплікативної групи поля дорівнює

$26 = 2 \cdot 13$. Усього в цьому полі є $\lambda(26) = \lambda(2) \cdot \lambda(13) = 12$ примітивних елементів. У полі F_3 є лише один примітивний елемент: він дорівнює 2. Мультиплікативнй порядок кожного з трьох елементів θ, $\theta+1$, $\theta+2$ дорівнює 13. Кожен з цих елементів породжує підгрупу, яка складається із $N_p = 13$ елементів.

Згідно з теоремою 5.3 елемент 2θ є примітивним. Спряжені з ним примітивні елементи: $2\theta+1$, $2\theta+2$. За теоремою 5.3 елемент $2\theta^2$ також є примітивним. Спряжені з ним примітивні елементи: $2\theta^2+\theta+2$, $2\theta^2+2\theta+2$. Наведені 6 примітивних елементів є елементами вигляду, описаного в теоремі 5.3. Наведені далі 6 примітивних елементів не є примітивними елементами такого вигляду.

Обчислення дали, що елемент $2\theta^2+1$ дорівнює θ^8. Тобто цей елемент належить до підгрупи елементів з нормою 1. Тоді згідно з теоремою 5.4 елемент $2(2\theta^2+2) = \theta^2+1$ є примітивним. Спряжені з ним примітивні елементи: $\theta^2+2\theta+2$, $\theta^2+\theta+2$.

Виконані обчислення показують, що елемент θ^2+2 дорівнює θ^{12}. Тобто цей елемент належить до підгрупи елементів з нормою 1. Тоді згідно з теоремою 5.4 елемент $2(\theta^2+2) = 2\theta^2+1$ є примітивним. Спряжені з ним примітивні елементи: $2\theta^2+\theta$, $\theta^2+2\theta$.

Як бачимо, у цьому прикладі згідно з теоремою 5.5 множина з 12 примітивних елементів розбивається на 4 підмножини по 3 спряжених примітивних елементи в кожній підмножині:

перша підмножина: $\{2\theta,\ 2\theta+1,\ 2\theta+2\}$;

друга підмножина: $\{2\theta^2, 2\theta^2+\theta+2,\ 2\theta^2+2\theta+2\}$;

третя підмножина: $\{\theta^2+1,\ \theta^2+2\theta+2,\ \theta^2+\theta+2\}$;

четверта підмножина: $\{2\theta^2+1,\ 2\theta^2+\theta,\ \theta^2+2\theta\}$.

Усі дванадцять примітивних елементів є елементами вигляду, описаного теоремою 5.4.

5.3. Нижня межа для добутку біноміальних коефіцієнтів

Ми даємо у даному підрозділі нижню межу для добутку біноміальних коефіцієнтів, пов'язаному з тестуванням простоти або побудовою елементів великого мультиплікативного порядку в певних скінченних полях.

Нехай m – натуральне число. Задача знаходження таких цілих чисел $d_{\_}$, d, які задовольняють умову $0 \le d_{\_} \le d < m$ та для яких добуток біноміальних коефіцієнтів

$$C(d_{\_}, d) = \binom{m}{d_{\_}} \binom{d}{d_{\_}} \binom{2m - d_{\_} - d - 1}{m - d - 1} \tag{5.4}$$

є великим, виникає у двох наступних випадках.

1. Оптимізація алгоритму AKS тестування простоти цілих чисел.

Ефективні тести простоти (які визначають є задане ціле число простим чи складеним) використовують у прикладних застосуваннях: низка криптографічних протоколів потребує великих простих чисел.

У 2002 році Агравал, Кайал та Саксена [23] запропонували детермінований поліноміальний алгоритм AKS, який визначає є вхідне ціле число n простим чи складеним. Доведено [80], що алгоритм AKS виконується за час $(\log n)^{7.5+o(1)}$. Також відомі суттєво змінені версії AKS [30, 80] із часом виконання $(\log n)^{4+o(1)}$. Алгоритм у [30] використовує поняття сертифіката для будь-якого цілого числа n. Доведено, що коли знайдено сертифікат для числа, то воно є степенем простого числа. У цьому разі легко вирішити, чи число є простим. Під час знаходження сертифіката суттєвим

моментом є перевірка певної нерівності, для чого необхідно обчислювати вираз виду (5.4). Для побудови сертифіката вибираємо d_- та d.

2. Побудова елементів великого порядку для певних розширень скінченних полів.

Згідно з підрозділом 4.2 маємо наслідок 4.1 для розширень Куммера, а згідно з підрозділом 5.2 аналогічний наслідок 5.1 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.

Бачимо, що добуток біноміальних коефіцієнтів виду (5.4) наявний у вказаних результатах. Таким чином, задача максимізації добутку (5.4) є важливою. У праці [30] показано, що для $d \approx m/2$ та $d_- \approx 0{,}2928m$ маємо $C(d_-, d) \approx 5{,}8284^m$. Зауважимо, що значення $5{,}8284^m$ не є нижньою межею для D, а лише певним наближеним значенням. Дійсно, розглянемо наступні числові приклади.

Для випадку $m = 37$, максимум D досягається при $d_- = 10, d = 17$ та дорівнює $D = C(10,17) \approx 2{,}81 \cdot 10^{25}$. Не обчислюємо точне ціле значення для величини D, бо хочемо лише порівняти її із значенням $(5{,}8284)^{37} = 2{,}12 \cdot 10^{28}$. Для випадку $m = 511$, маємо $D = C(149,254) \approx 4{,}17 \cdot 10^{386}$. У той же час, $(5{,}8284)^{511} = 1{,}57 \cdot 10^{391}$.

З точки зору низки прикладних застосувань (зокрема, криптографії) бажаною є теоретична нижня межа, яка є точним, а не наближеним значенням, для введеної величини D. Ми даємо далі у третьому підрозділі таку нижню межу для максимуму добутку біноміальних коефіцієнтів у формулі (5.4).

Лема 5.8. *Справедливі наступні рівності для біноміальних коефіцієнтів:*

$$\binom{u}{v} = \frac{u}{u-v}\binom{u-1}{v} \tag{5.5}$$

та

$$\binom{u}{v} = \frac{u}{v}\binom{u-1}{v-1}. \tag{5.6}$$

Доведення. Щоб довести (5.5) зауважимо, що

$$\binom{u}{v} = \frac{(u-v+1)\cdot\ldots\cdot u}{1\cdot 2\cdot\ldots\cdot v}$$

та

$$\binom{u-1}{v} = \frac{(u-v)\cdot\ldots\cdot(u-1)}{1\cdot 2\cdot\ldots\cdot v}.$$

Спостереження, що

$$\binom{u-1}{v-1} = \frac{(u-v+1)\cdot\ldots\cdot(u-1)}{1\cdot 2\cdot\ldots\cdot(v-1)}$$

дозволяє довести (5.6). Лему доведено.

Даємо далі в теоремі 5.6 та наслідку 5.2 нижню межу для максимуму D добутку (5.4) біноміальних коефіцієнтів. Вказана теорема використовує такі результати із другого розділу: нерівність (2.4) з леми 2.2 та нерівність (2.5) з наслідку 2.1.

Теорема 5.6. *При* $m \geq 8$ *маємо таку нижню межу:*

$$D > \frac{h^m}{30m^{3/2}}, \tag{5.7}$$

де $h = 4\cdot 5^{5/4}/3^{3/2}$.

Доведення. Виберемо значення для чисел k, d_- та d наступним чином: $k = m \bmod 4$, $d_- = (m-k)/4$, $d = (m-k)/2$. Зрозуміло, що k приймає значення із множини $\{0,1,2,3\}$.

Покажемо спочатку, що для числа $k \in \{0,1,2,3\}$ виконується така нерівність

$$\binom{m}{d_-} = \binom{m}{(m-k)/4} > \gamma(k)\binom{m-k}{(m-k)/4}, \qquad (5.8)$$

причому значення величини γ дорівнюють: $\gamma(0)=1$, $\gamma(1)=32/25$, $\gamma(2)=(16/13)\cdot(14/11)$, $\gamma(3)=(32/27)\cdot(28/23)\cdot(24/19)$.

Рівність $\gamma(0)=1$ очевидна. Для випадку $k=1$, застосувавши рівність (5.5) до лівої частини рівності (5.8), отримуємо:

$$\binom{m}{(m-1)/4} = 4m/(3m+1)\binom{m-1}{(m-1)/4}.$$

Оскільки, для $m \geq 8$, виконується умова $4m/(3m+1) \geq 32/25$, то маємо $\gamma(1)=32/25$.

Для випадку $k=2$, застосуємо рівність (5.5) до лівої частини рівності (5.8) послідовно два рази. Після першого застосування вказаної рівності отримуємо:

$$\binom{m}{(m-2)/4} = 4m/(3m+2)\binom{m-1}{(m-2)/4}$$

Друге застосування рівності (5.5) дає таке співвідношення:

$$\binom{m-1}{(m-2)/4} = 4(m-1)/[3(m-1)+1]\binom{m-2}{(m-2)/4}.$$

Так як для $m \geq 8$, справедлива умова $4m/(3m+2) \geq 16/13$ та умова $4(m-1)/[3(m-1)+1] \geq 14/11$, то маємо також співвідношення $\gamma(2)=(16/13)\cdot(14/11)$.

У випадку $k=3$, застосуємо рівність (5.5) до лівої частини рівності (5.8) послідовно три рази. Після першого застосування вказаної рівності отримуємо наступне співвідношення:

$$\binom{m}{(m-3)/4} = 4m/(3m+3)\binom{m-1}{(m-3)/4}.$$

Друге застосування рівності (5.5) дає таке співвідношення:

$$\binom{m-1}{(m-3)/4} = 4(m-1)/[3(m-1)+2]\binom{m-2}{(m-3)/4}.$$

Третє застосування рівності (5.5) приводить до наступного співвідношення:

$$\binom{m-2}{(m-3)/4} = 4(m-2)/[3(m-2)+1]\binom{m-3}{(m-3)/4}.$$

Оскільки, при $m \geq 8$, справедливі нерівності

$$4m/(3m+3) \geq 32/27,$$

$$4(m-1)[3(m-1)+2] \geq 28/23,$$

$$4(m-2)/[3(m-2)+1] \geq 24/19,$$

то маємо рівність $\gamma(3) = (32/27)\cdot(28/23)\cdot(24/19)$.

Покажемо тепер, що справедливі наступні співвідношення:

$$\binom{2m-d\_-d-1}{m-d-1} = \binom{2m-3(m-k)/4-1}{m-2(m-k)/4-1} > \delta(k)\binom{5(m-k)/4}{2(m-k)/4}, \qquad (5.9)$$

де значення величини δ дорівнюють: $\delta(0)=1/3$, $\delta(1)=39/25$, $\delta(2)=(21/8)\cdot(19/13)\cdot(17/11)$,

$\delta(3)=(5/2)\cdot(41/14)\cdot(37/27)\cdot(33/23)\cdot(29/19)$.

Для випадку $k=0$, застосувавши рівність (5.6) до лівої частини рівності (5.9), отримуємо:

$$\binom{5m/4-1}{2m/4-1}=(2m/4-1)/(5m/4-1)\binom{5m/4}{2m/4}.$$

Так як, для $m\geq 8$, виконується $(2m/4-1)/(5m/4-1)\geq 3/9$, то маємо $\delta(0)=1/3$.

Для випадку $k=1$, застосуємо рівність (5.5) до лівої частини рівності (5.9). У результаті отримуємо таке співвідношення:

$$\binom{5(m-1)/4+1}{2(m-1)/4}=(5(m-1)/4+1)/(3(m-1)/4+1)\binom{5m/4}{2m/4}.$$

Оскільки, для $m\geq 8$, виконується нерівність

$$(5(m-1)/4+1)/(3(m-1)/4+1)\geq 39/25,$$

то маємо $\delta(1)=39/25$.

У випадку $k=2$, спочатку застосуємо рівність (5.6) до лівої частини рівності (5.9):

$$\binom{5(m-2)/4+3}{2(m-2)/4+1}=(5(m-2)/4+3)/(2(m-2)/4+1)\binom{5(m-2)/4+2}{2(m-2)/4}.$$

Потім застосуємо до лівої частини рівності (5.9) рівність (5.5) послідовно два рази. Перше застосування вказаної рівності дозволяє отримати таке співвідношення:

$$\binom{5(m-2)/4+2}{2(m-2)/4}=(5(m-2)/4+2)/(3(m-2)/4+2)\binom{5(m-2)/4+1}{2(m-2)/4}.$$

Друге застосування вказаної рівності (5.5) дозволяє отримати наступне співідношення:

$$\binom{5(m-2)/4+1}{2(m-2)/4} = (5(m-2)/4+1)/(3(m-2)/4+1)\binom{5(m-2)/4}{2(m-2)/4}.$$

Так як, для $m \geq 8$, виконуються такі три нерівності:

$$(5(m-2)/4+3)/(2(m-2)/4+1) \geq 21/8,$$
$$(5(m-2)/4+2)/(3(m-2)/4+2) \geq 19/13,$$
$$(5(m-2)/4+1)/(3(m-2)/4+1) \geq 17/11,$$

то отримуємо $\delta(2) = (21/8)\cdot(19/13)\cdot(17/11)$.

Для $k=3$, спочатку до лівої частини рівності (5.9) застосуємо рівність (5.6) два рази. Після першого застосування вказаної рівності, отримуємо співвідношення:

$$\binom{5(m-3)/4+5}{2(m-3)/4+2} = (5(m-3)/4+5)/(2(m-3)/4+2)\binom{5(m-3)/4+4}{2(m-3)/4+1}$$

Після другого застосування вказаної рівності, отримуємо наступне співвідношення:

$$\binom{5(m-3)/4+4}{2(m-3)/4+1} = (5(m-3)/4+4)/(2(m-3)/4+1)\binom{5(m-3)/4+3}{2(m-3)/4}.$$

Потім застосуємо рівність (5.5) послідовно три рази. Після першого застосування маємо:

$$\binom{5(m-3)/4+3}{2(m-3)/4} = (5(m-3)/4+3)/(3(m-3)/4+3)\binom{5(m-3)/4+2}{2(m-3)/4}.$$

Друге застосування рівності (5.5) дає співідношення:

$$\binom{5(m-3)/4+2}{2(m-3)/4} = (5(m-3)/4+2)/(3(m-3)/4+2)\binom{5(m-3)/4+1}{2(m-3)/4}.$$

Третє застосування рівності (5.5) дає наступну рівність:

$$\binom{5(m-3)/4+1}{2(m-3)/4} = (5(m-3)/4+1)/(3(m-3)/4+1)\binom{5(m-3)/4}{2(m-3)/4}.$$

Оскільки, для $m \geq 8$, справедливі нерівності

$$(5(m-3)/4+5)/(2(m-3)/4+2)\binom{5(m-3)/4+4}{2(m-3)/4+1} \geq 5/2,$$

$$(5(m-3)/4+4)/(2(m-3)/4+1) \geq 41/14,$$

$$(5(m-3)/4+3)/(3(m-3)/4+3) \geq 37/27,$$

$$(5(m-3)/4+2)/(3(m-3)/4+2) \geq 33/23$$

та

$$(5(m-3)/4+1)/(3(m-3)/4+1) \geq 29/19,$$

то маємо

$$\delta(3) = (5/2)\cdot(41/14)\cdot(37/27)\cdot(33/23)\cdot(29/19).$$

Комбінуючи (5.8) та (5.9), отримуємо, що для $k \in \{0,1,2,3\}$ та $n = m-k$ виконується наступна нерівність:

$$D > \gamma(k)\delta(k)\binom{n}{n/4}\binom{n/2}{n/4}\binom{5n/4}{2n/4}. \qquad (5.10)$$

Тепер ми даємо, використовуючи нерівності (2.4) та (2.5), нижні межі для кожного біноміального коефіцієнта з правого боку нерівності (5.10).

Застосовуючи нерівність (2.5) до коефіцієнта $\binom{n}{n/4}$ з правого боку (5.10) (у цьому випадку $t = n/4$, $s = 4$), маємо:

$$\binom{n}{n/4} > (1/\sqrt{2\pi}) \cdot e^{1-1/(2n)} (n/4)^{-1/2} \frac{4^{n-3}}{3^{3n/4-3}}. \qquad (5.11)$$

Зауважимо, що має виконуватися $t \geq 2$, тобто $m - k \geq 8$, і якщо $k = 0$, то $m \geq 8$.

Застосовуючи нерівність (2.5) до коефіцієнта $\binom{n/2}{n/4}$ з правого боку (5.10) (у цьому разі $t = n/4$, $s = 2$), маємо:

$$\binom{n/2}{n/4} > (1/\sqrt{2\pi}) \cdot e^{1-1/(2n)} (n/4)^{-1/2} 2^{n/2-1} \qquad (5.12)$$

Застосовуючи нерівність (2.4) до коефіцієнта $\binom{5n/4}{2n/4}$ з правого боку (5.10) (у цьому випадку $t = n/4$, $s = 5$, $r = 2$), маємо:

$$\binom{5n/4}{3n/4} > \frac{1}{\sqrt{2\pi}} \cdot e^{3-1/(2n)} (n/4)^{-1/2} \frac{5^{5n/4-4}}{2^{n/2-4} \cdot 3^{3n/4+1/2}}. \qquad (5.13)$$

Підставляючи нерівності (5.11), (5.12) та (5.13) в нерівність (5.10) та беручи до уваги

$$\frac{1}{e^{3/(2(m-k))}} \geq \frac{1}{e^{3/(2(m-3))}},\ 1 < e^{3/(2(m-3))} < 1{,}35 \text{ для } m \geq 8,\ \frac{1}{(m-k)^{3/2}} \geq \frac{1}{m^{3/2}},$$

отримуємо таку межу

$$D > \frac{3^7 \cdot e^4}{10^5 \cdot \pi^{3/2} \cdot 1{,}35} \cdot \frac{\gamma(k)\delta(k)}{h^k} \cdot \frac{h^m}{m^{3/2}}. \qquad (5.14)$$

Оскільки справедлива нерівність

$$\frac{3^7 \cdot e^4}{10^5 \cdot \pi^{3/2} \cdot 1{,}35} > 0{,}1588,$$

а мінімальне значення для $\frac{\gamma(k)\delta(k)}{h^k}$ досягається при $k = 3$ та дорівнює 0,21, то нерівність (5.14) перетворюється в нижню межу (5.7). Теорему доведено.

Отримана нижня межа (5.7) для добутку (5.4) біноміальних коефіцієнтів є точною теоретичною межею та порівняною із відповідним значенням з роботи [30]. Беручи до уваги в (5.7), що $5{,}7556 < 4 \cdot 5^{5/4} / 3^{3/2} < 5{,}7557$, маємо наступний наслідок.

Наслідок 5.4. *Для* $m \geq 8$ *виконується наступна нерівність:*

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

Зрозуміло, що для достатньо великих m основний внесок у праву частину останньої нерівності дається членом $(5{,}7556)^m$.

Зауважимо, що наш результат у наслідку 5.2 є нижньою межею для D при $m \geq 8$ із константою 5,7556. Якщо дозволити m бути більшим, скажімо $m \geq 32$, то отримуємо аналогічну нижню межу з константою 5,8230. Щоб досягнути це, вибираємо в доведенні теореми 5.6 $d_- = m/4 + m/32$, $d = m/2$. Для випадку $m \geq 1024$, беручи наступні значення величин: $d_- = m/4 + m/32 + m/128 + m/512 + m/1024$, $d = m/2$, можна отримати нижню межу з константою 5,8284.

5.4. Обмеження на порядок елемента, який задає розширення

У четвертому підрозділі розглядаємо обмеження на порядок $\operatorname{ord}\theta$ елемента θ, який задає розширення Артіна-Шраєра, та спряжених з ним елементів, якщо виконується обмеження $\operatorname{ord}\theta < N_p$. Наведені далі результати узагальнюють деякі результати з праці [37] та спрощують певні доведення із вказаної роботи.

Нехай розклад числа u за основою p має вигляд

$$u = u_{p-1}p^{p-1} + ... + u_1 p + u_0,$$

де $0 \le u_i \le p-1$ $(i = 0,..., p-1)$. Тоді циклічним зсувом вліво на один розряд розрядів цього числа називаємо перестановку σ розрядів числа за правилом: $\sigma(u_i) = u_{(i+1) \bmod p}$ для $i = 0,..., p-1$. У результаті отримуємо таке число v:

$$v = u_{p-2}p^{p-1} + ... + u_0 p + u_{p-1}.$$

Циклічний зсув вліво на один розряд розрядів числа u проілюстровано на рис. 5.1.

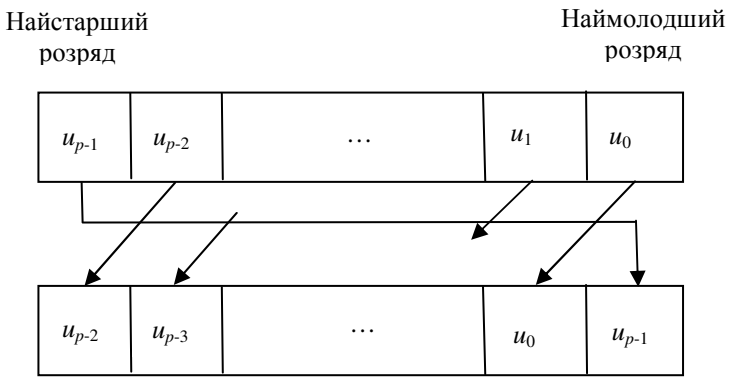

Рис. 5.1. Циклічний зсув розрядів числа на один розряд вліво.

Якщо маємо рівність $\theta^u = 1$, то застосування циклічного зсуву вліво на один розряд до розрядів числа u рівносильне дії автоморфізму Фробеніуса φ на ліву частину вказаної рівності. Циклічний зсув вліво на k розрядів – це послідовне застосування k разів циклічного зсуву вліво на один розряд, тобто дія k-го степеня φ^k автоморфізму Фробеніуса.

Циклічним зсувом вправо на один розряд розрядів числа u називаємо перестановку τ розрядів цього числа за правилом: $\tau(u_i) = u_{(i-1) \bmod p}$ для $i = 0,..., p-1$. У результаті циклічного зсуву вправо на один розряд розрядів числа u отримуємо таке число w:

$$w = u_0 p^{p-1} + ... + u_2 p + u_1 .$$

Циклічний зсув вправо на один розряд розрядів числа u проілюстровано на рис. 5.2.

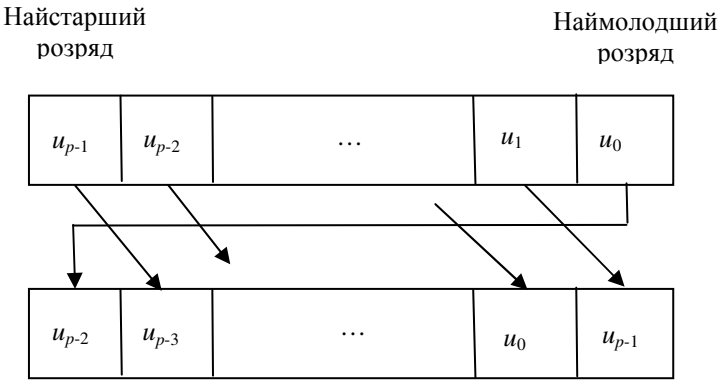

Рис. 5.2. Циклічний зсув розрядів числа на один розряд вправо.

Якщо маємо рівність $\theta^u = 1$, то застосування циклічного зсуву вправо на один розряд до розрядів числа u рівносильне дії автоморфізму $\varphi^{-1} = \varphi^{p-1}$ на ліву частину вказаної рівності. Циклічний зсув вправо на k розрядів – це

послідовне застосування k разів циклічного зсуву вправо на один розряд. При цьому зрозуміло, що φ^p є тотожним відображенням.

Зауважимо, що циклічний зсув вліво (вправо) на k розрядів дає той самий результат, що і циклічний зсув вправо (відповідно вліво) на $p-k$ розрядів. Зокрема, циклічний зсув вліво на 1 розряд дає такий же ж результат, як і циклічний зсув вправо на $p-1$ розряд. Проте, з точки зору простоти розгляду варто користуватися поняттями як циклічного зсуву вліво, так і циклічного зсуву вправо.

Лема 5.9. (лема про циклічний зсув) *Нехай виконується рівність* $\theta^u = 1$ *та число* v *отримане циклічним зсувом розрядів числа* u. *Тоді справедливе співвідношення* $\theta^v = 1$.

Доведення. Не втрачаючи загальності для визначеності припустимо, що число v отримане циклічним зсувом вліво числа u на k розрядів, де $k < p$. Рівність $\theta^u = 1$ можна записати у вигляді:

$$(\theta^{p^{p-1}})^{u_{p-1}} \ldots (\theta^p)^{u_1} \theta^{u_0} = 1.$$

Враховуючи, що $\theta^p = \theta + 1$, останню рівність перетворюємо до такої форми:

$$(\theta + p - 1)^{u_{p-1}} \ldots (\theta + 1)^{u_1} \theta^{u_0} = 1.$$

Застосуємо тепер до лівої та правої частини рівності k-й степінь φ^k автоморфізму Фробеніуса φ. Так як

$$\varphi^k[(\theta + i)^{u_i}] = (\theta + (i + k) \bmod p)^{u_i} = (\theta + i)^{v_i},$$

то $\theta^v = 1$. Лему доведено.

Приклад 5.3. Проілюструємо введені поняття циклічних зсувів та лемму 5.9 (про циклічний зсув) на прикладі для $p=11$. У цьому випадку всі числа, які розглядаємо, мають одинадцять розрядів у системі числення за основою 11. При цьому маємо $N_p = 28531167061$. Це число розкладається в добуток двох простих чисел 15797 та 1806113. Останній співмножник записуємо за степенями числа 11 таким чином:

$$1806113 = 0\cdot 11^{10} + 0\cdot 11^9 + 0\cdot 11^8 + 0\cdot 11^7 + 1\cdot 11^6 + 0\cdot 11^5 + \\ + 2\cdot 11^4 + 3\cdot 11^3 + 10\cdot 11^2 + 6\cdot 11^1 + 1\cdot 11^0 .$$

Якщо виписувати лише розряди числа, то маємо $u = 00001023A61_{11}$, де A позначає цифру рівну числу 10. Циклічний зсув вліво на один розряд дає число $v = 0001023A610_{11}$. Циклічний зсув вправо на один розряд дає число $w = 100001023A6_{11}$.

Введемо позначення $\theta_1 = \theta^{15797}$. Зрозуміло, що справедлива рівність $(\theta_1)^u = 1$. Виходячи із леми 5.9, виконується також рівність $(\theta_1)^v = 1$ та рівність $(\theta_1)^w = 1$.

Твердження 5.1. *Нехай p –просте число. Нехай $\theta \in F_{p^p}$ є коренем полінома $x^p - x - 1$. Нехай $u = \operatorname{ord}\theta$ – порядок елемента θ. Запишемо u за степенями числа p наступним чином $u = u_{p-1}p^{p-1} + ... + u_1 p + u_0$. Припустимо, що $\operatorname{ord}\theta < N_p$. Тоді виконуються співвідношення:*

$$u_0 = 1,\ u_{p-1} = u_{p-2} = 0,\ u_{p-3} \le \frac{p-1}{2}.$$

Доведення. Оскільки кожен дільник числа N_p має вигляд $2kp+1$, де k – деяке натуральне число, то, очевидно, що наймолодший розряд числа u дорівнює $u_0 = 1$.

Покажемо, що серед розрядів числа u є хоча б один нульовий. Якщо це не так, тобто всі розряди ненульові, то рівність

$$(\theta + p - 1)^{u_{p-1}} \ldots (\theta + 1)^{u_1} \theta^{u_0} = 1$$

ділимо на $(\theta + p - 1)^{u_m} \ldots (\theta + 1)^{u_m} \theta^{u_m} = 1$, де u_m – найменше із чисел u_i $(i = 0, \ldots, p-1)$. Отримуємо число v із нулем на місці з номером m. Це число менше за число u, і, згідно з лемою 5.9, володіє властивістю $\theta^v = 1$. Тоді маємо суперечність із тим, що u є порядком елемента θ.

Припустимо, що u_{p-1} не дорівнює нулю. Використовуючи циклічний зсув, пересуваємо нульовий розряд числа u на місце $p-1$. Маємо число v із нулем у розряді, який має індекс $p-1$. Зрозуміло, що число v менше за число u, і, за лемою 5.9, задовольняє рівність $\theta^v = 1$. У результаті маємо суперечність із тим фактом, що u – порядок елемента θ. Таким чином, ми показали, що u_{p-1} дорівнює нулю.

Користуючись тим, що $u = \operatorname{ord} \theta$ є дільником числа N_p, та, згідно з лемою 5.7. кожен дільник числа N_p має вигляд $2kp + 1$, де k – натуральне число, можемо записати наступну рівність:

$$u(2kp + 1) = p^{p-1} + \ldots + p + 1,$$

де k є натуральним числом. Звідси маємо таку нерівність:

$$u \le \frac{p^{p-1} + \ldots + p + 1}{2p + 1} \le \frac{p-1}{2} \cdot p^{p-3}.$$

З останньої нерівності отримуємо, що $u_{p-2} = 0$ та $u_{p-3} \le \frac{p-1}{2}$. Твердження доведено.

Лема 5.10. *Нехай величини* p, θ *та* u *– такі, як в формулюванні твердження* 5.1. *Тоді виконується наступна нерівність:*

$$u_{p-1} + \ldots + u_1 + u_0 > p.$$

Доведення. Позначимо через m кількість ненульових розрядів u_j. Рівність $\theta^u = 1$ можна записати у вигляді:

$$(\theta + p - 1)^{u_{p-1}} \ldots (\theta + 1)^{u_1} \theta^{u_0} = (\theta + p - 1) \ldots (\theta + 1)\theta.$$

Скорочуючи ліву та праву частину останньої рівності на такі множники $\theta + j$, для яких числа j не дорівнюють нулю, отримуємо наступне співвідношення:

$$\prod_{j, u_j \neq 0} (\theta + j)^{u_j - 1} = \prod_{j, u_j = 0} (\theta + j).$$

Таким чином, маємо, що елемент θ є коренем такого полінома:

$$\varphi(x) = \prod_{j, u_j \neq 0} (x + j)^{u_j - 1} - \prod_{j, u_j = 0} (x + j).$$

Степінь цього полінома повинен бути не менший, ніж p, бо мінімальний поліном для елемента θ дорівнює $x^p - x - 1$ і має степінь p. Доданок $-\prod_{j, u_j = 0} (x + j)$ в поліномі $\varphi(x)$ має степінь менший, ніж p, бо не всі розряди числа u дорівнюють нулю. Значить, не меншим від p повинен бути степінь першого доданка полінома $\varphi(x)$, а саме доданка $\prod_{j, u_j \neq 0} (x + j)^{u_j - 1}$. Отже, можемо записати наступну нерівність:

$$\sum_{j, u_j \neq 0} (u_j - 1) \geq p.$$

Так як число u має хоча б один ненульовий розряд, то отримуємо, що $u_{p-1}+...+u_1+u_0=\sum_{j,u_j\neq 0}u_j>p$. Лему доведено.

Лема 5.11. [37, лема 3.4] *Нехай p, θ та u – такі, як в формулюванні твердження* 5.1. *Тоді $u_{p-1}+...+u_1+u_0>p$. Нехай Tr позначає слід елемента розширеного поля F_{p^p} над початковим полем F_p. Нехай виконується співвідношення*

$$(x+p-1)^{u_{p-1}}...(x+1)^{u_1}x^{u_0}-1=\Omega(x)(x^p-x-1),$$

де $\Omega(x)=\omega_n x^n+...+\omega_1 x+\omega_0$ – деякий поліном із коефіцієнтами ω_k ($k=0,...,n$) із поля F_p. Покладемо $d=u_{p-1}+...+u_1+u_0$ та $n=\deg\Omega(x)$. Тоді правильні такі твердження:

(a) $Tr(\Omega(\theta))\equiv d(\bmod p)$,

(b) $Tr(\Omega(\theta))=-\sum_{k\geq 1,kp-1\leq n}\omega_{kp-1}$.

Твердження 5.2. *Нехай p, θ та u – такі, як в формулюванні твердження* 5.1. *Тоді правильні наступні нерівності:*

$$2p-1\leq u_{p-1}+...+u_1+u_0\leq p^2-\frac{9p}{2}+\frac{5}{2}.$$

Доведення. Покажемо спочатку, що верхня межа, наведена в формулюванні цієї теореми, є вірною. Максимально можливе значення для суми розрядів $u_{p-1}+...+u_1+u_0$ отримуємо, якщо замість кожного із p розрядів беремо найбільшу можливу величину $p-1$, тобто $u_{p-1}+...+u_1+u_0\leq p(p-1)$. Тепер слід врахувати, що згідно із твердженням 5.1 два найстарших розряди u_{p-1} та u_{p-2} дорівнюють нулю, розряд u_{p-3} не перевищує $=\frac{p-1}{2}$, а наймолодший

розряд u_0 дорівнює одиниці. Тому від правої частини останньої нерівності треба відняти числа $p-1$, $p-1$, $p-1-\frac{p-1}{2}=\frac{p-1}{2}$ та $(p-1)-1=p-2$. У результаті отримуємо потрібну межу зверху.

Покажемо тепер, що нижня межа, наведена в формулюванні цієї теореми, є вірною. Із рівності поліномів

$$(x+p-1)^{u_{p-1}}...(x+1)^{u_1}x^{u_0}-1=\Omega(x)(x^p-x-1)$$

маємо $n=d-p$. Припустимо, що $n<p-1$. Оскільки при $k\geq 1$ виконується нерівність $kp-1>n$, то на підставі леми 5.11, частина b, бачимо, що $Tr(\Omega(\theta))=-\sum_{k\geq 1,kp-1\leq n}\omega_{kp-1}=0$ Тоді за лемою 5.11, частина a, отримуємо порівняння $d\equiv 0\,(\mathrm{mod}\,p)$. Враховуючи, що число u має ненульові розряди, тобто $d>0$ та $d=n+p<2p-1$, маємо $d=p$. Тоді виходячи з леми 5.10, приходимо до суперечності, адже $p=d>p$. Таким чином, припущення, що $n<p-1$, тобто $n\geq p-1$. Оскільки $n=d-p$, то нижня межа в формулюванні даної теореми справедлива. Твердження доведено.

Твердження 5.3. *Нехай p, θ та u – такі, як в формулюванні твердження* 5.1. *Тоді кількість нулів всередині запису числа u за степенями числа p не може бути більшою, ніж кількість нулів спереду.*

Доведення. Дійсно, якщо це не так, то за рахунок циклічного зсуву пересуваємо більшу кількість нулів на початок. У результаті отримуємо число менше за початкове, що дає суперечність. Твердження доведено.

Лема 5.12. *Якщо виконується рівність*

$$\begin{aligned}&(\theta+p-1)^{u_{p-1}}...(\theta+t+1)^{u_{t+1}}(\theta+t)^{u_t}(\theta+t-1)^{u_{t-1}}...(\theta+1)^{u_1}\theta^{u_0}=\\&=(\theta+p-1)^{v_{p-1}}...(\theta+t+1)^{v_{t+1}}(\theta+t)^{v_t}(\theta+t-1)^{v_{t-1}}...(\theta+1)^{v_1}\theta^{v_0}\end{aligned},\quad (5.15)$$

то справедлива також рівність

$$(\theta+p-1)^{u_{p-1}}...(\theta+t+1)^{u_{t+1}+1}(\theta+t-1)^{u_{t-1}}...(\theta+1)^{u_1}\theta^{u_0}= \\ =(\theta+p-1)^{v_{p-1}}...(\theta+t+1)^{v_{t+1}}(\theta+t)^{v_t+(p-u_t)}(\theta+t-1)^{v_{t-1}}...(\theta+1)^{v_1}\theta^{v_0}. \quad (5.16)$$

Доведення. Для того, щоб довести рівність (5.16), зауважимо, що

$$(\theta+t)^{u_t}=(\theta+t)^{p}(\theta+t)^{-(p-u_t)}=(\theta+t+1)(\theta+t)^{-(p-u_t)}. \quad (5.17)$$

Представляючи співмножник $(\theta+t)^{u_t}$ у рівності (5.15) згідно з рівністю (5.17) та домножаючи ліву й праву частини рівності (5.15) на величину $(\theta+t)^{p-u_t}$, отримуємо рівність (5.16). Лему доведено.

Твердження 5.4. *Нехай* p, θ *та* u *– такі, як в формулюванні твердження 5.1. Якщо виконується нерівність* $\mathrm{u}=\mathrm{ord}\,\theta<N_p$, *то вірні наступні твердження:*

(a) *кількість ненульових розрядів числа* u *не менша п'яти,*

(b) *якщо кількість ненульових розрядів числа* u *рівна п'яти, то сума будь-яких двох розрядів цього числа, які не дорівнюють нулю або одиниці, не менша, ніж* $p+2$.

Доведення. (a) Будемо використовувати позначення $d=u_{p-1}+...+u_1+u_0$. Згідно з твердженням 5.1 $u_0=1$, а відповідно до твердження 5.2 $d\geq 2p-1$. Оскільки значення усіх розрядів числа u знаходяться між 0 та $p-1$, то кількість k ненульових розрядів не може бути меншою за три, тобто $k\geq 3$.

Розглянемо спочатку випадок $k=3$. Тоді розряд $u_0=1$, а інші два ненульові розряди повинні мати максимальне значення $p-1$. У цьому разі $u_a=u_b=p-1$ для індексів a та b, які задовольняють умови $1\leq a,b\leq p-3$. Візьмемо для визначеності, що $a<b$. Саме число u має в системі числення за основою p такий вигляд:

$$u = (p-1)p^b + (p-1)p^a + 1.$$

Оскільки u є мультиплікативним порядком елемента θ, то можемо записати наступну рівність:

$$(\theta + b)^{p-1}(\theta + a)^{p-1}\theta = 1. \qquad (5.18)$$

Застосовуючи до рівності (5.18) лему 5.10, маємо таке співвідношення:

$$(\theta + b + 1)(\theta + a + 1)\theta = (\theta + b)(\theta + a).$$

Як бачимо, елемент θ є коренем не рівного тотожно нулю полінома третього степеня. Це приводить до суперечності, бо за теоремою 5.2 при $p = 3$ маємо, що величини $\operatorname{ord}\theta$ та N_p співпадають.

Розглянемо тепер випадок $k = 4$. У цьому разі число u має в системі числення за основою p наступний вигляд:

$$u = u_c p^c + u_b p^b + u_a p^a + 1$$

для деяких індексів , що задовольняють умови $1 \le a, b, c \le p-3$. Оскільки u – мультиплікативний порядок елемента θ, то можемо записати наступну рівність:

$$(\theta + c)^{u_c}(\theta + b)^{u_b}(\theta + a)^{u_a}\theta = 1. \qquad (5.19)$$

Застосовуючи до рівності (5.19) лему 5.10, маємо таке співвідношення:

$$(\theta + c + 1)(\theta + b + 1)(\theta + a)^{u_a}\theta = (\theta + c)^{p-u_c}(\theta + b)^{p-u_b}. \qquad (5.20)$$

Враховуючи твердження 5.2, яке дає для суми цифр числа u наступну нижню межу: $d = u_c + u_b + u_a + 1 \ge 2p - 1$, можемо записати такі нерівності:

$$u_a + 3 > u_a + 2 \geq 2p - u_c - u_b .$$

Таким чином, справедливе співвідношення:

$$u_a + 3 > 2p - u_c - u_b . \tag{5.21}$$

Величина $u_a + 3$ в лівій частині (5.21) дорівнює степеню лівої частини нерівності (5.20) як полінома від елемента θ. Величина $2p - u_c - u_b$ в правій частині (5.21) рівна степеню правої частини нерівності (5.20) як полінома від елемента θ. Нерівність (5.21) тоді означає, що елемент θ є коренем тотожно не рівного нулю полінома степеня $u_a + 3$. З іншого боку мінімальний поліном для θ має степінь p. Таким чином, $u_a + 3 \geq p$, тобто

$$p - u_a \leq 3 . \tag{5.22}$$

Застосовуючи такі ж самі міркування, можна отримати нерівності для величин u_b та u_c, аналогічні нерівності (5.22), а саме:

$$p - u_b \leq 3 \tag{5.23}$$

та

$$p - u_c \leq 3 . \tag{5.24}$$

Застосовуючи до рівності (5.19) лему 5.10, можна дістати наступне співвідношення:

$$(\theta + c + 1)(\theta + b + 1)(\theta + a + 1)\theta = (\theta + c)^{p-u_c}(\theta + b)^{p-u_b}(\theta + c)^{p-u_a} .$$

З останньої нерівності бачимо, що елемент θ є коренем полінома степеня, який є максимумом двох чисел : 4 та $(p - u_c) + (p - u_b) + (p - u_a)$. Виходячи з отриманих нерівностей (5.22), (5.23) та (5.24), величина $(p - u_c) + (p - u_b) + (p - u_a)$ не перевищує число 9. Значить, елемент θ є коренем полінома щонайбільше дев'ятого степеня. Тоді отримуємо, що

$p \le 9$. Це приводить до суперечності, бо, на підставі теореми 5.2, у випадку $p \le 9$ (тобто при $p = 2, 3, 5, 7$) маємо, що величини $\operatorname{ord}\theta$ та N_p співпадають.

(b) Для доведення цього пункту слід розглянути випадок $k = 5$. У цьому разі число u має в системі числення за основою p такий вигляд:

$$u = u_e p^e + u_c p^c + u_b p^b + u_a p^a + 1$$

для деяких індексів , що задовольняють умови $1 \le a, b, c, e \le p - 3$. Оскільки u – мультиплікативний порядок елемента θ, то можемо записати наступну рівність:

$$(\theta + e)^{u_e} (\theta + c)^{u_c} (\theta + b)^{u_b} (\theta + a)^{u_a} \theta = 1. \qquad (5.25)$$

Застосовуючи до рівності (5.25) лему 5.10, маємо таке співвідношення:

$$(\theta + e + 1)(\theta + c + 1)(\theta + b)^{u_b} (\theta + a)^{u_a} \theta = (\theta + e)^{p - u_e} (\theta + c)^{p - u_c}. \qquad (5.26)$$

Оскільки, згідно із твердженням 5.2, маємо для суми цифр числа u наступну нижню межу: $d = u_e + u_c + u_b + u_a + 1 \ge 2p - 1$, то виконується нерівність $u_b + u_a + 3 > u_b + u_a + 1 \ge 2p - u_e - u_c$. Таким чином, справедливе співвідношення:

$$u_b + u_a + 3 > 2p - u_c - u_b. \qquad (5.27)$$

Величина $u_b + u_a + 3$ в лівій частині (5.27) дорівнює степеню лівої частини нерівності (5.20) як полінома від елемента θ. Величина $2p - u_c - u_b$ в правій частині (5.27) рівна степеню правої частини нерівності (5.20) як полінома від елемента θ. Нерівність (5.27) тоді означає, що елемент θ є коренем тотожно не рівного нулю полінома степеня $u_b + u_a + 3$. З іншого боку мінімальний поліном для θ має степінь p. Таким чином, $u_b + u_a + 3 \ge p$, тобто

$$u_b + u_a \geq p - 3. \qquad (5.28)$$

Застосовуючи такі ж самі міркування, можна для будь-якої пари із величин u_a, u_b, u_c та u_e отримати нерівності, аналогічні нерівності (5.28). Щоб завершити доведення пункту (b), візьмемо для визначеності (не зменшуючи загальності) пару u_a та u_b. Враховуючи раніше отриману нерівність $u_b + u_a + 1 \geq 2p - u_e - u_c$ та нерівність $u_e + u_c \geq p - 3$ аналогічну нерівності (5.28) для пари u_c та u_e, маємо наступне співвідношення: $u_b + u_a \geq p + 2$, що завершує доведення пункту (b).

Твердження доведено.

5.5. Висновки до розділу

У першому підрозділі явно будуємо елементи великого порядку в розширеннях Артіна-Шраєра скінченних полів та даємо явну оцінку знизу на їх мультиплікативний порядок. Доводимо, що при $p \geq 41$, для будь-якого ненульового елемента b поля F_p елемент $\theta + b$ поля F_{p^p} має порядок більший, ніж величина $(p-1) \cdot 4^p$.

У другому підрозділі показано, що елемент $\theta + ia$, $i = 0,..., p-1$, має в розширенні F_{p^p} початкового простого поля F_p мультиплікативний порядок, який дорівнює величині N_p для $p < 126$ та для p=137,163,167,173. Також проведено часткові перевірки для більших значень простого числа p. Описано певні примітивні елементи в припущенні, що розглянуті раніше елементи мають порядок, що дорівнює величині N_p.

У третьому підрозділі даємо нижню межу для добутку біноміальних коефіцієнтів, пов'язаному з тестуванням великих натуральних чисел на простоту або побудовою елементів великого мультиплікативного порядку в

скінченних полів одного із двох видів: розширеннях Куммера та розширеннях Артіна-Шраєра.

У четвертому підрозділі розглядаємо обмеження на мультиплікативний порядок елемента, який задає розширення Артіна-Шраєра скінченних полів, та спряжених із ним елементів при умові, що цей порядок менший, ніж кількість елементів відповідної мультиплікативної підгрупи.

Результати п’ятого розділу опубліковано в роботах [7, 12, 19, 113, 118].

Розділ 6

Елементи великого порядку в рекурсивних розширеннях скінченних полів

Ефективно побудувати примітивний елемент для заданого скінченного поля в обчислювальній теорії скінченних полів важко – проблема залишається відкритою. Ось чому розглядають менш обмежувальне питання: знайти елемент великого мультиплікативного порядку. Інше менш амбітне, але, мабуть, більш важливе питання, знайти примітивні елементи для якогось конкретного класу скінченних полів. Поліноміальний алгоритм, що знаходить примітивний елемент у скінченному полі малої характеристики, описано в [85]. Проте, алгоритм спирається на два недоведених припущення і не підкріплений ніяким обчислювальним прикладом. Даний розділ можна розглядати як крок у напрямку опису примітивних елементів для якогось конкретного класу скінченних полів. Вивчаємо рекурсивні розширення скінченних полів характеристики два, визначені Конвеєм та визначені Відеманом, а також рекурсивні розширення скінченних полів характеристики більшої від двох. Ми наводимо нижню межу для мультиплікативного порядку деяких елементів у двійкових рекурсивних розширеннях скінченних полів, визначених Конвеєм. Далі описуємо деякі примітивні елементи для перших дванадцяти полів у вежах Конвея. Також формулюємо умову, при виконанні якої елементи такого вигляду є примітивними для довільного поля у вказаній вежі полів. Потім виводимо нижню межу для мультиплікативного порядку деяких елементів у двійкових рекурсивних розширеннях скінченних полів, визначених Відеманом. Крім того, знаходимо нижні межі для порядку елементів у вежах скінченних полів недвійкової характеристики.

6.1. Нижня межа для порядку у вежах Конвея

У першому підрозділі даємо нижню межу для мультиплікативного порядку деяких елементів у двійкових рекурсивних розширеннях скінченних полів, визначених Д. Конвеєм в монографії [62] з комбінаторної теорії ігор та теорії множин. У цій теорії [62, 63, 128, 150] ігри разом із заданою над ними операцією додавання утворюють абелеву групу. Ординальні (порядкові) числа є підмножиною множини ігор, на якій додатково задана операція множення. Ординальні числа з цими операціями додавання та множення утворюють поле.

Також у комбінаторній теорії ігор було введено так звані номери, чи німбери, чи числа Грюнді (англ. терміни nimbers або Grundy numbers), де їх визначено як значення “купи” в нім-іграх. Німбери розглядали як ординальні числа, наділені операціями додавання та множення, що відрізняються від загально прийнятих додавання та множення цих чисел.

Показано, що німбери утворюють із точки зору аксіоматичної теорії множин властивий клас, а не множину. Вказаний клас визначає алгебраїчно замкнене поле характеристики два. Більш точно, доведена Конвеєм теорема стверджує, що клас On ординальних чисел з додаванням $\oplus$ та множенням $\circ$ є алгебраїчно замкнутим полем характеристики два. Це поле будемо позначати On_2.

Для всіх натуральних чисел n, множина німберів менших, ніж 2^{2^n}, утворює скінченне поле $F_{2^{2^n}}$, яке має 2^{2^n} елементів. Зокрема, з цього випливає, що множина скінченних німберів ізоморфна прямій границі при $n \to \infty$ полів $F_{2^{2^n}}$. Це підполе не є алгебраїчно замкненим, оскільки ніяке інше поле F_{2^k} (де k не є степенем двійки) не належить до жодного з цих полів, а, значить, і до їх прямої границі.

Скінченні німбери додають побітово за модулем два. Є також прийоми обчислення добутку скінченних німберів. Це визначається наступними правилами множення степенів Ферма числа два (тобто чисел вигляду 2^{2^n}):

1. Якщо маємо різні степені Ферма числа два: 2^{2^m} та 2^{2^n}, тобто $m \neq n$, то їх німбер добуток дорівнює їх звичайному добутку $2^{2^m+2^n}$;
2. Якщо маємо однакові степені Ферма числа два, тобто $m = n$: власне обчислюємо німбер квадрат степеня Ферма числа два x, то результат дорівнює числу $\frac{3x}{2} = 3 \cdot 2^{2^n-1}$, обчисленому за допомогою звичайного множення натуральних чисел.

Використовуючи ці правила, можемо розкласти два числа на суми степенів двійки та разом з тим для кожного степеня двійки розкласти порядок на степені двійки. Тоді можна використовувати наведені два правила для знаходження добутків степенів, що спрощує спростити обчислення.

При виконанні множення, записуємо таблицю для менших значень і використовуємо її, щоб розширити до більших значень. Розглядаємо всі числа до найближчого степеня Ферма числа два. Так, таблиця 2x2 є частиною таблиці 4x4, а та в свою чергу є частиною таблиці 16x16.

Приклад 6.1. Дамо приклади нім-множення натуральних чисел згідно з наведеними правилами. У цьому разі значок $\circ$ означає нім-множення, а замість звичайного множення натуральних чисел ставитимемо крапку або нічого не ставитимемо. Значок $\oplus$ означає нім-додавання, тобто побітове додавання (без переносу) за модулем числа два.

$16 \circ 16 = 3 \cdot (2^{4-1}) = 3 \cdot 8 = 24$,

$2 \circ 3 = 2 \circ (2 \oplus 1) = 2 \circ 2 \oplus 2 \circ 1 = 3 \cdot 2^{1-1} \oplus 2 = 3 \oplus 2 = (11)_2 \oplus (10)_2 = (01)_2 = 1$,

$2 \circ 4 = 2^{1+2} = 8$, бо 2 та 4 є різними степенями Ферма,

$3 \circ 3 = (2 \oplus 1) \circ (2 \oplus 1) = 2 \circ 2 \oplus 2 \circ 1 \oplus 2 \circ 1 \oplus 1 \circ 1 = 3 \oplus 2 \oplus 2 \oplus 1 = 3 \oplus 1 = 2$,

$$3 \circ 4 = (2 \oplus 1) \circ 4 = 2 \circ 4 \oplus 1 \circ 4 = 8 \oplus 4 = 12,$$

$$10 \circ 7 = (2 \circ 4 \oplus 2) \circ (3 \oplus 4) = 2 \circ 4 \circ 3 \oplus 2 \circ 4 \circ 4 \oplus 2 \circ 3 \oplus 2 \circ 4 =$$
$$= 2 \circ (4 \circ 4) \oplus (2 + 3 \circ 2) \circ 4 \oplus 3 \circ 2 = 2 \circ 6 \oplus (2 \oplus 1) \circ 4 \oplus 1 = \quad ,$$
$$= 2 \circ (2 \oplus 4) \oplus 8 \oplus 4 \oplus 1 = 3 \oplus 8 \oplus 12 \oplus 1 = 6$$

$$100 \circ 200 = (6 \circ 16 \oplus 4) \circ (12 \circ 16 \oplus 8) = (6 \circ 12) \circ (16 \oplus 8) \oplus (6 \circ 8 \oplus 4 \circ 12) \circ 16 \oplus 4 \circ 8 =$$
$$= 9 \circ (16 \oplus 8) \oplus (7 \oplus 13) \circ 16 \oplus 11 = (9 \oplus 7 \oplus 13) \circ 16 \oplus 9 \circ 8 \oplus 11 =$$
$$= (9 \oplus 7 \oplus 13) \circ 16 \oplus (5 \oplus 11) = 3 \circ 16 \oplus 14 = 62$$

Виконання операції додавання та операції множення німберів, менших від 16, проілюстровано відповідно в табл. 6.1. та табл. 6.2.

Таблиця 6.1

Виконання операції додавання німберів

$\oplus$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Таблиця 6.2

Виконання операції множення німберів

∘	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	3	1	8	10	11	9	12	14	15	13	4	6	7	5
3	0	3	1	2	12	15	13	14	4	7	5	6	8	11	9	10
4	0	4	8	12	6	2	14	10	11	15	3	7	13	9	5	1
5	0	5	10	15	2	7	8	13	3	6	9	12	1	4	11	14
6	0	6	11	13	14	8	5	3	7	1	12	10	9	15	2	4
7	0	7	9	14	10	13	3	4	15	8	6	1	5	2	12	11
8	0	8	12	4	11	3	7	15	13	5	1	9	6	14	10	2
9	0	9	14	7	15	6	1	8	5	12	11	2	10	3	4	13
10	0	10	15	5	3	9	12	6	1	11	14	4	2	8	13	7
11	0	11	13	6	7	12	10	1	9	2	4	15	14	5	3	8
12	0	12	4	8	13	1	9	5	6	10	2	14	11	7	15	3
13	0	13	6	11	9	4	15	2	14	3	8	5	7	10	1	12
14	0	14	7	9	5	11	2	12	10	4	13	3	15	1	8	6
15	0	15	5	10	1	14	4	11	2	13	7	8	3	12	6	9

Як було сказано раніше, шлях формування таблиць додавання та множення полягає в записові кожного числа в двійковій системі числення, та розкладові відповідних степенів у суму степенів двійки. Якщо позначимо через e_n німбер число 2^n, то спрощуючим правилом для додавання є те, що для всіх n виконується умова $e_n + e_n = 0$.

З точки зору теорії скінченних полів, поля скінченних німберів зручніше описувати в термінах послідовних розширень попередніх полів з використанням нерозкладних поліномів. Зокрема, так ці поля описано в праці [150], і цей підхід використано в першому та другому підрозділах.

Більш точно, ми розглядаємо наступні скінченні поля, ізоморфні полям німберів:

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

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

$$c_{i+1}^2 + c_{i+1} + \prod_{j=-1}^{i} c_j = 0. \qquad (6.1)$$

Зауважимо, що наведений поліном є нерозкладним над полем L_i, виходячи з такого загального результату, який використовуватимемо і надалі в цьому розділі для встановлення нерозкладності поліномів, які з'являються у вежах скінченних полів.

Лема 6.1. [97, вправа 3.85] *Якщо поліном* $x^p - x - \alpha$ *є нерозкладним над полем* F_q *характеристики* p, а β *– корінь цього полінома в якомусь розширенні поля* F_q, *то поліном* $x^p - x - \alpha\beta^{p-1}$ *є нерозкладним над* $F_q(\beta)$.

У даному випадку $p = 2$, $\alpha = \prod_{j=-1}^{i-1} c_j$, $\beta = c_i$. Оскільки $p = 2$, то $-1 = 1$ та $\beta^{p-1} = c_i$. Отже, виникає така вежа скінченних полів характеристики два:

$$L_{-1} = F_2(c_{-1}) = F_2 \subset L_0 = F_2(c_0) \subset L_1 = L_0(c_1) \subset L_2 = L_1(c_2) \subset \ldots$$

При цьому число елементів кожного наступного поля у даній вежі дорівнює кількості елементів попереднього поля, піднесеній до квадрату. Вказана побудова дуже приваблива з точки зору прикладних застосувань, оскільки можна виконувати операції над елементами скінченного поля рекурсивно, а тому ефективно [87].

Множина N натуральних чисел із згаданими раніше додаванням та множенням є підполем поля On_2. Це підполе ізоморфне квадратичному замиканню поля F_2. Вказане замикання можна описати як $F_2(c_0, c_1, c_2, ...)$, де c_i задовольняє рівнянню (6.1). Для кожного i маємо

$$F_2(c_0, c_1, ..., c_{i-1}) = F_{2^{2^i}},$$

а елемент c_i має степінь два над цим полем. З цього випливає, що будь-який елемент поля $F_2(c_0, c_1, c_2, ...)$ можна записати єдиним способом у вигляді:

$$\sum_{V \in W} \prod_{i \in V} c_i, \tag{6.2}$$

де W є скінченною множиною скінченних підмножин множини N.

Будь-яке натуральне число можна однозначно записати як $\sum_{k \in W} 2^k$, де множина $W \subset \mathrm{N}$ є скінченною. Записуючи кожне $k \in W$ як $\sum_{i \in V} 2^i$ для деякої скінченної множини $V \subset \mathrm{N}$, залежної від k, бачимо, що кожне натуральне число має єдине подання:

$$\sum_{V \in W} \prod_{i \in V} 2^{2^i}, \tag{6.3}$$

де множина W така ж, як і раніше.

Конвей довів [62], що існує ізоморфізм полів $(N, \oplus, \circ) \to F_2(c_0, c_1, c_2, ...)$, який відображає елемент вигляду (6.2) в елемент вигляду (6.3). Виходячи із рівняння (6.1), можемо виконувати нім-множення будь-яких двох натуральних чисел.

Приклад 6.2. Проілюструємо нім-множення $77 \circ 77$ двох натуральних чисел, виходячи із рівняння (6.1). Число $77 = 2^{2^2} \cdot 2^{2^1} + 2^{2^1} \cdot 2^{2^0} + 2^{2^1} + 1$ відображається в $c_2 c_1 + c_1 c_0 + c_1 + 1$. Тоді $77 \circ 77$ відображається в

$$c_2^2 c_1^2 + c_1^2 c_0^2 + c_1^2 + 1.$$

Оскільки, згідно з рівнянням (6.1), $c_2^2 = c_2 + c_1 c_0$, $c_1^2 = c_1 + c_0$, $c_0^2 = c_0 + 1$, то останній вираз зводиться до такого виразу:

$$c_2 c_1 + c_2 c_0 + c_1 c_0 + c_1 + 1.$$

Цей вираз є образом натурального числа

$$2^{2^2} \cdot 2^{2^1} + 2^{2^2} \cdot 2^{2^0} + 2^{2^1} \cdot 2^{2^0} + 2^{2^1} + 1 = 109.$$

Таким чином, маємо рівність $77 \circ 77 = 109$.

Із наведеного ізоморфізму полів випливає, що для кожного i ординальне число $2^{2^i} = \{0,1,2,...,2^{2^{i-1}}\}$ є підполем поля N.

Легко безпосередньо перевірити наступні факти: елемент c_0 є примітивним у полі L_0, а елемент c_1 є примітивним у полі L_1. Разом з тим, Х. Ленстра [94, вправа 2] довів таке твердження: елемент 2^{2^i} є примітивним коренем поля $2^{2^{i+1}}$, тоді і тільки тоді, коли $i = 0$ або $i = 1$. У термінах поліномів це означає: якщо $i \geq 2$, то елемент c_i не є примітивним у полі L_i. Деякі примітивні елементи для підполів поля N, ізоморфних L_2, L_3 та L_4, знайдені в праці [35] з використанням середовища SageMath. Таким чином, для випадку $i \geq 2$, виникають наступні запитання:

1) дати нижню межу для мультиплікативного порядку ord c_i елемента c_i;

2) які елементи є примітивними в полях L_i.

Ми частково даємо відповіді на сформульовані запитання у підрозділі 6.1 та підрозділі 6.2.

Далі отримуємо допоміжні для першого підрозділу результати.

Зауважимо що, для $i \geq 0$, кількість елементів мультиплікативної групи $L_i^* = L_i \setminus \{0\}$ дорівнює $2^{2^{i+1}} - 1$. Якщо позначити числа Ферма $N_j = 2^{2^j} + 1$ ($j \geq 0$), то потужність множини L_i^* дорівнює $\prod_{j=0}^{i} N_j$. Наприклад, для перших п’яти полів у вежі Конвея маємо:

$$\left|K_0^*\right| = 2^{2^1} - 1 = 3,\ \left|K_1^*\right| = 2^{2^2} - 1 = 15 = 3 \cdot 5,$$

$$\left|K_2^*\right| = 2^{2^3} - 1 = 255 = 3 \cdot 5 \cdot 17,$$

$$\left|K_3^*\right| = 2^{2^4} - 1 = 65535 = 3 \cdot 5 \cdot 17 \cdot 257,$$

$$\left|K_4^*\right| = 2^{2^5} - 1 = 4294967295 = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537.$$

Будемо при $k \geq 0$ використовувати позначення $a_k = \prod_{j=0}^{k} c_j$. Наводимо далі результати, пов'язані з властивостями чисел Ферма.

Лема 6.2. [64, розділ 1.3]. *Для* $j \geq 1$, *виконується наступна рівність:*

$$N_j = \prod_{k=0}^{j-1} N_k + 2.$$

Як наслідок з леми 6.2, можна записати наступну лему.

Лема 6.3. [64, розділ 1.3] Для $j \geq 0$, *числа Ферма* N_j *є попарно взаємно простими.*

Відомо, що для $1 \leq j \leq 4$ числа Ферма $N_1 = 5$, $N_2 = 17$, $N_3 = 257$, $N_4 = 65537$ є простими [64, таблиця 1.3], а для $5 \leq j \leq 11$ вони повністю розкладені на прості множники. Також відомі часткові розклади цих чисел для $j > 11$.

Лема 6.4. *Для* $j \geq 2$, *дільник* $m > 1$ *числа* N_j *має вигляд* $m = l \cdot 2^{j+2} + 1$, *де* l – *натуральне число.*

Доведення. Результат, отриманий Ейлером і Лукасом, (див. [64 , теорема 1.3.5]) стверджує: для $j \geq 2$, простий дільник числа N_j має вигляд $l \cdot 2^{j+2} + 1$,

де l є натуральним числом. Розглянемо добуток двох чисел вказаного вигляду:

$$(l_1 \cdot 2^{j+2} + 1)(l_2 \cdot 2^{j+2} + 1) = (l_1 l_2 \cdot 2^{j+2} + l_1 + l_2) \cdot 2^{j+2} + 1.$$

Як бачимо, це число такого ж вигляду. Лему доведено.

Лема 6.5. *При* $i \geq 2$*, числа* $N_i + 1$ *та* N_j *є взаємно простими для* $1 \leq j \leq i-1$.

Доведення. Виходячи з леми 6.2, отримуємо таке співвідношення: $N_i + 1 = \prod_{j=0}^{i-1} N_j + 3$. Тоді найбільший спільний дільник чисел $N_i + 1$ та $\prod_{j=0}^{i-1} N_j$ ділить їх різницю, яка рівна 3. Так як $N_0 = 3$, то маємо

$$\gcd\left(N_i + 1, \prod_{j=0}^{i-1} N_j\right) = 3.$$

Оскільки, згідно з лемою 6.3, числа N_j взаємно прості, то $\gcd(N_i + 1, N_j) = 1$ при $i \geq 2$ та $1 \leq j \leq i-1$. Лему доведено.

Лема 6.6. *Якщо* m_i *– найменше натуральне число з властивістю* $(c_i)^{m_i} \in K_{i-1}$, *то* $(c_i)^{m_i - 1} = u(c_i + 1)$, *де* $u \in K_{i-1}$.

Доведення. Виходячи з властивості числа m_i, маємо $(c_i)^{m_i - 1} = uc_i + v$, де $u, v \in F_2(c_{i-1})$ та $u \neq 0$. Тоді виконуються співвідношення $(c_i)^{m_i} = (uc_i + v)c_i = (u + v)c_i + ua_{i-1}$. Оскільки $(c_i)^{m_i} \in K_{i-1}$, то $u + v = 0$, тобто $u = v$. Лему доведено.

Лема 6.7. *Для* $i \geq 0$ *справедлива рівність* $(c_i)^{2^{2^i}} = c_i + 1$.

Доведення. Безпосередньо можна перевірити, що елемент $c_i + 1$, як і c_i, є коренем рівняння (6.1). Тоді елементи c_i та $c_i + 1$ спряжені над полем F_2. Відповідна група Галуа [1, 6] складається лише з двох автоморфізмів:

одиничного (тотожного) та автоморфізму, який полягає у піднесенні елементів до степеня 2^{2^i}. Виходячи з цього можемо записати, що $(c_i)^{2^{2^i}} = c_i + 1$. Лему доведено.

Лема 6.8. *Припустимо, що* $i \geq 0$. *Для* $k \geq 1$ *виконується наступне співвідношення:*

$$(c_i)^{2^k} = c_i + a_{i-1} + ... + (a_{i-1})^{2^{k-1}}.$$

Доведення. Індукцією за числом k. При $k = 1$ маємо правильну рівність (6.1). Якщо виконується рівність

$$(c_i)^{2^{k-1}} = c_i + a_{i-1} + ... + (a_{i-1})^{2^{k-2}},$$

то з неї виводимо наступні співідношення:

$$(c_i)^{2^k} = (c_i + a_{i-1} + ... + (a_{i-1})^{2^{k-2}})^2 = c_i^2 + a_{i-1}^2 + ... + (a_{i-1})^{2^{k-1}}.$$

Враховуючи в останній рівності вираз (6.1), отримуємо потрібний результат. Лему доведено.

Лема 6.9. *Для* $i \geq 1$ *виконується наступне співвідношення:*

$$a_{i-1} + ... + (a_{i-1})^{2^{2^{i-1}}-1} = 1.$$

Доведення. За лемою 6.8 маємо, що справедлива така рівність:

$$(c_i)^{2^{2^i}} = c_i + a_{i-1} + ... + (a_{i-1})^{2^{2^i}-1}.$$

З іншого боку, виходячи з леми 6.7, маємо рівність $(c_i)^{2^{2^i}} = c_i + 1$. Порівнюючи праві частини двох останнніх рівностей, отримуємо потрібний результат. Лему доведено.

Для довільного невід'ємного числа r та елемента $x \in K_{i-1}$ введемо позначення $S_r(x) = \sum_{j=0}^{r-1} x^{2^j}$. Записана сума послідовних квадратів елемента x аналогічна до поняття сліду [97, 102] елемента x. Наступна лема дає низку властивостей, якими володіє введена сума.

Лема 6.10. *Для довільних елементів x, t, u поля K_{i-1} справедливі наступні твердження:*

(a) *якщо* $r = h_1 + h_2$, *то* $S_r(x) = S_{h_1}(x) + S_{h_2}(x^{2^{h_1}})$;

(b) *якщо* $r = gw$, *то* $S_r(x) = \sum_{l=0}^{g-1} [S_w(x)]^{2^{wl}}$;

(c) *якщо* $r = gw + h$, *то* $S_r(x) = \sum_{l=0}^{g-1} [S_w(x)]^{2^{wl}} + S_h(x^{2^{gw}})$;

(d) *якщо елементи t і u спряжені над якимось підполем поля K_{i-1} та $S_r(t) = d \in F_2$, то $S_r(u) = d$.*

Доведення. (a) Твердження даного пункту отримуємо з таких співвідношень:

$$S_r(x) = S_{h_1+h_2}(x) = \sum_{j=0}^{h_1-1} x^{2^j} + \sum_{j=h_1}^{h_1+h_2} x^{2^j} = \sum_{j=0}^{h_1-1} x^{2^j} + \sum_{j=0}^{h_2} x^{2^{h_1}} = S_{h_1}(x) + S_{h_2}(x^{2^{h_1}}).$$

(b) Даний пункт доводимо, виписуючи такі співвідношення:

$$S_r(x) = S_{gw}(x) = \sum_{j=0}^{gw-1} x^{2^j} = \sum_{j=0}^{w-1} x^{2^j} + \ldots + \sum_{j=(g-1)w}^{gw-1} x^{2^j} = \sum_{j=0}^{w-1} x^{2^j} + \ldots + \left[\sum_{j=0}^{w-1} x^{2^j}\right]^{2^{w(g-1)}} =$$

$$= S_w(x) + \ldots + [S_w(x)]^{2^{w(g-1)}}$$

(c) Твердження цього пункту доводимо, застосовуючи пункт (a) та пункт (b) даної леми.

(d) Якщо елемент t задовольняє рівність $S_r(t) = d$ для $d \in F_2$, то, подіявши відповідним автоморфізмом G, отримаємо:

$$G(S_r(t)) = S_r(G(t)) = S_r(u) = G(d) = d\,.$$

Лему доведено.

Лема 6.11. *При* $i \geq 1$, *виконуються рівності*

$$(c_i)^{N_i} = a_{i-1} \tag{6.4}$$

та

$$(a_i)^{N_i} = (a_{i-1})^{N_i+1}. \tag{6.5}$$

Доведення. Покажемо спочатку, що рівність (6.4) справедлива. Дійсно, зауважимо, що c_i є коренем рівняння $x^2 + x + a_{i-1} = 0$ над полем L_{i-1}. Можна безпосередньо перевірити, що $c_i + 1$ також є коренем цього рівняння. Тоді елементи c_i та $c_i + 1$ є спряженими над полем $L_{i-1} = F_{2^{2^i}}$, тобто $(c_i)^{2^{2^i}} = c_i + 1$. Тоді можемо записати співвідношення

$$(c_i)^{2^{2^i}+1} = (c_i + 1)c_i = a_{i-1},$$

а, значить, рівність (6.4) виконується. Застосовуючи співідношення (6.4), отримуємо наступну рівність:

$$(a_i)^{N_i} = (c_i a_{i-1})^{N_i} = (a_{i-1})^{N_i+1}.$$

Отже, рівність (6.5) також справедлива. Лему доведено.

Якщо u_j – послідовність натуральних чисел та $s > t$, то розглядаємо далі порожній добуток $\prod_{j=s}^{t} u_j = 1$.

Лема 6.12. П*ри* $k \geq 0$, *справедливі наступні рівності:*

$$(c_i)^{\prod_{j=0}^{k} N_{i-j}} = (a_{i-k-1})^{\prod_{j=1}^{k} (N_{i-j}+1)} \tag{6.6}$$

та

$$(a_i)^{\prod_{j=0}^{k} N_{i-j}} = (a_{i-k-1})^{\prod_{j=0}^{k} (N_{i-j}+1)} \tag{6.7}$$

для $i > k$.

Доведення. Доведення виконаємо індукцією за k. При $k = 0$ (й при $i \geq 1$) маємо рівності (6.4) та (6.5).

Припустимо, що рівності (6.6) та (6.7) виконуються для $k-1$, тобто

$$(c_i)^{\prod_{j=0}^{k-1} N_{i-j}} = (a_{i-(k-1)-1})^{\prod_{j=1}^{k-1} (N_{i-j}+1)} \tag{6.8}$$

та

$$(a_i)^{\prod_{j=0}^{k-1} N_{i-j}} = (a_{i-(k-1)-1})^{\prod_{j=0}^{k-1} (N_{i-j}+1)}. \tag{6.9}$$

Покажемо спочатку, що рівність (6.6) справедлива й для k. Дійсно, застосовуючи (6.8) та (6.5), отримуємо

$$(c_i)^{\prod_{j=0}^{k} N_{i-j}} = \left((c_i)^{\prod_{j=0}^{k-1} N_{i-j}} \right)^{N_{i-k}} = \left((a_{i-k})^{N_{i-k}} \right)^{\prod_{j=1}^{k-1} (N_{i-j}+1)} = (a_{i-k-1})^{\prod_{j=1}^{k} (N_{i-j}+1)}.$$

Тепер покажемо, що рівність (6.7) також вірна для k. Дійсно, використовуючи співвідношення (6.9) та (6.5), маємо

$$(a_i)^{\prod_{j=0}^{k} N_{i-k}} = \left((a_i)^{\prod_{j=0}^{k-1} N_{i-k}} \right)^{N_{i-k}} = \left((a_{i-k})^{N_{i-k}} \right)^{\prod_{j=0}^{k-1} (N_{i-j}+1)} = (a_{i-k-1})^{\prod_{j=0}^{k} (N_{i-j}+1)}.$$

Лему доведено.

Лема 6.13. *Нехай* $K \subset L$ *– вежа полів. Нехай* $x \in L \setminus K$ *та* m *– найменше натуральне число, що задовольняє умову* $x^m \in K$. *Якщо* $x^n \in K$ *для деякого натурального числа* n, *то* m *ділить* n.

Доведення. Можна записати $n = um + v$, де $0 \le v < m$. Тоді $x^n = (x^m)^u \cdot x^v$, і, значить, $x^v = x^n[(x^m)^u]^{-1} \in K$. Так як m – найменше натуральне число з умовою $x^m \in K$ та $v < m$, то маємо $v = 0$, і отримуємо потрібний результат. Лему доведено.

Лема 6.14. *При* $u \ge 1$, *якщо* $(c_u)^l \in L_{u-1}$, *де* l – *натуральне число, то* $\gcd(l, N_u) > 1$.

Доведення. Рівність (6.4) дає $(c_u)^{N_u} = a_{u-1} \in L_{u-1}$. Згідно з лемою 6.13, якщо d найменше натуральне число з умовою $(c_u)^d \in L_{u-1}$, то d ділить число Ферма N_u та d ділить число l. Очевидно, що $d > 1$. Значить $\gcd(l, N_u) \ge d > 1$. Лему доведено.

Лема 6.15. *Нехай* $L_1 \subset L_2$ *вежа полів та* $b \in L_2^*$. *Нехай* $b^r = a \in L_1^*$ *та* r – *найменше натуральне число з умовою* $b^r \in L_1^*$. *Тоді* $\operatorname{ord} b = r \cdot \operatorname{ord} a$.

Доведення. Так як $b^{\operatorname{ord} b} = 1 \in L_1^*$, то маємо нерівність $\operatorname{ord} b \ge r$. Запишемо $\operatorname{ord} b = sr + t$, де $s \in N$ та $0 \le t < r$. Тоді виконується наступне співвідношення:

$$1 = b^{\operatorname{ord} b} = b^{sr+t} = a^s b^t .$$

Отже, $b^t = a^{-s} \in L_1^*$. За визначенням r, це можливо лише при $t = 0$. Маємо $a^s = 1$, $s \ge \operatorname{ord} a$ та $\operatorname{ord} b = sr \ge r \cdot \operatorname{ord} a$. З іншого боку, $b^{r \cdot \operatorname{ord} a} = a^{\operatorname{ord} a} = 1$, і, значить, $\operatorname{ord} b = r \cdot \operatorname{ord} a$. Лему доведено.

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* $i \geq 2$, $(c_i)^{\prod_{j=0}^{k} N_{i-j}} \in L_{i-k-1} \setminus L_{i-k-2}$ *для* $0 \leq k \leq i-1$.

Доведення. Застосовуючи рівність (6.6), отримуємо

$$(c_i)^{\prod_{j=0}^{k} N_{i-j}} = (c_{i-k-1})^{\prod_{j=1}^{k} (N_{i-j}+1)} (a_{i-k-2})^{\prod_{j=1}^{k} (N_{i-j}+1)}. \qquad (6.10)$$

Зрозуміло, що $(c_{i-k-1})^{\prod_{j=1}^{k} (N_{i-j}+1)} \in L_{i-k-1}$ та $(a_{i-k-2})^{\prod_{j=1}^{k} (N_{i-j}+1)} \in L_{i-k-2}$. Значить, добуток з правого боку рівності (6.10) належить до L_{i-k-1}. Для $1 \leq j \leq k$, згідно з лемою 6.5, $\gcd(N_{i-j}+1, N_{i-k-1}) = 1$ та $\gcd(\prod_{j=1}^{k} (N_{i-j}+1), N_{i-k-1}) = 1$. Тоді, за лемою 6.14, $(c_{i-k-1})^{\prod_{j=1}^{k} (N_{i-j}+1)} \notin L_{i-k-2}$. Отже, наступний елемент

$$(c_{i-k-1})^{\prod_{j=1}^{k} (N_{i-j}+1)} (a_{i-k-2})^{\prod_{j=1}^{k} (N_{i-j}+1)}$$

не належить до L_{i-k-2}. Теорему доведено.

Уведені раніше елементи a_i володіють властивістю, аналогічною до властивості елементів c_i і описаною в теоремі 6.1.

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

Доведення. Застосовуючи рівність (6.7), можемо записати таку рівність:

$$(a_i)^{\prod_{j=0}^{k} N_{i-j}} = (c_{i-k-1})^{\prod_{j=0}^{k} (N_{i-j}+1)} (a_{i-k-2})^{\prod_{j=0}^{k} (N_{i-j}+1)}. \qquad (6.11)$$

Зрозуміло. що $(c_{i-k-1})^{\prod_{j=0}^{k} (N_{i-j}+1)} \in L_{i-k-1}$ та $(a_{i-k-2})^{\prod_{j=0}^{k} (N_{i-j}+1)} \in L_{i-k-2}$. Значить, добуток з правого боку рівності (6.11) належить до L_{i-k-1}. Для $0 \le j \le k$, згідно з лемою 6.5, $\gcd(N_{i-j}+1, N_{i-k-1}) = 1$ та $\gcd(\prod_{j=0}^{k}(N_{i-j}+1), N_{i-k-1}) = 1$. Таким чином, за лемою 6.14, $(c_{i-k-1})^{\prod_{j=0}^{k} (N_{i-j}+1)} \notin L_{i-k-2}$. Отже, елемент

$$(c_{i-k-1})^{\prod_{j=0}^{k} (N_{i-j}+1)} (a_{i-k-2})^{\prod_{j=0}^{k} (N_{i-j}+1)}$$

не належить до L_{i-k-2}. Теорему доведено.

Використовуючи доведені в теоремі 6.1 та теоремі 6.2 властивості елементів c_i та a_i, в теоремі 6.3 отримано вирази для мультиплікативних порядків цих елементів.

Теорема 6.3. *При $i \ge 2$, справедливі наступні рівності:*

$$\text{(a) } \operatorname{ord} c_i = \prod_{j=1}^{i} \alpha_j, \text{ де } \alpha_j \mid N_j,\ \alpha_j > 1;$$

$$\text{(b) } \operatorname{ord} a_i = \prod_{j=1}^{i} \beta_j, \text{ де } \beta_j \mid N_j,\ \beta_j > 1.$$

Доведення. (a) Означимо рекурсивно послідовність натуральних чисел $\alpha_i, ..., \alpha_{1i}$ таким чином. Число α_i є найменшим натуральним числом, яке задовольняє умову $(c_i)^{\alpha_i} \in L_{i-1}$. Якщо $\alpha_i, \ldots, \alpha_{i-j}$, де $0 \le j \le i-2$, вже задані, то α_{i-j-1} – найменше натуральне число з умовою

$$\{(c_i)^{\prod_{k=i-j}^{i}\alpha_k}\}^{\alpha_{i-j-1}} \in L_{i-j-2}.$$

Оскільки потужність групи L_i^* дорівнює $\prod_{j=0}^{i} N_j$, а потужність групи L_{i-1}^* дорівнює $\prod_{j=0}^{i-1} N_j$, то маємо, що кількість елементів фактор-групи L_i^* / L_{i-1}^* рівна N_i. Якщо d є класом елемента c_i у фактор-групі, то $\alpha_i = \operatorname{ord} d$ і, як наслідок теореми Лагранжа для скінченних груп, число α_i ділить N_i. Очевидно, що $\alpha_i > 1$. Справедливе включення $(c_i)^{\alpha_i} \in L_{i-1} \setminus L_{i-2}$, бо згідно з теоремою 6.1 $(c_i)^{N_i} \in L_{i-1} \setminus L_{i-2}$. Дійсно, якщо припустити $(c_i)^{\alpha_i} \in L_{i-2}$, то $[(c_i)^{\alpha_i}]^{N_i/\alpha_i} = (c_i)^{N_i} \in L_{i-2}$ - суперечність. Згідно з лемою 6.15, $\operatorname{ord} c_i = \alpha_i \operatorname{ord} (c_i)^{\alpha_i}$.

Аналогічно до попереднього, можна показати у випадку знаходження α_{i-j-1}, що $\alpha_{i-j-1} \mid N_{i-j-1}$ $(\alpha_{i-j-1} > 1)$ та виконується включення

$$\{(c_i)^{\prod_{k=i-j}^{i}\alpha_{i-k}}\}^{\alpha_{i-j-1}} \in L_{i-j-2} \setminus L_{i-j-3}.$$

Відповідно до леми 6.15, маємо таку рівність для порядків:

$$\operatorname{ord} (c_i)^{\alpha_i \ldots \alpha_{i-j}} = \alpha_{i-j-1} \operatorname{ord} (c_i)^{\alpha_i \ldots \alpha_{i-j}\alpha_{i-j-1}}.$$

Оскільки, згідно з (6.6), виконується наступне співвідношення:

$$(c_i)^{\prod_{j=0}^{i-1} N_{i-j}} = ((a_0)^{N_1+1})^{\prod_{j=1}^{i-2}(N_{i-j}+1)} = 1,$$

то отримуємо $\operatorname{ord} c_i \mid \prod_{j=0}^{i-1} N_{i-j}$, та $\operatorname{ord} c_i = \alpha_i \ldots \alpha_1$.

(b) Доведення аналогічне до попереднього пункту, але використовуючи теорему 6.2 замість теореми 6.1.

Теорему доведено.

Наслідок 6.1. *При* $i \geq 2$, $\operatorname{ord}(c_i c_0) = N_0 \cdot \operatorname{ord} c_i$ *та* $\operatorname{ord}(a_i a_0) = N_0 \cdot \operatorname{ord} a_i$.

Доведення. Зауважимо, що $\operatorname{ord} c_0 = N_0$. Оскільки, відповідно до теореми 6.3, $\operatorname{ord} c_i$ ділить $\prod_{j=1}^{i} N_j$, а лема 6.3 дає $\gcd(\prod_{j=1}^{i} N_j, N_0) = 1$, то маємо $\gcd(\operatorname{ord} c_i, \operatorname{ord} c_0) = 1$. Тоді $\operatorname{ord}(c_i c_0) = \operatorname{ord} c_i \cdot \operatorname{ord} c_0$, і отримуємо бажаний результат для елемента $c_i c_0$. Доведення для елемента $a_i a_0 = a_i c_0$ аналогічне. Наслідок доведено.

У теоремі 6.4 описано певне обмеження на порядок елементів c_i у фактор-групі K_i / K_{i-1}.

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 $k = 2^i$.

Доведення. Методом від протилежного. Припустимо, що m_i – найменше натуральне число з властивістю $(c_i)^{m_i} \in K_{i-1}$, $m_i = 2^k + 1$ та $k < 2^i$. Тоді $(c_i)^{2^k+1} \in K_{i-1}$, і за лемою 6.6 $(c_i)^{2^k+1} = u(c_i + 1)$, де $u \in K_{i-1}$. Оскільки за лемою 6.8 справедлива рівність

$$(c_i)^{2^k} = c_i + a_{i-1} + \ldots + (a_{i-1})^{2^{k-1}},$$

то

$$S_k(a_{i-1}) = a_{i-1} + \ldots + (a_{i-1})^{2^{k-1}} = 1. \qquad (6.12)$$

Разом з тим за лемою 6.9 маємо таке співвідношення:

$$S_{2^i}(a_{i-1}) = a_{i-1} + \ldots + (a_{i-1})^{2^{2^i-1}} = 1. \qquad (6.13)$$

Далі рекурсивно будуємо для $j \geq 1$ елементи $S_{k_j}(a_{i-1}) \in F_2$. При $j = 1$ беремо $k_1 = k$, тобто $S_{k_1}(a_{i-1}) = S_k(a_{i-1}) = 1 \in F_2$.

Якщо $S_{k_j}(a_{i-1})$ відоме, то виконуємо таке. Зауважимо, що $S_k(a_{i-1})$ з рівності (6.12) має k доданків, а $S_{2^i}(a_{i-1})$ з рівності (6.13) має 2^i доданків. Виконуємо ділення $2^i = g_j k_j + h_j$, де $0 \leq h_j < k_j$. Якщо $h_j = 0$, то g_j - парне, і за лемою 6.10, пункт (c) виконуються наступні співвідношення:

$$1 = S_{2^i}(a_{i-1}) = \sum_{m=0}^{g_j - 1} [S_{k_j}(a_{i-1})]^{2^m} = g_j S_{k_j}(a_{i-1}) = 0.$$

Отримали суперечність. Під час перетворення останньої рівності скористалися таким фактом: оскільки $S_{k_j}(a_{i-1}) \in F_2$, то $[S_{k_j}(a_{i-1})]^{2^m} = S_{k_j}(a_{i-1})$ для $m = 0,..., g_j - 1$. Отже, $h_j > 0$ і, за лемою 6.10, пункт (c), виконується така рівність:

$$S_{2^i}(a_{i-1}) = g_j S_{k_j}(a_{i-1}) + S_{h_j}((a_{i-1})^{2^{g_j k_j}}).$$

Тоді справедливі наступні співвідношення:

$$S_{h_j}((a_{i-1})^{2^{g_j k_j}}) = 1 + g_j S_{k_j}(a_{i-1}) \in F_2.$$

Покладаємо $k_{j+1} = h_j$. Зрозуміло, що $k_j > k_{j+1}$. Оскільки елементи a_{i-1} та $(a_{i-1})^{2^{g_j k_j}}$ спряжені над підполем поля K_{i-1}, то за лемою 6.10, пункт (d), отримуємо, що

$$S_{h_j}(a_{i-1}) = S_{h_j}((a_{i-1})^{2^{g_j k_j}}) \in F_2.$$

Так як послідовність чисел $k_1 > k_2 > \ldots$ строго спадальна, то за скінченну кількість кроків отримаємо $k_r = 0$ та $S_{k_r}(a_{i-1}) = S_0(a_{i-1}) = a_{i-1} \in F_2$ – суперечність. Теорему доведено.

На підставі теореми 6.4, в наслідку 6.2 наводимо нижню межу для мультиплікативного порядку розглянутих раніше елементів c_i, a_i 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 $1 \le i \le 4$ та має значення принаймні $\prod_{j=1}^{4} N_j \cdot \prod_{j=5}^{i} (3 \cdot 2^{j+2} + 1)$ для $i \ge 5$.

Доведення. Розглянемо вирази для мультиплікативних порядків елементів c_i та a_i, які наведені в теоремі 6.3. Як було сказано раніше, для $1 \le j \le 4$ числа Ферма $N_1 = 5$, $N_2 = 17$, $N_3 = 257$, $N_4 = 65537$ є простими. Тому, $\alpha_j = \beta_j = N_j$ для $1 \le j \le 4$.

Покажемо тепер, що для $j \ge 5$ справедлива нерівність $\alpha_j, \beta_j \ge 3 \cdot 2^{j+2} + 1$. Згідно з лемою 6.13, α_j та β_j ділить N_j. Виходячи з леми 6.4, $\alpha_j = s \cdot 2^{j+2} + 1$ та $\beta_j = s \cdot 2^{j+2} + 1$, де s – натуральне число. За теоремою 6.4, число s не може дорівнювати 1 або 2, тобто $s \ge 3$. Наслідок доведено.

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

6.2. Деякі примітивні елементи у вежах Конвея

У даному підрозділі формулюємо в наслідку 6.3 умову, при якій розглянуті в підрозділі 6.1 елементи є примітивними. Також 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:*

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

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

Доведення. Для елемента a_i доведення виконуємо індукцією за $i \geq 5$. Зауважимо, що α_j – найменше натуральне число з умовою $(c_j)^{\alpha_j} \in L_{j-1}$ тоді і тільки тоді, коли α_j – найменше натуральне число з умовою $(a_j)^{\alpha_j} \in L_{j-1}$.

Для $i = 5$ отримуємо з рівності (6.5), що $(a_5)^{N_5} = (a_4)^{N_5+1}$. Тоді, згідно з лемою 6.15, $\operatorname{ord} a_5 = N_5 \operatorname{ord} (a_4)^{N_5+1}$. Маємо $\operatorname{ord} a_4 = \prod_{j=1}^{4} N_j$ за наслідком 6.2 та $(N_5 + 1, \prod_{j=1}^{4} N_j) = 1$ за лемою 6.5. Тепер використаємо загально відомий факт, що піднесення елемента групи до степеня, який взаємно простий з порядком групи, не змінює порядку елемента. Отримуємо $\operatorname{ord} (a_4)^{N_5+1} = \operatorname{ord} a_4$ та $\operatorname{ord} a_5 = \prod_{j=1}^{5} N_j$.

Припустимо, що твердження теореми вірне для $i-1$. Для i маємо з рівності (6.5) $(a_i)^{N_i} = (a_{i-1})^{N_i+1}$. Тоді, застосовуючи лему 6.15, отримуємо $\operatorname{ord} a_i = N_i \operatorname{ord} (a_{i-1})^{N_i+1}$. Так як $\operatorname{ord} a_{i-1} = \prod_{j=1}^{i-1} N_j$ за припущенням індукції й $(N_i + 1, \prod_{j=1}^{i-1} N_j) = 1$ за лемою 6.5, то отримуємо, аналогічно до попереднього, $\operatorname{ord} (a_{i-1})^{N_i+1} = \operatorname{ord} a_{i-1}$ та $\operatorname{ord} a_i = \prod_{j=1}^{i} N_j$.

Для завершення доведення зауважимо, що, згідно з рівністю (6.4) та лемою 6.15, $\text{ord}\, c_i = N_i \text{ord}\, a_{i-1} = \text{ord}\, a_i$. Теорему доведено.

Зауважимо, що, коли умова теореми 6.5 виконується, то маємо наступний ланцюг циклічних підгруп:

$$\langle c_i \rangle = \langle a_i \rangle \supset \langle c_{i-1} \rangle = \langle a_{i-1} \rangle \supset \ldots \supset \langle c_2 \rangle = \langle a_2 \rangle \supset \langle a_1 \rangle .$$

Разом з тим $\langle a_1 \rangle \neq \langle c_1 \rangle$, бо $\text{ord}\, c_1 = 15$, $\text{ord}\, a_1 = \text{ord}\,(c_1 c_0) = 5$.

Як наслідок теореми 6.5 та наслідку 6.1, отримуємо наслідок 6.3. Він 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:* $\alpha_j = N_j$ *є найменшим натуральним число, що задовольняє умову* $(c_j)^{\alpha_j} \in L_{j-1}$, то елемент $c_i c_0$ та елемент $a_i a_0$ є примітивними.

Доведення. Оскільки $\text{ord}\,(c_i c_0) = \text{ord}\,(a_i a_0) = \prod_{j=0}^{i} N_j$, то отримуємо потрібний результат. Наслідок доведено.

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* $5 \leq j \leq 11$, *число* $\alpha_j = N_j$ *є найменшим натуральним числом з умовою* $(c_j)^{\alpha_j} \in L_{j-1}$.

Доведення. Для $5 \leq j \leq 11$, числа Ферма повністю розкладені на прості множники [64]. Відповідні розклади та пов'язані з ними результати перевірки

з використанням комп'ютерних обчислень наведені далі. Зауважимо, що для доведення факту: N_j найменше натуральне число з умовою $(c_j)^{\alpha_j} \in L_{j-1}$, достатньо перевірити $c_j^{N_j/p} \notin L_{j-1}$ для кожного простого дільника p числа N_j. Дійсно, якщо елемент c_j у степені N_j / p не належить до L_{j-1}, то елемент c_j у степені якогось дільника $N_j /(pq)$ числа N_j / p також не належить до L_{j-1}.

Для $j = 5$, маємо такий розклад на прості множники: $N_5 = 641 \cdot 6700417$. Згідно з рівністю (6.4), виконується співвідношення $(c_5)^{N_5} = c_4 c_3 c_2 c_1 c_0 \in L_4$. Ми перевірили з використанням комп'ютерних обчислень, що $\alpha_5 = N_5$ є найменшим натуральним числом, яке задовольняє умову $(c_5)^{\alpha_5} \in L_4$.

Для $j = 6$, маємо такий розклад

$$N_6 = 274177 \cdot 67280421310721.$$

Згідно з рівністю (6.4), справедливе співвідношення $(c_6)^{N_6} = c_5 c_4 c_3 c_2 c_1 c_0 \in L_5$. Ми перевірили, що $\alpha_6 = N_6$ є найменшим натуральним числом, яке задовольняє умову $(c_6)^{\alpha_6} \in L_5$.

Для $j = 7$ маємо наступний розклад:

$$N_7 = 59649589127497217 \cdot 5704689200685129054721.$$

Згідно з рівністю (6.4), можемо записати $(c_7)^{N_7} = c_6 c_5 c_4 c_3 c_2 c_1 c_0 \in L_6$. Ми перевірили, що $\alpha_7 = N_7$ є найменшим натуральним числом, яке задовольняє умову $(c_7)^{\alpha_7} \in L_6$.

Для $j = 8$, маємо такий розклад $N_8 = 1238926361552897 \cdot \mathrm{P}_{62}$, де P_{62} просте число з 62 десятковими розрядами:

P_{62}=93461639715357977769163558199606896584051237541638188580280321.

Згідно з рівністю (6.4), виконується співвідношення $(c_8)^{N_8} = c_7c_6c_5c_4c_3c_2c_1c_0 \in L_7$. Ми перевірили, що $\alpha_8 = N_8$ є найменшим натуральним числом, яке задовольняє умову $(c_8)^{\alpha_8} \in L_7$.

Для $j = 9$, маємо такий розклад:

$$N_9 = 2424833 \cdot 7455602825647884208337395736200454918783366342657 \cdot \mathrm{P}_{99},$$

де P_{99} – просте число з 99 десятковими розрядами:

P_{99}=741640062627530801524787141901937474059940781097519023905821316144415759504705008092818711693940737.

Згідно з рівністю (6.4), можна записати $(c_9)^{N_9} = c_8c_7c_6c_5c_4c_3c_2c_1c_0 \in L_8$. Ми перевірили, що $\alpha_9 = N_9$ є найменшим натуральним числом, яке задовольняє умову $(c_9)^{\alpha_9} \in L_8$.

Для $j = 10$, маємо такий розклад:

$$N_{10} = 45592577 \cdot 6487031809 \cdot 4659775785220018543264560743076778192897 \cdot \mathrm{P}_{252}$$

де P_{252} просте число з 252 десятковими розрядами:

P_{252}=130439874405488189727484768796509903946608530841611892186895295776832416251471863574140227977573104895898783928842923844831149032913798729088601617946094119449010595906710130531906171018354491609619193912488538116080712299672322806217820753127014424577.

Згідно з рівністю (6.4), можемо записати $(c_{10})^{N_{10}} = c_9c_8c_7c_6c_5c_4c_3c_2c_1c_0 \in L_9$. Ми перевірили, що $\alpha_{10} = N_{10}$ є найменшим натуральним числом, яке задовольняє умову $(c_{10})^{\alpha_{10}} \in L_9$.

Для $j = 11$, маємо такий розклад:

$$N_{11} = 319489 \cdot 974849 \cdot 167988556341760475137 \cdot 3560841906445833920513 \cdot \mathrm{P}_{564}$$

де P_{564} – просте число з 564 десятковими розрядами:

P_{564}=173462447179147555430258970864309778377421844723664084649347019061363579192879108857591038330408837177983810868451546421940712978306134189864280826014542758708589243873685563973118948869399158545506611147420216132557017260564139394366945793220968665108959685482705388072645828554151936401912464931182546092879815733057795573358504982279280090942872567591518912118622751714319229788100979251036035496917279912663527358783236647193154777091427745377038294584918917590325110939381322486044298573971650711059244462177542540706913047034664643603491382441723306598834177.

Згідно з рівністю (6.4), $(c_{11})^{N_{11}} = c_{10}c_9c_8c_7c_6c_5c_4c_3c_2c_1c_0 \in L_{10}$. Ми перевірили, що $\alpha_{11} = N_{11}$ є найменшим натуральним числом, яке задовольняє умову $(c_{11})^{\alpha_{11}} \in L_{10}$. Теорему доведено.

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_ic_0 та a_ia_0, є примітивними.

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

Доведення. Результат у випадку $2 \le i \le 4$ випливає з наслідку 6.2. Результат у випадку $5 \le i \le 11$ випливає з теореми 6.5 та теореми 6.6. Наслідок доведено.

Виходячи з наслідку 6.1 та наслідку 6.4, отримуємо такий наслідок.

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 у наслідку 6.5 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.

Приклад 6.3. Розглянемо на закінчення підрозділу наступний приклад, пов'язаний з мультиплікативною групою поля L_2. Маємо у даному випадку $\operatorname{ord} c_2 = 5 \cdot 17 = 85$. Елемент $c_2 c_0$ є примітивним для цього поля, тобто $\operatorname{ord} (c_2 c_0) = 3 \cdot 5 \cdot 17 = 255$. Візьмемо також елемент $c_2 + c_1 + 1$. Оскільки $c_2 + c_1 + 1 = (c_2)^5$, то отримуємо $\operatorname{ord} (c_2 + (c_1 + 1)) = 17$.

6.3. Нижня межа для порядку у вежах Відемана

У даному підрозділі розглядаються рекурсивні двійкові розширення скінченних полів $E_{i+1} = E_i(x_{i+1})$, $i \ge -1$, визначені Відеманом. Основна мета підрозділу – описати деякі власні дільники чисел Ферма N_i, які не дорівнюють мультиплікативному порядку $\operatorname{ord} x_i$.

Ми даємо обмеження та, як наслідок, нижню межу для мультиплікативного порядку деяких елементів у двійкових рекурсивних розширеннях скінченних полів, визначених Відеманом [150]. Даний підрозділ пов'язаний з відкритим питанням, поставленим Відеманом [103 (проблема 28), 150]. Волох [144] дав першу нетривіальну оцінку порядку елементів у цій конструкції, а саме $\exp(2^{2^i \delta})$, де δ – абсолютна константа.

Проте, значення цієї константи невідоме. Наша межа не залежить ні від якої невідомої константи.

Більш точно, розглядаємо наступні скінченні поля, визначені Відеманом, які будуються рекурсивно:

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

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

$$x_{i+1}^2 + x_{i+1}x_i + 1 = 0. \qquad (6.14)$$

Зауважимо, що наведений поліном є нерозкладним над полем E_i згідно з [150, теорема 1]. Таким чином, ми отримуємо наступну вежу скінченних полів характеристики два:

$$F_2 \subset E_0 = F_2(x_0) \subset E_1 = E_0(x_1) \subset ...$$

Для порівняння, аналогічну вежу скінченних полів, визначену Конвеєм, розглянуто в підрозділах 6.1 та 6.2.

Зауважимо, що кількість елементів мультиплікативної групи E_i^* ($i \geq 0$), тобто число ненульових елементів поля E_i, як і у випадку веж Конвея дорівнює $2^{2^{i+1}} - 1$. З використанням чисел Ферма, потужність множини E_i^* ($i \geq 0$) дорівнює $2^{2^{i+1}} - 1 = \prod_{j=0}^{i} N_j$. Наприклад, маємо для перших трьох полів:

$$\left|E_0^*\right| = 2^{2^1} - 1 = 3,$$

$$\left|E_1^*\right| = 2^{2^2} - 1 = 15 = 3 \cdot 5,$$

$$\left|E_2^*\right| = 2^{2^3} - 1 = 255 = 3 \cdot 5 \cdot 17.$$

Далі даємо в лемах допоміжні для даного підрозділу результати.

Лема 6.16. [150] *При* $i \geq 0$*, виконується наступна рівність:* $(x_i)^{N_i} = 1$.

Згідно з теоремою Лагранжа для скінченних груп [1, 6], з леми 6.16 випливає, що порядок елемента x_i ділить N_i. У випадку, коли N_i – просте число, x_i має порядок, що точно дорівнює N_i. Відкрите питання, поставлене Відеманом [103 (проблема 28), 150], полягає в такому: чи мультиплікативний порядок $\operatorname{ord} x_i$ елемента x_i завжди дорівнює N_i. У будь-якому випадку, порядок елемента x_i ділить число Ферма N_i.

Лема 6.17. *Нехай* $u_r = \prod_{i=0}^{r} x_i$ *для* $r = 0,1....$ *Тоді мультиплікативний порядок елемента* u_r *дорівнює* $\operatorname{ord} u_r = \prod_{i=0}^{r} \operatorname{ord} x_i$.

Доведення. Оскільки числа Ферма є попарно взаємно простими (див. лему 6.3), то порядок елемента $u_r = \prod_{i=0}^{r} x_i$ є добутком порядків елементів x_i, $0 \leq i \leq r$. Число елементів мультиплікативної групи E_i^* $(i = 0,1,...)$ дорівнює $\prod_{j=0}^{i} N_j$. Як наслідок леми 6.16 маємо, що група E_i^* $(i = 0,1,...)$ є внутрішнім прямим добутком підгруп з N_j $(j = 0,...,i)$ елементів. Елемент x_i належить до підгрупи порядку N_i. Лему доведено.

Якщо порядок елемента x_i є, дійсно, N_i для $0 \leq i \leq r$, то $u_r = \prod_{i=0}^{r} x_i$ є примітивним елементом у E_r, бо $2^{2^{i+1}} - 1 = \prod_{j=0}^{i} N_j$. Отже, наведене раніше питання Відемана можна переформулювати таким чином: чи є елемент $u_r = \prod_{i=0}^{r} x_i$ примітивним.

Лема 6.18. *Нехай* K *– скінченне поле характеристики два та* $x, y \in K$. *Якщо*

$$y^2 = yx + 1, \tag{6.15}$$

то

$$y^{2^k} = yx^{2^k-1} + \sum_{j=1}^{k} x^{2^k-2^j}. \tag{6.16}$$

для будь-якого натурального числа k.

Доведення. Індукцією за k. При $k = 1$ отримуємо рівність (6.15).

Припустимо, що рівність (6.16) виконується для деякого натурального числа k. Тоді

$$y^{2^{k+1}} = \left(y^{2^k}\right)^2 = \left(yx^{2^k-1} + \sum_{j=1}^{k} x^{2^k-2^j} \right)^2 = y^2 x^{2^{k+1}-2} + \sum_{j=1}^{k} x^{2^{k+1}-2^{j+1}}.$$

Враховуючи (6.15), маємо

$$y^{2^{k+1}} = yx^{2^{k+1}-1} + \sum_{j=1}^{k+1} x^{2^{k+1}-2^j},$$

тобто рівність (6.16) вірна також і для $k+1$. Лему доведено.

Лема 6.19. *Мультиплікативний порядок* $\operatorname{ord} x_i = N_i$ *для* $0 \le i \le 11$.

Доведення. Для $0 \le i \le 4$ числа Ферма є простими [64]: $N_0 = 3$, $N_1 = 5$, $N_2 = 17$, $N_3 = 257$, $N_4 = 65537$. Тому очевидно для цих чисел, як наслідок леми 6.16, що порядок елемента x_i співпадає з відповідним числом Ферма, тобто $\operatorname{ord} x_i = N_i$.

Решта доведення використовує комп'ютерні обчислення. Ми виконуємо обчислення порядку елемента x_i для $5 \le i \le 11$. У цьому разі числа

Ферма повністю розкладені на прості множники [64]. Відповідні розклади наведені при доведенні теореми 6.6.

Використовуючи вказані розклади, обчислюємо x_i у степені N_i / q для кожного простого дільника q числа N_i. Дійсно, якщо елемент в степені N_i / q не дорівнює одиниці, то цей елемент у степені будь-якого дільника числа N_i / q також не дорівнює одиниці. У результаті отримуємо, що для $5 \le i \le 11$ порядок x_i не менший від N_i, а саме точно дорівнює N_i. Лему доведено.

Лема 6.20. *При* $i \ge 0$ *обернений до елемента* x_i *дорівнює* $(x_i)^{-1} = x_i + x_{i-1}$.

Доведення. Спираючись на наведене раніше рекурсивне рівняння (6.1), яке визначає вежу Відемана, маємо $x_i(x_i + x_{i-1}) = (x_i)^2 + x_i x_{i-1} = 1$. Значить, елемент x_i є оберненим до елемента $x_i + x_{i-1}$. Лему доведено.

Лема 6.21. *Для* $i \ge 1$ *виконуються наступні рівності:*

$$x_i^2 = x_i x_{i-1} + 1, \tag{6.17}$$

$$x_i^3 = x_{i-1}(x_{i-2} x_i + 1) \tag{6.18}$$

$$x_i^5 = x_{i-1}[(x_{i-2}^2 + 1)x_{i-1} x_i + x_{i-2} x_{i-1} + 1]. \tag{6.19}$$

Доведення Рівність (6.17) випливає безпосередньо з рівності (6.1). Застосовуючи рівність (6.17) до елемента x_i^2 послідовно два рази, отримуємо наступні співвідношення:

$$x_i^3 = x_i^2 \cdot x_i = x_{i-1} x_i^2 + x_i = x_{i-1}^2 x_i + x_{i-1} + x_i .$$

Підстановка тепер значення x_{i-1}^2 із (6.17), приводить до (6.18). Використовуючи (6.17) та (6.18), маємо

$$x_i^5 = x_i^3 \cdot x_i^2 = x_{i-1}(x_{i-2}x_i + 1)(x_{i-1}x_i + 1) = x_{i-1}(x_{i-2}x_{i-1}x_i^2 + x_{i-2}x_i + x_{i-1}x_i + 1) =$$
$$= x_{i-1}(x_{i-1}^2 x_{i-2}x_i + x_{i-2}x_{i-1} + x_{i-2}x_i + x_{i-1}x_i + 1).$$

Підставляння тепер значення величини x_{i-1}^2 із (6.17), дає рівність (6.19). Лему доведено.

Далі даємо в теоремах 6.7-6.9 та наслідку 6.6 основні результати даного підрозділу. При цьому доводимо твердження (теорема 6.7 та теорема 6.8), 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* $\operatorname{ord} x_i$ $(i \geq 0)$ *не може бути дільником числа вигляду* $2^k + 1$, *де* k *натуральне число та* $k < 2^i$.

Доведення. Доведення виконуємо індукцією за i. Для $0 \leq i \leq 11$ твердження справедливе згідно з лемою 6.19. Нехай твердження виконується для чисел від 12 до $i-1$.

Покажемо методом від протилежного, що твердження також виконується для i. Припустимо, що $\operatorname{ord} x_i$ ділить $2^k + 1$, де $k < 2^i$. Тоді $(x_i)^{2^k+1} = 1$ і з леми 6.20 випливає

$$(x_i)^{2^k} = (x_i)^{-1} = x_i + x_{i-1}. \tag{6.20}$$

З іншого боку, покладаючи в (6.16) $y = x_i$, $x = x_{i-1}$, маємо

$$(x_i)^{2^k} = x_i (x_{i-1})^{2^k - 1} + \sum_{j=1}^{k} (x_{i-1})^{2^k - 2^j}. \tag{6.21}$$

Порівнюючи коефіцієнти біля x_i в рівностях (6.20) та (6.21), отримуємо $(x_{i-1})^{2^k-1}=1$. Таким чином, ord x_{i-1} ділить число 2^k-1. Разом з тим, за лемою 6.16, ord x_{i-1} є дільником числа $2^{2^{i-1}}+1$. Тоді ord x_{i-1} ділить суму чисел $2^{2^{i-1}}+1$ та 2^k-1, яка дорівнює $S=2^{2^{i-1}}+2^k$. Розглянемо три можливих випадки.

1) Якщо $k=2^{i-1}$, то $S=2^{2^{i-1}}+2^{2^{i-1}}=2^{2^{i-1}+1}$. У цьому разі ord x_{i-1} дорівнює степеню двійки. Це суперечить факту, що порядок ord x_{i-1} повинен ділити число $2^{2^{i-1}}+1$.

2) Якщо $k<2^{i-1}$, то $S=2^k(2^{2^{i-1}-k}+1)$. Так як 2^k є взаємно простим з $2^{2^{i-1}}+1$, то порядок ord x_{i-1} ділить $2^{2^{i-1}-k}+1$. Оскільки $k\geq 1$, то виконується нерівність $2^{i-1}-k<2^{i-1}$ – суперечність з припущенням індукції.

3) Якщо $k>2^{i-1}$, то $S=2^{2^{i-1}}(2^{k-2^{i-1}}+1)$. Так як $2^{2^{i-1}}$ взаємно просте з $2^{k-2^{i-1}}+1$, то ord x_{i-1} є дільником $2^{k-2^{i-1}}+1$. Оскільки $k<2^i$, то справедлива нерівність $k-2^{i-1}<2^{i-1}$ – суперечність з припущенням індукції.

Таким чином, ми отримали суперечність у всіх трьох можливих випадках, а це показує, що твердження виконується також і для числа i. Значить, твердження теореми справедливе для будь-якого цілого числа $i\geq 0$. Теорему доведено.

Теорема 6.8. *Порядок* 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.*

Доведення. Виконуємо методом від протилежного. Якщо ord x_i є дільником числа вигляду $s\cdot 2^k+1$, то $(x_i)^{s\cdot 2^k+1}=1$ і очевидно

$$(x_i)^{s\cdot 2^k}=(x_i)^{-1}. \qquad (6.22)$$

Введемо позначення $t = 2^i - k$. Тоді $2^{2^i} = 2^t \cdot 2^k$. Підносячи ліву та праву частини рівності (6.22) до степеня 2^t та беручи до уваги, що $(x_i)^{2^{2^i}} = (x_i)^{-1}$, отримуємо

$$(x_i)^{2^t} = (x_i)^s.$$

Розглянемо випадок $s = 3$. Згідно з лемою 6.18, справедлива рівність:

$$(x_i)^{2^t} = x_i (x_{i-1})^{2^t - 1} + \sum_{j=1}^{t} (x_{i-1})^{2^t - 2^j}. \qquad (6.23)$$

Порівнюючи коефіцієнти біля x_i з правого боку рівності (6.23) та рівності (6.18), отримуємо

$$(x_{i-1})^{2^t - 2} = x_{i-2}.$$

Оскільки $x_{i-2} \neq 1$ та, за лемою 6.3, числа Ферма є попарно взаємно простими, то отримуємо $\langle x_{i-1} \rangle \cap \langle x_{i-2} \rangle = 1$ – суперечність. Як наслідок, ord x_i $(i \geq 0)$ не може бути дільником числа вигляду $3 \cdot 2^k + 1$, де k – невід'ємне ціле число.

Розглянемо тепер випадок $s = 5$. Порівнюючи коефіцієнти біля елемента x_i з правого боку рівності (6.23) та рівності (6.19), маємо

$$(x_{i-1})^{2^t - 3} = (x_{i-2})^2 + 1.$$

Оскільки $(x_{i-2})^2 + 1 = x_{i-2} x_{i-3} \neq 0$, то можна записати $(x_{i-2})^2 + 1 \in [F_2(x_{i-2})]^*$. Зауважимо, що $(x_{i-2})^2 + 1 \neq 1$, бо $(x_{i-2})^2 \neq 0$. Той факт, що N_{i-1} взаємно просте з $N_{i-2} N_{i-3}$ (див. лему 6.3), веде до $\langle x_{i-1} \rangle \cap [F_2(x_{i-2})]^* \neq 1$ – суперечність. З цієї причини, ord x_i $(i \geq 0)$ не може бути дільником числа вигляду $5 \cdot 2^k + 1$, де k – невід'ємне ціле число. Теорему доведено.

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 $0 \le i \le 11$ мультиплікативний порядок $\operatorname{ord} x_i = N_i$, тобто є максимально можливим.

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

Доведення. За лемою 6.19, рівність $\operatorname{ord} x_i = N_i$ виконується для $0 \le i \le 11$. Покажемо тепер, що для $i \ge 12$ справедлива нерівність $\operatorname{ord} x_i \ge 7 \cdot 2^{i+2} + 1$. Якщо $(x_i)^{n_i} = 1$, то, як наслідок теореми Лагранжа для скінченних груп, n_i ділить N_i. Згідно з лемою 6.4, $n_i = s \cdot 2^{i+2} + 1$, де s – натуральне число. За теоремою 6.7, число s не може дорівнювати 1, 2 або 4, а за теоремою 6.8 число s не може дорівнювати 3, 5 або 6, тобто $s \ge 7$. Таким чином, отримуємо потрібний результат. Теорему доведено.

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

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

Доведення. Відповідно до леми 6.17, маємо рівність $\operatorname{ord} u = \prod_{i=0}^{r} \operatorname{ord} x_i$. Застосовуючи тепер теорему 6.9, отримуємо наведені в формулюванні даного наслідку межі для порядку елемента $u = \prod_{i=0}^{r} x_i$. Наслідок доведено.

Отримана в наслідку 6.6 нижня межа не залежить ні від якої невідомої константи.

6.4. Нижня межа для порядку елементів у вежах скінченних полів недвійкової характеристики

У даному 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 в [86, 87] 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 нступне рівняння:

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

Нагадаємо, що поліном $x_1^p - x_1 - 1 = 0$ є нерозкладним над полем F_p (див. підрозділ 5.1). Також зауважимо, що наведений поліном $x_r^p - x_r - \prod_{i=0}^{r-1} x_i^{p-1}$ є нерозкладним над полем E_r, виходячи з леми 6.1. У даному випадку, $\alpha = \prod_{i=-1}^{r-2} x_i$, $\beta = x_{r-1}$. Тобто, у результаті отримуємо таку вежу скінченних полів недвійкової характеристики:

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

З точки зору прикладних застосувань такі побудови викликають суттєвий інтерес, оскільки операції над елементами скінченого поля можна виконувати рекурсивно, а тому ефективно [86, 87].

Зауважимо, що число елементів мультиплікативної групи E_r^* $(r = 1,2,\ldots)$ дорівнює $p^{p^r} - 1$. Наприклад, при $p = 3$ маємо

$\left|E_0^*\right| = 3^{3^1} - 1 = 26$,

$\left|E_1^*\right| = 3^{3^2} - 1 = 19682 = 26 \cdot 757$.

Для довільних простого числа p та натурального числа r введемо числа наступного вигляду

$$N_{p,r} = \frac{p^{p^r} - 1}{p^{p^{r-1}} - 1}.$$

З одного боку їх можна розглядати як узагальнення чисел Ферма [64]

$$N_{2,r} = \frac{2^{2^r} - 1}{2^{2^{r-1}} - 1} = 2^{2^{r-1}} + 1,$$

а з іншого боку - як узагальнення чисел вигляду $N_{p,1} = \frac{p^p - 1}{p - 1}$, які є мінімальним періодом послідовності чисел Белла за модулем p [101]. Ці ж числа виникають і в п’ятому розділі цієї роботи при розгляді порядків елементів у розширеннях Артіна-Шраєра. Зауважимо, що виконується наступна рівність:

$$N_{p,r} = \sum_{i=0}^{p-1} (p^{p^{r-1}})^i.$$

Далі даємо в лемах доведення допоміжних для данного підрозділу результатів.

Лема 6.22. *Для довільного натурального числа r справедлива така рівність:*

$$p^{p^r}-1=(p-1)\prod_{i=1}^{r}N_{p,i}. \qquad (6.24)$$

Доведення. Індукцією за числом r. При $r=1$ маємо справедливу рівність

$$p^{p}-1=(p-1)(1+p+...+p^{p-1})=(p-1)N_{p,r}.$$

Припустимо, що рівність (6.24) справджується для $r=s-1$, тобто

$$p^{p^{s-1}}-1=(p-1)\prod_{i=1}^{s-1}N_{p,i}. \qquad (6.25)$$

Тоді $p^{p^s}-1=(p^{p^{s-1}}-1)N_{p,s}$. Враховуючи (6.25), отримуємо, що рівність (6.24) виконується також і для $r=s$. Лему доведено.

Лема 6.23. *Нехай p - просте число та p ділить q. Тоді числа $q-1$ та $\sum_{j=0}^{p-1}q^j$ є взаємно простими.*

Доведення. Методом від протилежного. Нехай t – спільний дільник чисел $q-1$ та $\sum_{j=0}^{p-1}q^j$. Тоді $q\equiv 1(\mathrm{mod}\,t)$. Звідси маємо $\sum_{j=0}^{p-1}q^j\equiv p(\mathrm{mod}\,t)$. Оскільки t ділить $\sum_{j=0}^{p-1}q^j$, то $t=p$. Отримуємо, що p одночасно ділить $q-1$ та q - суперечність. Лему доведено.

Лема 6.24. *Числа $p-1$, $N_{p,1}$, $N_{p,2}$,..., є попарно взаємно простими.*

Доведення. Зауважимо, що згідно з рівністю (6.24) виконується співвідношення $(p-1)N_{p,r-1} = p^{p^{r-1}} - 1$. Позначимо $q = p^{p^{r-1}} - 1$. Тоді $(p-1)N_{p,r-1} = q-1$ та $N_{p,r} = \sum_{i=0}^{p-1} q^i$. Зрозуміло, що p ділить q. Застосовуючи лему 6.23, отримуємо, що числа $q-1$ та $N_{p,r}$ взаємно прості. Тому взаємно простими є й числа $N_{p,r-1}$ та $N_{p,r}$. Також взаємно простими є $p-1$ і $N_{p,r}$. Лему доведено.

Лема 6.25. *Нехай r – довільне натуральне число та $u_r = \prod_{i=1}^{r} x_i$. Тоді мультиплікативний порядок елемента u_r дорівнює* $\operatorname{ord} u_r = \prod_{i=1}^{r} \operatorname{ord} x_i$.

Доведення. Як наслідок з леми 6.24 маємо, що група E_r^* $(r = 1,2,...)$ є внутрішнім прямим добутком підгрупи F_p^* з $p-1$ елемента та підгруп з $N_{p,i}$ $(i = 1,...,r)$ елементів. Елемент x_i належить до підгрупи порядку $N_{p,i}$. Значить, порядок елемента u_r дорівнює добутку порядків елементів x_i $(i = 1,...,r)$. Лему доведено.

Основні результати даного підрозділу даємо далі в теоремі 6.10 та теоремі 6.11.

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.*

Доведення. Нехай q – просте число, яке ділить $N_{p,r}$. Позначимо $s = p^{p^{r-1}}$ та $t = sp - s$. Тоді справедливі порівняння $sp \equiv s \bmod t$, $sp^2 \equiv s \bmod t, \ldots$ Таким чином, маємо

$$N_{p,r} = 1 + \sum_{i=1}^{p-1} s^i \equiv 1 + \sum_{i=1}^{p-1} s = 1 + s(p-1) \equiv 1 \bmod s .$$

Звідси $(N_{p,r}, s(p-1)) = 1$ і $(q, s(p-1)) = 1$. Число q – непарне (бо є дільником непарного числа $N_{p,r}$) та $q \neq p^{p^{r-1}}$.

Оскільки $p^{p^{r-1}} \equiv 1 \bmod N_{p,r}$ та $q \mid N_{p,r}$, то $p^{p^{r-1}} \equiv 1 \bmod q$. Нехай d – найменше натуральне число, для якого $p^d \equiv 1 \bmod q$. Не може бути $d \mid p^{r-1}$, бо, виходячи з леми 6.24, q не ділить $p^{p^{r-l}} - 1$ для $l = 1, ..., r$. Але $d \mid p^r$ і тому $d = p^r$.

Згідно з малою теоремою Ферма, $p^{q-1} \equiv 1 \bmod q$ і, значить, $p^r \mid q-1$. Відношення $(q-1)/p^r$ парне, бо числа p та q непарні. Таким чином, $q = 2kp^r + 1$ для деякого натурального k. Теорему доведено.

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

Доведення. Згідно з лемою 6.25, справедливі такі співвідношення:

$$\operatorname{ord} u_r = \operatorname{ord} \left(\prod_{i=1}^{r} x_i \right) = \prod_{i=1}^{r} \operatorname{ord} x_i .$$

За теоремою Лагранжа для скінченних груп, $\operatorname{ord} x_i$ є дільником $N_{p,i}$. Тоді, виходячи з теореми 6.10, $\operatorname{ord} x_i$ має вигляд $2kp^i + 1 \geq 2p^i + 1$. Звідси отримуємо потрібний результат. Теорему доведено.

Як було зауважено раніше, елемент x_i належить до підгрупи, порядок якої дорівнює $N_{p,i}$. Узагальнення на недвійкові поля відкритого питання,

поставленого Відеманом [103, 150] для полів характеристики два, полягає в такому: чи мультиплікативний порядок $\operatorname{ord} x_i$ елемента x_i дорівнює $N_{p,i}$. Якщо це так, то au_r, де a – примітивний елемент поля F_p, є примітивним елементом поля E_r.

У випадку $r=1$, тобто для розширень вигляду $E_1(x_1)=F_{p^p}$, нами виконано у підрозділі 5.2 комп'ютерні обчислення порядку елемента x_1 для всіх простих $p<126$. При цьому використано відомі [103] розклади чисел $N_{p,1}$ на прості множники. У всіх розглянутих випадках $\operatorname{ord} x_1 = N_{p,1}$. Також нами виконано обчислення для $p=3$ та $r=2,3,4$. Отримано, що $\operatorname{ord} x_i = N_{p,i}$ ($i=2,3,4$).

6.5. Елементи великого порядку в одній вежі скінченних полів недвійкової характеристики

У даному підрозділі розглядаємо скінченні поля, 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:

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

Зауважимо, що число елементів поля E_1 дорівнює p^p, а число елементів поля E_2 рівне p^{p^2}. Відомо [97], що $x^p - x - a$ нерозкладний поліном над F_p для будь-якого ненульового елемента a з F_p. Тому з обчислювальної точки

зору можна вважати, що $E_1 = F_{p^p} = F_p[x]/(x^p - x - 1)$. При цьому зрозуміло, що виконується рівність $x^p = x + 1$.

Також згідно з лемою 6.1 поліном $y^p - y - x^{p-1}$ є нерозкладним над полем E_1. Виходячи з цього, можемо записати:

$$E_1(y) = F_{p^{p^2}} = F_{p^p}[y]/(y^p - y - x^{p-1})$$

і тоді справедлива рівність $y^p = y + x^{p-1}$.

Допоміжними для даного підрозділу результатами є лема 5.2 та лема 6.26, доведення якої наводимо далі.

Лема 6.26. *Для числа сполучень з повтореннями H_b^a з b елементів по a елементів виконується нерівність:* $H_b^a > \left(\frac{b}{a}\right)^a$.

Доведення. Відомо, що справедлива рівність $H_b^a = \binom{b+a-1}{a}$. Використовуючи відому оцінку для величини біноміальних коефіцієнтів $\binom{n}{k} \geq \left(\frac{n}{k}\right)^k$ при $n = b + a - 1$ та $k = a$, отримуємо наступне співвідношення:

$$H_b^a = \binom{b+a-1}{a} \geq \left(\frac{b+a-1}{a}\right)^a > \left(\frac{b}{a}\right)^a.$$

Лему доведено.

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

$$y^{p^i} = y + u\sum_{k=0}^{s}(x+k)^{p-1} + v\sum_{l=s+1}^{p-1}(x+l)^{p-1}, \qquad (6.26)$$

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

Доведення. Доведення теореми виконуємо методом індукції за числом i.

При $i = 0$ твердження очевидним чином виконується, бо вірною є рівність $y^{p^0} = y$.

Припустимо, що дане твердження справедливе для $i-1$. Покажемо, що тоді воно справедливе для i. Розглянемо такі можливі випадки.

1) $u = v = 0$, тобто $y^{p^{i-1}} = y$. Тоді $y^{p^i} = y^p = y + x^{p-1}$. Таким чином, елемент y^{p^i} має вигляд (6.26).

2) $u = 1$, $v = 0$, $0 \le s \le p-2$, тобто $y^{p^{i-1}} = y + \sum_{k=0}^{s}(x+k)^{p-1}$. У цьому випадку можемо записати такі рівності:

$$y^{p^i} = y + x^{p-1} + \sum_{k=0}^{s}(x+k+1)^{p-1} = y + \sum_{k=0}^{s+1}(x+k)^{p-1}.$$

Як бачимо, елемент y^{p^i} має вигляд (6.26), де $1 \le s \le p-1$.

3) $u = 1$, $v = 0$, $s = p-1$, тобто $y^{p^{i-1}} = y + \sum_{k=0}^{p-1}(x+k)^{p-1}$. Тоді виконуються наступні співвідношення:

$$y^{p^i} = y + x^{p-1} + \sum_{k=0}^{p-1}(x+k+1)^{p-1} = y + x^{p-1} + \sum_{k=1}^{p-1}(x+k)^{p-1} + (x+p)^{p-1} =$$
$$= y + 2x^{p-1} + \sum_{k=1}^{p-1}(x+k)^{p-1}.$$

Таким чином, у цьому випадку елемент y^{p^i} має вигляд (6.26).

4) $u = 0$, $v = p-1$, $0 \le s \le p-2$, тобто

$$y^{p^{i-1}} = y + (p-1)\sum_{k=s}^{p-1}(x+k)^{p-1}.$$

У цьому разі можемо записати

$$y^{p^i} = y + x^{p-1} + (p-1)\sum_{k=s}^{p-1}(x+k+1)^{p-1} = y + (1+p-1)x^{p-1} + (p-1)\sum_{k=s+1}^{p-1}(x+k)^{p-1} =$$

$$= y + (p-1)\sum_{k=s+1}^{p-1}(x+k)^{p-1}$$

.

Зрозуміло, що елемент y^{p^i} має вигляд як у формулі (6.26).

5) $u=0,\ v=p-1,\ s=p-1$, тобто маємо

$$y^{p^{i-1}} = y + (p-1)(x+p-1)^{p-1}.$$

У цьому випадку отримуємо

$$y^{p^i} = y + x^{p-1} + (p-1)(x+p-1+1)^{p-1} = y + x^{p-1} + (p-1)x^{p-1} = y.$$

Очевидно, що елемент y^{p^i} має вигляд згідно з (6.26).

6) $u,v \neq 0,\ u,v \neq p-1,\ u=v+1,\ 0 \le s \le p-3$, тобто маємо наступну рівність:

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

У цьому випадку справедливі співвідношення:

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

$$= y + u\sum_{k=0}^{s+1}(x+k)^{p-1} + v\sum_{l=s+2}^{p-1}(x+l)^{p-1}.$$

Очевидно, що y^{p^i} має вигляд (6.26).

7) $u,v \neq 0,\ u,v \neq p-1,\ u=v+1,\ s=p-2$, тобто маємо наступну рівність:

$$y^{p^{i-1}} = y + u\sum_{k=0}^{p-2}(x+k)^{p-1} + v(x+p-1)^{p-1}.$$

У цьому випадку справедливі співвідношення:

$$y^{p^i} = y + x^{p-1} + u\sum_{k=0}^{p-2}(x+k+1)^{p-1} + v(x+p-1+1)^{p-1} = y + u\sum_{k=0}^{p-1}(x+k)^{p-1}.$$

Очевидно, що y^{p^i} також має вигляд (6.26).

Теорему доведено.

Спряжені елемента $y \in F_{p^{p^2}}$ відносно F_p отримуємо застосовуючи всі автоморфізми поля $F_{p^{p^2}}$ над простим полем F_p до елемента y [97]. Згадані автоморфізми утворюють групу з операцією, яка є композицією відображень. Згідно з [97, теорема 2.21] ця група циклічна, а кількість її елементів дорівнює p^2.

Основний результат даного підрозділу даємо далі в теоремі 6.13.

Теорема 6.13. *Елемент y поля $F_{p^{p^2}}$ має мультиплікативний порядок більший від величини* $\dfrac{p^p - 1}{p-1}$.

Доведення. До підгрупи $\langle y \rangle$, породженої елементом y, належать спряжені елемента y (за рахунок p^2 автоморфізмів над F_p), які мають за теоремою 6.12 вигляд (6.26). У результаті маємо p^2 різних лінійних двочленів від y з коефіцієнтами з поля F_{p^p}. З них утворюємо добутки, вибираючи щонайбільше $p-1$ двочлен (двочлени можна повторювати). У результаті отримуємо різні добутки за модулем полінома $y^p - y - x^{p-1}$. Оцінимо знизу загальне можливе число таких добутків.

Зрозуміло, що маємо сполучення з повтореннями з p^2 елементів по r елементів ($0 \le r \le p-1$). Тобто загалом маємо $\sum_{r=0}^{p-1} H^{r}_{p^2}$ варіантів. Далі даємо нижню межу для цієї величини.

Згідно лемою 6.26 можемо записати такі нерівності:

$$\sum_{r=0}^{p-1} H^{r}_{p^2} > \sum_{r=0}^{p-1} \left(\frac{p^2}{r} \right)^r > \sum_{r=0}^{p-1} p^r = \frac{p^p - 1}{p-1}.$$

Теорему доведено.

Як можна бачити, для часткового випадку $r = 2$, теорема 6.13 дає кращий результат, ніж теорема 6.11. Разом з тим, випадок $r > 2$ потребує подальших додаткових досліджень, зокрема опису спряжених елементів до елементів, що задають розширення. Слід також зауважити, що використані в доведенні теореми 6.13 спряжені елемента y – це поліноми за модулем полінома степеня p над проміжним полем $F_{p^p} = F_p[x]/(x^p - x - 1)$ розглянутої вежі з трьох полів, а не полінома степеня p^2 над початковим полем F_p цієї вежі. Тому й отримано відповідний результат. Знайшовши спряжені елемента y за модулем полінома більшого степеня, а власне p^2, цей результат можна підсилити.

Приклад 6.4. Розглянемо для прикладу випадок $p = 5$. У цьому разі маємо

$$E_1 = F_{p^p} = F_p[x]/(x^p - x - 1) = F_{5^5} = F_5[x]/(x^5 - x - 1).$$

Тоді, згідно з лемою 5.2, виконуються наступні рівності:

$$x^5 = x + 1,\ x^{5^2} = x + 2,\ x^{5^3} = x + 3,\ x^{5^4} = x + 4.$$

Тобто, елемент x має 5 спряжених елементів (враховуючи сам елемент) над полем F_5. Також маємо такі співвідношення:

$$E_2 = F_{p^{p^2}} = F_{p^p}[y]/(y^p - y - x^{p-1}) = F_{5^{5^2}} = F_{5^5}[y]/(y^5 - y - x^4) = F_{5^5}(y)$$

Елемент y має 25 спряжених елементів над початковим полем F_5. Вони виписані далі. Це лінійні поліноми за модулем полінома $y^5 - y - x^4$ над проміжним полем $F_{5^5} = F_5[x]/(x^5 - x - 1)$ у вежі з трьох полів. Разом з тим їх можна було б записати за модулем полінома степеня 25 над початковим полем F_5 цієї вежі, проте в загальному невідомо чи вони залишаться лінійними поліномами.

$$y^{5^0} = y$$

$$y^{5^1} = y + x^4$$

$$y^{5^2} = y + x^4 + (x+1)^4$$

$$y^{5^3} = y + x^4 + (x+1)^4 + (x+2)^4$$

$$y^{5^4} = y + x^4 + (x+1)^4 + (x+2)^4 + (x+3)^4$$

$$y^{5^5} = y + x^4 + (x+1)^4 + (x+2)^4 + (x+3)^4 + (x+4)^4$$

Зауважимо, що виконується наступне співвідношення (воно є частковим випадком (6.26)):

$$y^{5^5} - y^{5^0} = x^4 + (x+1)^4 + (x+2)^4 + (x+3)^4 + (x+4)^4,$$

яке випливає із того факту, що $y^5 = y + x^4$. Аналогічні вирази також виписано далі для $y^{5^{10}} - y$, $y^{5^{15}} - y$, $y^{5^{20}} - y$.

$$y^{5^6} = y + 2x^4 + (x+1)^4 + (x+2)^4 + (x+3)^4 + (x+4)^4$$

$$y^{5^7} = y + 2x^4 + 2(x+1)^4 + (x+2)^4 + (x+3)^4 + (x+4)^4$$

$$y^{5^8} = y + 2x^4 + 2(x+1)^4 + 2(x+2)^4 + (x+3)^4 + (x+4)^4$$

$$y^{5^9} = y + 2x^4 + 2(x+1)^4 + 2(x+2)^4 + 2(x+3)^4 + (x+4)^4$$

$$y^{5^{10}} = y + 2x^4 + 2(x+1)^4 + 2(x+2)^4 + 2(x+3)^4 + 2(x+4)^4$$

$$y^{5^{11}} = y + 3x^4 + 2(x+1)^4 + 2(x+2)^4 + 2(x+3)^4 + 2(x+4)^4$$

$$y^{5^{12}} = y + 3x^4 + 3(x+1)^4 + 2(x+2)^4 + 2(x+3)^4 + 2(x+4)^4$$

$$y^{5^{13}} = y + 3x^4 + 3(x+1)^4 + 3(x+2)^4 + 2(x+3)^4 + 2(x+4)^4$$

$$y^{5^{14}} = y + 3x^4 + 3(x+1)^4 + 3(x+2)^4 + 3(x+3)^4 + 2(x+4)^4$$

$$y^{5^{15}} = y + 3x^4 + 3(x+1)^4 + 3(x+2)^4 + 3(x+3)^4 + 3(x+4)^4$$

$$y^{5^{16}} = y + 4x^4 + 3(x+1)^4 + 3(x+2)^4 + 3(x+3)^4 + 3(x+4)^4$$

$$y^{5^{17}} = y + 4x^4 + 4(x+1)^4 + 3(x+2)^4 + 3(x+3)^4 + 3(x+4)^4$$

$$y^{5^{18}} = y + 4x^4 + 4(x+1)^4 + 4(x+2)^4 + 3(x+3)^4 + 3(x+4)^4$$

$$y^{5^{19}} = y + 4x^4 + 4(x+1)^4 + 4(x+2)^4 + 4(x+3)^4 + 3(x+4)^4$$

$$y^{5^{20}} = y + 4x^4 + 4(x+1)^4 + 4(x+2)^4 + 4(x+3)^4 + 4(x+4)^4$$

$$y^{5^{21}} = y + 4(x+1)^4 + 4(x+2)^4 + 4(x+3)^4 + 4(x+4)^4$$

$$y^{5^{22}} = y + 4(x+2)^4 + 4(x+3)^4 + 4(x+4)^4$$

$$y^{5^{23}} = y + 4(x+3)^4 + 4(x+4)^4$$

$$y^{5^{24}} = y + 4(x+4)^4$$

Таким чином, отримали $p^2 = 25$ різних лінійних двочленів від формальної змінної y з коефіцієнтами з поля F_{p^p}. З цих двочленів утворюємо всеможливі добутки по $p-1=4$ співмножники. У результаті маємо, що мультиплікативний порядок елемента y більший від величини $\frac{5^5-1}{5-1} = 781$.

6.6. Висновки до розділу

У даному розділі даємо нижню межу для мультиплікативного порядку деяких елементів у рекурсивних розширеннях скінченних полів характеристики два, визначених Конвеєм та Відеманом, а також у рекурсивних розширеннях скінченних полів характеристики більшої від двох.

У першому підрозділі наводимо нижню межу для мультиплікативного порядку деяких елементів у двійкових рекурсивних розширеннях скінченних полів, визначених Конвеєм. У цьому випадку явно будуємо елементи мультиплікативного порядку принаймні $\prod_{j=1}^{i} N_j$ для $1 \le i \le 4$ та мультиплікативного порядку принаймні $\prod_{j=1}^{4} N_j \cdot \prod_{j=5}^{i} (3 \cdot 2^{j+2} + 1)$ для $i \ge 5$, де N_j позначає j-те число Ферма.

В другому підрозділі описуємо деякі примітивні елементи для перших дванадцяти полів у вежах Конвея. Ці елементи задають розширенння полів у вказаній вежі. Також формулюємо умову, при виконанні якої елементи такого вигляду є примітивними для довільного поля у вказаній вежі скінченних полів характеристики два.

У третому підрозділі наводимо нижню межу для мультиплікативного порядку деяких елементів у двійкових рекурсивних розширеннях скінченних полів, визначених Відеманом. При цьому, зокрема, отримано результати, які накладають обмеження на порядок елементів, що задають вказані розширення полів. Дані результати можуть мати також і самостійне значення.

Четвертий та п’ятий підрозділи присвячено отриманню нижніх меж для порядку елементів у вежах скінченних полів характеристики більшої, ніж два. Наведено нижню межу для порядків елементів, які задають розширення у недвійковій вежі скінченних полів. У п’ятому підрозділі розглядаємо частковий випадок вежі, введеної в четвертому підрозділі, а саме вежі, що складається з двох скінченних полів, які будуємо рекурсивно. У цьому частковому випадку вежі з двох полів описано спряжені елемента, що задає останнє поле у вежі над початковим полем. У цьому разі отримано кращу нижню межу, ніж у загальному випадку.

Результати цього розділу опубліковано в роботах [13, 15, 16, 17, 113].

Розділ 7

Елементи великого порядку в скінченних полях загального вигляду

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

7.1. Елементи великого порядку в скінченних полях загального вигляду на основі гіпотези Гао

У даному підрозділі даємо підсилення нижньої межі Гао-Конфлітті для мультиплікативного порядку елементів у скінченних полях загального вигляду. Якщо ніякі обмеження не накладаємо на степінь розширення n, то відомо дуже мало результатів. У праці [73] Гао дає алгоритм для побудови елементів великого порядку в загальних розширеннях F_{q^n} скінченого поля F_q з нижньою межею для порядку рівною

$$n^{\frac{\log_q n}{4\log_q(2\log_q n)}-\frac{1}{2}}.$$

Його алгоритм припускає деяку правдоподібну, але не доведену гіпотезу. Розвиваючи цей підхід, Конфлітті [61] запропонував уточнений аналіз результатів з роботи [73].

Покладемо $F_q(\theta) = F_{q^n} = F_q[x]/f(x)$, де $f(x)$ – нерозкладний поліном над F_q степеня n та $\theta = x \bmod f(x)$ – суміжний клас елемента x за модулем полінома $f(x)$.

У даному підрозділі ми беремо конструкцію Гао для будь-якого скінченого поля F_{q^n} і показуємо, що вона дає елементи мультиплікативного порядку принаймні

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

де d – найближче більше ціле число до величини $2\log_q n$, а t – найближче менше ціле число до величини $\log_d n$. Використовуємо для доведення метод подібний до того, що описаний в роботах [61, 73]. Основним результатом даного підрозділу є наступна теорема.

Теорема 7.1. *Елемент θ має в полі $F_q(\theta) = F_{q^n} = F_q[x]/f(x)$ мультиплікативний порядок принаймні*

$$\binom{n+t-1}{t}\prod_{i=0}^{t-1}\frac{1}{d^i}. \qquad (7.1)$$

Далі даємо допоміжні результати для доведення теореми 7.1.

Нехай m – найменший степінь числа q, який більший або рівний числу n. Підхід Гао [73] спирається на висловлену ним гіпотезу, яка стверджує таке: для довільного цілого числа n існує такий поліном $g(x) \in F_q[x]$ степеня d (який не перевищує $2\log_q n$), що поліном $x^m - g(x)$ має нерозкладний дільник $f(x)$ степеня n. Поліном $x^m - g(x)$, який фігурує в гіпотезі, подібний 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 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 $x^m - g(x)$.

Зауважимо, що наведені обчислювальні дані [73] підтверджують гіпотезу лише для полів характеристики два, а для полів характеристики, більшої від двох, такі дані в літературі відсутні.

Якщо гіпотеза виконується, то зрозуміло, що справедлива рівність $\theta^m = g(\theta)$. Гао розглядав множину $S = \left\{ \sum_{i=0}^{t-1} u_i m^i \mid 0 \le u_i \le \mu \right\}$ і вибирав величини t та μ з умови $\mu d^t < n$. Він довів, що степені θ^u є різними елементами для різних $u \in S$, беручи $t = \left\lfloor \frac{\log_q n}{2\log_q d} \right\rfloor$, $\mu = \sqrt{n}$ та показуючи виконання наступної нерівності:

$$| S | = (\mu + 1)^t \ge n^{\frac{\log_q n}{4\log_q (2\log_q n)} - \frac{1}{2}}.$$

Конфлітті в праці [61] у свою чергу розглядав наступну видозмінену множину:

$$S = \left\{ \sum_{i=0}^{t-1} u_i m^i \mid 0 \le u_i \le \mu_i, \frac{n}{td^i} - 1 \le \mu_i \le \frac{n}{td^i} \right\}$$

і вибирав числа t та μ з умови $\sum_{i=0}^{t-1} \mu_i d^i < n$. Він довів, що степені θ^u є різними елементами для $u \in S$, беручи $t = \lfloor \log_d n \rfloor$ та показуючи справедливість такого співвідношення:

$$| S_t |= \prod_{i=0}^{t-1} (\mu_i + 1) \geq \left(\frac{n}{t} \right)^t \prod_{i=0}^{t-1} \frac{1}{d^i}. \qquad (7.2)$$

Підставляючи величину $t = \lfloor \log_d n \rfloor$ у рівність (7.2), отримуємо наступну нерівність:

$$\operatorname{ord} \theta \geq \left(\frac{nd}{\log_d^2 n} \right)^{\frac{1}{2}\log_d n}. \qquad (7.3)$$

Результати із вказаних робіт [61, 73] ґрунтуються на такому твердженні.

Лема 7.1. ([50, теорема 1.4]) *Припустимо, що* $f(x) \in F_q[x]$ *не є ні одночленом, ні двочленом вигляду* $ax^{p^l} + b$, *де* p *– характеристика поля* F_q. *Тоді поліноми*

$$f^{(1)}(x) = f(x), \quad f^{(k)}(x) = f^{(k-1)}(x), \quad k \geq 2$$

є мультиплікативно незалежними в $F_q[x]$, *тобто, якщо*

$$(f^{(1)}(x))^{k_1} (f^{(2)}(x))^{k_2} \ldots (f^{(s)}(x))^{k_s} = 1$$

для будь-яких натуральних чисел $s \geq 1$, $k_1, \ldots, k_s$, *то* $k_1 = k_2 = \ldots = k_s = 0$.

Наступна лема дає нижню межу для кількості невід'ємних розв'язків лінійної діофантової нерівності.

Лема 7.2. [91] *Нехай* $a_0, \ldots, a_{r-1}$ *– натуральні числа, що задовольняють умову* $(a_0, \ldots, a_{r-1}) = 1$. *Тоді кількість невід'ємних цілочисельних розв'язків* $x_0, \ldots, x_{r-1}$ *лінійної діофантової нерівності*

$$\sum_{i=0}^{r-1} a_i x_i \le m, \tag{7.4}$$

є принаймні наступна величина:

$$\binom{m+r}{r} \prod_{i=0}^{r-1} \frac{1}{a_i}.$$

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. Більш точно, щоб підсилити результат Конфлікті, ми розглядаємо множину

$$S = \left\{ \sum_{i=0}^{t-1} u_i m^i \mid \sum_{i=0}^{t-1} d^i u_i \le n-1 \right\},$$

тобто $u_0,...,u_{r-1}$ є розв'язком лінійної діофантової нерівності $\sum_{i=0}^{r-1} d^i u_i \le m$, і показуємо що θ^u є різними елементами в полі F_{q^n} для різних елементів $u \in S$.

Далі даємо доведення нашого основного результату для першого підрозділу.

Доведення теореми 7.1. Якщо елемент θ є коренем полінома $x^m - g(x)$, то оскільки m є степенем числа q, застосовуючи до θ послідовно автоморфізм Фробеніуса, маємо для будь-якого натурального числа i наступну рівність:

$$\theta^{m^i} = g^{(i)}(\theta), \tag{7.5}$$

де, як у формулюванні леми 7.1, $g^{(i)}(x)$ є поліномом, отриманим компонуванням $g(x)$ самого з собою i разів.

Розглянемо наступну множину:

$$S = \left\{ \sum_{i=0}^{t-1} u_i m^i \mid \sum_{i=0}^{t-1} d^i u_i \le n-1, \quad u_i \ge 0 \right\}.$$

Для кожного елемента $u \in S$ будуємо степінь θ^u, який належить до групи, породженої елементом θ. Покажемо, що коли два елементи $u, v \in S$ є різними, то відповідні їм степені не співпадають.

Припустимо, що елементи $u = \sum_{i=0}^{t-1} u_i m^i$ та $v = \sum_{i=0}^{t-1} v_i m^i$ з множини S різні, а відповідні їм степені співпадають, тобто $\theta^u = \theta^v$. Тоді маємо наступну рівність:

$$\prod_{i=0}^{t-1} \left(\theta^{m^i}\right)^{u_i} = \prod_{i=0}^{t-1} \left(\theta^{m^i}\right)^{v_i}.$$

Беручи до уваги рівність (7.5), отримуємо таке співвідношення:

$$\prod_{i=0}^{t-1} \left(g^{(i)}(\theta)\right)^{u_i} = \prod_{i=0}^{t-1} \left(g^{(i)}(\theta)\right)^{v_i}.$$

Введемо позначення для поліномів: $h_1(x) = \prod_{u_i > v_i} \left(g^{(i)}(x)\right)^{u_i - v_i}$ та $h_2(x) = \prod_{v_i > u_i} \left(g^{(i)}(x)\right)^{v_i - u_i}$. Тоді, виходячи з останньої рівності, маємо $h_1(\theta) = h_2(\theta)$. Оскільки поліном $g(x)$ є мінімальним поліномом для елемента θ, то можемо записати $h_1(x) = h_2(x) \bmod f(x)$. Так як поліном $g^{(i)}(x)$ має степінь d^i, то $h_1(x)$ є поліномом степеня щонайбільше $\sum_{i=0}^{t-1} u_i d^i \le n-1$ та $h_2(x)$ є поліномом степеня щонайбільше $\sum_{i=0}^{t-1} v_i d^i \le n-1$. Значить $h_1(x)$ та $h_2(x)$

повинні бути рівні як поліноми над полем F_q. Тому справедлива така рівність:

$$\prod_{i=0}^{t-1}\left(g^{(i)}(x)\right)^{u_i-v_i}=1.$$

Згідно з лемою 7.1 поліноми $g^{(i)}(x)$ є мультиплікативно незалежними в $F_q[x]$. Отже, $u_i=v_i$ для $i=0,...,t-1$, і значить $u=v$. У результаті ми отримали суперечність. Значить, різним елементам з множини S відповідають різні степені елемента θ.

Таким чином, кількість елементів множини S (і мультиплікативний порядок елемента θ) є принаймні кількість невід'ємних цілочисельних розв'язків діофантової нерівності $\sum_{i=0}^{t-1} d^i x_i \le n-1$. На завершення доведення даної теоерми, застосовуючи лему 7.2, маємо наступну нерівність:

$$|S|\ge\binom{n+t-1}{t}\prod_{i=0}^{t-1}\frac{1}{d^i},$$

і отримуємо потрібний результат. Теорему доведено.

Тепер порівняємо наш результат, який наведений у формулі (7.1), із результатом Конфлітті, що дається формулою (7.2). Підрахуємо з цією метою відношення R нижньої межі (7.1) до нижньої межі (7.2).

$$R=\prod_{i=1}^{t-1}\frac{n+i}{n}\cdot\frac{t}{i}.$$

Оскільки при $i=1,...,t-1$ виконуються нерівності $\frac{n+i}{i}>1$ та $\frac{t}{i}>1$, то зрозуміло, що $R>1$ для будь-яких чисел q та n (нагадаємо, що величина t залежить від q та n).

Наводимо далі низку числових прикладів нижніх меж для мультиплікативних порядків розглянутого раніше елемента θ та відношення R вказаних меж.

Позначимо нижні межі для порядку елемента θ, отримані в праці [48] та у даному підрозділі через b_1 та b_2 відповідно. Значення величин q, n, d, t, b_1, b_2 та відношення R нижніх меж у запропонованих прикладах даються в табл. 7.1.

Таблиця 7.1

Порівняння відомих та отриманих нижніх меж для мультиплікативного порядку елемента θ

№	q	n	d	t	b_1	b_2	R
1	127	1000	3	6	$1{,}49\cdot10^{6}$	$9{,}82\cdot10^{7}$	65,77
2	257	10000	3	8	$2{,}6\cdot10^{11}$	$1{,}08\cdot10^{14}$	417,26
3	19991	100000	2	16	$4{,}07\cdot10^{24}$	$3{,}59\cdot10^{30}$	882716,52
4	17	400	4	4	$2{,}44\cdot10^{4}$	$2{,}64\cdot10^{5}$	10,83
5	101	109	2	6	$1{,}07\cdot10^{3}$	$8{,}14\cdot10^{4}$	74,19
6	1031	1000	2	9	$3{,}76\cdot10^{7}$	$4{,}16\cdot10^{10}$	1106,65
7	10007	10000	2	13	$1{,}09\cdot10^{14}$	$5{,}36\cdot10^{18}$	49019,55
8	103	300	2	8	$1{,}46\cdot10^{4}$	$6{,}65\cdot10^{6}$	456,00
9	107	700	3	5	$9{,}11\cdot10^{5}$	$2{,}41\cdot10^{7}$	26,40
10	131	1000	3	6	$1{,}49\cdot10^{6}$	$9{,}83\cdot10^{7}$	65,80
11	257	1000	2	9	$3{,}76\cdot10^{7}$	$4{,}16\cdot10^{10}$	111,00
12	701	1000	3	8	$2{,}61\cdot10^{11}$	$1{,}09\cdot10^{14}$	417,00
13	1019	1000	2	9	$3{,}76\cdot10^{7}$	$4{,}16\cdot10^{10}$	1106,65
14	1019	10000	3	8	$2{,}61\cdot10^{11}$	$1{,}09\cdot10^{14}$	417,27

7.2. Побудова елементів великого порядку в скінченних полях загального вигляду без використання гіпотези Гао

У даному підрозділі розглянуто можливі варіанти побудови елементів великого мультиплікативного порядку в розширеннях скінченних полів загального вигляду без використання гіпотези Гао.

Відомо дуже мало результатів, коли жодне обмеження не накладене на степінь розширення поля. Нижче розглядаємо можливі варіанти побудови елементів великого мультиплікативного порядку в скінченних полях загального вигляду. На відміну від досліджень [61, 73] не спираємося на так звану гіпотезу Гао про існування відповідного полінома. Для отримання нижніх меж, зокрема, застосовуємо наслідок із ABC теореми Стовера–Мейсона [29]. Основні результати другого підрозділу – це теорема 7.5 та теорема 7.7.

Розглядаємо скінченне поле загального вигляду

$$F_{q^n} = F_q[x]/(f(x)),$$

де поліном $f(x)$ – нерозкладний над початковим полем F_q та $\deg f(x) = n$. Через θ позначаємо клас елемента x у вказаному фактор-кільці, яке є полем. Оскільки елемент θ задає розширення поля F_q степеня n, то θ не може бути коренем ніякого полінома з коефіцієнтами з F_q степеня, меншого за n.

Справедлива наступна теорема.

Теорема 7.2. *Елемент θ має мультиплікативний порядок принаймні n.*

Доведення. Покажемо, що елементи 1, θ,…, θ^{n-1} є попарно різними. Припустимо, що це не так. Тоді для деяких $0 \le i < j \le n-1$ виконується рівність

$\theta^i = \theta^j$, тобто $\theta^{i-j} \equiv 1 \pmod{f(x)}$. Оскільки $j - i < n = \deg f(x)$, то $x^{j-i} - 1 = 0$. Таким чином, θ є коренем тотожно не рівного нулю полінома $x^{j-i} - 1$ з коефіцієнтами з F_q степеня щонайбільше $n-1$. Отримуємо суперечність, що завершує доведення теореми. Теорему доведено.

Насправді можемо збудувати для поля $F_{q^n} = F_q[x]/(f(x))$ багато елементів з мультиплікативним порядком принаймні n.

Теорема 7.3. *Нехай b – довільний ненульовий елемент скінченного поля F_q. Тоді елемент $\theta + b$ має мультиплікативний порядок принаймні n.*

Доведення. Покажемо, що елементи 1, $\theta + b$,…, $(\theta + b)^{n-1}$ є попарно різними. Припустимо, що це не так. Тоді для деяких цілих чисел $0 \le i < j \le n-1$ виконується рівність $(\theta + b)^i = (\theta + b)^j$. Таким чином, θ є коренем тотожно не рівного нулю полінома $(x + b)^{j-i} - 1$ з коефіцієнтами із скінченого поля F_q степеня щонайбільше $n-1$. Отримуємо суперечність, що й завершує доведення теореми. Теорему доведено.

Згідно з працею [97] справедлива така теорема.

Теорема 7.4. [97, теорема 3.86] *Нехай F_q – скінченне поле характеристики p. Для будь-якого цілого числа $n \ge 2$ такого, що $2n(n-1)$ не ділиться на p, нехай $T_n(q)$ позначає кількість елементів $a \in F_q$, для яких тричлен $x^n + x + a$ нерозкладний над F_q. Тоді існує така константа B_n, залежна лише від n, що виконується нерівність*

$$\left| T_n(q) - \frac{q}{n} \right| \le B_n \sqrt{q}\,.$$

Формулювання теореми 7.4 означає, що для значної кількості скінченних полів поліном, який задає поле, можна вибрати у вигляді

$f(x) = x^n + x + a$. Позначимо через θ суміжний клас елемента x за модулем полінома $f(x)$, який задає розширене поле. Тоді справедлива наступна рівність: $\theta^n = -(\theta + a)$.

Зауважимо, що умова теореми 7.4 не виконується для випадку $n = p$, який окремо розглянуто в підрозділі 5.1 (розширення полів на основі поліномів Артіна–Шраєра). Показано, що можна явно збудувати елементи з мультиплікативним порядком принаймні 4^p. Якщо n ділиться на p (але n не збігається з p), тобто маємо розширення $F_{p^{pt}}$ для деякого цілого числа t, то можемо, взявши підполе F_{p^p}, отримати елемент порядку принаймні 4^p. Проте загальну ситуацію у цьому разі не розглянуто. Також не досліджено випадок, коли $n-1$ ділиться на p.

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

Доведення. Зрозуміло, що підгрупа, породжена елементом θ, містить елементи $\theta, \ldots, \theta^{n-1}$ і, оскільки $\theta^n = -(\theta + a)$, також елементи $-(\theta + a), \ldots, (-1)^{n-1}(\theta + a)^{n-1}$.

Розглянемо множину з таких добутків цих елементів: $(-1)^j \theta^i (\theta + a)^j$, $i, j \geq 0$, $i + j \leq n-1$. Покажемо, що всі добутки з наведеної множини різні.

Припустимо, що для деяких різних пар (i_1, j_1) та (i_2, j_2) таких, що $i_1, j_1 \geq 0, i_1 + j_1 \leq n-1$ та $i_2, j_2 \geq 0, i_2 + j_2 \leq n-1$, маємо однакові добутки, тобто $(-1)^{j_1} \theta^{i_1} (\theta + a)^{j_1} = (-1)^{j_2} \theta^{i_2} (\theta + a)^{j_2}$. Розглянемо можливі принципово різні випадки.

1) $i_1 > i_2, j_1 = j_2$.

Тоді θ є коренем тотожно не рівного нулю полінома $x^{i_1-i_2}-1$ з коефіцієнтами з F_q степеня щонайбільше $n-1$. Отримуємо суперечність.

2) $i_1 > i_2, j_1 > j_2$.

У цьому разі θ є коренем тотожно не рівного нулю полінома $(-1)^{j_1-j_2}x^{i_1-i_2}(x+a)^{j_1-j_2}-1$ з коефіцієнтами з F_q степеня щонайбільше $n-1$. Також отримуємо суперечність.

3) $i_1 > i_2, j_1 < j_2$.

Тут θ є коренем полінома $x^{i_1-i_2}-(-1)^{j_2-j_1}(x+a)^{j_2-j_1}$ з коефіцієнтами з F_q степеня щонайбільше $n-1$. Цей поліном тотожно не рівний нулю, оскільки при $i_1-i_2 > j_2-j_1$ його доданок найбільшого степеня дорівнює $x^{i_1-i_2}$, при $j_2-j_1 > i_1-i_2$ – дорівнює $(-1)^{j_2-j_1+1}x^{j_2-j_1}$, а при $i_1-i_2 = j_2-j_1$ – дорівнює $-ax^{j_2-j_1-1}$ для парного j_2-j_1 та $2x^{j_2-j_1}$ для непарного j_2-j_1. Отримуємо суперечність і в третьому випадку.

Обчислимо тепер кількість цих добутків. Якщо зафіксуємо $0 \le i \le n-1$, то j може набувати значення від 0 до $n-i-1$. Таким чином, загальна кількість добутків дорівнює сумі

$$\sum_{i=0}^{n-1}(n-i-1) = \frac{(n-1)n}{2}.$$

Теорему доведено.

Згідно з працею [29] справедлива така теорема, яка є наслідком так званої ABC теореми Стовера–Мейсона для поліномів. Як звичайно, $\operatorname{rad} L$ позначає найбільший вільний від квадратів зі старшим коефіцієнтом 1 дільник полінома L, тобто, добуток всіх нерозкладних поліномів зі старшим коефіцієнтом 1, які ділять L.

Теорема 7.6. [29, теорема 2.2] *Нехай K – поле, а h – елемент додатного степеня з поліноміального кільця $K[x]$. Припустимо, що $1,2,3,...,3\deg h-2$ є оборотними в полі K. Нехай A,B,C – різні ненульові елементи з $K[x]$. Якщо $\gcd(A,B,C)$ взаємно простий з h та $A\equiv B\equiv C(\bmod h)$, то виконується така нерівність:*

$$\max\{\deg A,\deg B,\deg C\}>2\deg h-\deg\operatorname{rad} A-\deg\operatorname{rad} B-\deg\operatorname{rad} C+$$
$$+\deg\operatorname{rad}\gcd(A,B)+\deg\operatorname{rad}\gcd(A,C)+\deg\operatorname{rad}\gcd(B,C).$$

Початково ідея використання ABC теореми Стовера–Мейсона для підсилення оцінки для порядку певних мультиплікативних підгруп скінченних кілець висловлена в праці [145]. Далі цю думку розвинув Д. Бернштейн [29]. Пропозицію використати ABC теорему для поліпшення оцінки для порядку гауссового періоду навели як відкрите питання автори праці [22].

У припущенні $p\geq 3n-1$ можна, застосувавши наслідок з ABC теореми – теорему 7.6 [29], отримати кращу нижню оцінку для порядку елемента θ. Це зроблено в наступній теоремі.

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*

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

Доведення. Будемо використовувати позначення

$$K = F_{q^n} = F_q[x]/(h(x))$$

та $h(x) = x^n + x + a$. Елемент 1 тривіально має обернений у полі K. Якщо $p \geq 3\deg h - 1$, то елементи $2,3,...,3\deg h - 2$ також мають обернені в полі K.

Покладемо $u = x$ та $v = -(x + a)$. Розглянемо множину S з таких добутків елементів u та v: $(-1)^j u^i v^j$, $i, j \geq 0$, $i + j \leq 2n - 2$. Обчислимо кількість цих добутків. Якщо зафіксуємо $0 \leq i \leq 2n - 2$, то j може набувати значень від 0 до $2n - 2 - i$. Таким чином, загальна можлива кількість добутків дорівнює

$$\sum_{i=0}^{2n-2}(2n - i - 2) = \frac{(2n-1)(2n-2)}{2}.$$

Зрозуміло, що для добутків будь-яких трьох елементів A, B, C з вказаної множини S маємо $\gcd(A, B, C) = u^k v^l$ для деяких невід'ємних цілих чисел k та l. Очевидно, що $h(x) = x^n + x + a$ не ділиться на $u = x$ та не ділиться на $v = -(x + a)$. Значить, $\gcd(A, B, C) = u^k v^l$ є взаємно простим з h.

Розглянемо можливі варіанти для нерівності, яка фігурує в формулюванні теореми 7.6.

1). $\deg\operatorname{rad} A = \deg\operatorname{rad} B = \deg\operatorname{rad} C = 2$

У цьому випадку справедливі умови:

$$\deg\operatorname{rad}\gcd(A, B) = \deg\operatorname{rad}\gcd(A, C) = \deg\operatorname{rad}\gcd(B, C) = 2$$

Тоді вказана нерівність зводиться до такої нерівності:

$$\max\{\deg A, \deg B, \deg C\} > 2\deg h.$$

2). $\deg\operatorname{rad} A = \deg\operatorname{rad} B = \deg\operatorname{rad} C = 1$

У цьому випадку справедливі умови:

$$\deg \operatorname{rad} \gcd(A,B) = \deg \operatorname{rad} \gcd(A,C) = \deg \operatorname{rad} \gcd(B,C) = 1$$

Тоді вказана нерівність зводиться до такої ж нерівності, як і у випадку 1, а саме:

$$\max\{\deg A, \deg B, \deg C\} > 2\deg h.$$

3). Не зменшуючи загальності можемо прийняти, що для одного з елементів, скажімо A, маємо: $\deg \operatorname{rad} A = 1$, а для двох інших виконується $\deg \operatorname{rad} B = \deg \operatorname{rad} C = 2$.

У цьому випадку справедливі умови:

$$\deg \operatorname{rad} \gcd(A,B) = \deg \operatorname{rad} \gcd(A,C) = 1, \quad \deg \operatorname{rad} \gcd(B,C) = 2$$

Тоді вказана нерівність зводиться до такої нерівності:

$$\max\{\deg A, \deg B, \deg C\} > 2\deg h - 1.$$

4). Не зменшуючи загальності можемо прийняти, що для одного з елементів, скажімо C, маємо: $\deg \operatorname{rad} A = 2$, а для двох інших виконується $\deg \operatorname{rad} A = \deg \operatorname{rad} B = 1$.

У цьому випадку справедливі умови:

$$\deg \operatorname{rad} \gcd(A,B) = \deg \operatorname{rad} \gcd(A,C) = \deg \operatorname{rad} \gcd(B,C) = 1$$

Тоді вказана нерівність зводиться до такої нерівності, як і в попередньому випадку:

$$\max\{\deg A, \deg B, \deg C\} > 2\deg h - 1.$$

Виходячи із розглянутих чотирьох випадків, бачимо, що у найгіршому випадку маємо нерівність

$$\max\{\deg A, \deg B, \deg C\} > 2\deg h - 1 = 2n - 1.$$

Оскільки степінь будь-якого елемента з множини S не перевищує $2n-2$, то остання нерівність завжди не виконується.

Виходячи із теореми 7.6 робимо висновок, що пари добутків із розглянутої множини S можуть бути рівними за модулем $h(x)=x^n+x+a$, а жодна трійка добутків – не може бути рівною за модулем $h(x)$. Це означає, що кількість різних добутків з цієї множини за модулем полінома $h(x)$ дорівнює в найгіршому випадку половині від загальної кількості добутків, тобто рівна наступній величині:

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

Таким чином, ми отримали межу, наведену в формулюванні цієї теореми. Теорему доведено.

На завершення підрозділу зауважимо, що можна додатково використати для посилення нижньої межі для порядку елементів поля $F_{q^n}=F_q[x]/(x^n+x+a)$ елементи вигляду

$$(\theta+b)^{q^t}=\theta^{q^t}+b,$$

де $t>\lfloor \log_q n \rfloor$. Наприклад, у випадку $q=3$, $n=100$, $t>4$ такими елементами, зокрема, є наступні елементи:

$$(\theta+b)^{3^5}=(\theta+a)^2\theta^{43}+b,$$
$$(\theta+b)^{3^6}=(\theta+a)^6\theta^{86}+b,$$
$$(\theta+b)^{3^7}=(\theta+a)^{20}\theta^{58}+b.$$

7.3. Елементи великого порядку при доведенні простоти чисел

Прості числа мають фундаментальне значення в математиці в цілому: є небагато краще відомих або легших для розуміння проблем у чистій 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 [23] представили детермінований поліноміальний алгоритм AKS, який визначає є вхідне число n простим чи складеним. Доведено [80], що AKS виконується за час $(\log n)^{7.5+o(1)}$. Х. Ленстра та Померанс [80] дали суттєво змінену версію AKS з часом виконання $(\log n)^{6+o(1)}$. Відомі також імовірнісні варіанти AKS [30] з часом виконання $(\log n)^{4+o(1)}$. Для подальшого покращення оцінки часу виконання було запропоновано таку гіпотезу [23]: якщо r – просте число, яке не ділить n, та якщо $(X-1)^n = X^n - 1 \,(\mathrm{mod}\, n, X^r - 1)$, то або n – просте або справедливе порівняння $n^2 \equiv 1 \,(\mathrm{mod}\, r)$.

Якщо ця гіпотеза, яку часто називають гіпотезою Агравала, виявиться справедливою, то це покращить оцінку часу виконання алгоритму AKS до $(\log n)^{3+o(1)}$. Наведена гіпотеза перевірена для значень цілих чисел $r < 100$ та $n < 10^{10}$ [23].

Х.Ленстра та Померанс [95] дали евристичний аргумент, який припускає, що наведена гіпотеза хибна. Проте, М.Агравал, Н.Кайал, Н.Саксена [23] зауважили, що певний варіант гіпотези може все ж бути вірним (наприклад, якщо покладаємо $r > \log n$). У даному підрозділі ми доводимо, що твердження Х.Ленстри з [95], яке припускає існування

багатьох контрприкладів для гіпотези Аггравала, є вірним у більш загальному випадку. Разом з тим, отримано строго зростаючий ланцюг підгруп мультиплікативної групи відповідного скінченного поля і сформульовано модифіковану гіпотезу про те, що множина з двох елементів породжує досить велику підгрупу цієї групи.

Далі аналізуємо , в чому полягає підґрунтя алгоритму AKS. Для $r \in N$, $\varphi(r)$ є функцією Ейлера, яка дає кількість чисел менших від r і взаємно простих з r. Легко бачити, що $\mathrm{ord}_r(a) \mid \varphi(r)$ ділить $\varphi(r)$ для будь-якого цілого числа a взаємно простого з r.

Нагадаємо, що коли число p – просте число та $h(X)$ – нерозкладний над $Z_p = F_p$ поліном степеня d, то $Z_p[X]/h(X)$ - скінченне поле із p^d елементів. Ми будемо використовувати позначення $f(X) = g(X)(\mathrm{mod}\, n, h(X))$ для подання рівняння $f(X) = g(X)$ в кільці $Z_n[X]/h(X)$. log позначатиме логарифм за основою 2.

В основі алгоритму AKS лежать такі міркування [23]. Нехай n – довільне натуральне число, для якого слід визначити: воно просте чи складене. Для цього перевіряємо рівності $(X+a)^n \equiv X^n + a$ в кільці $Z_n(X)/(X^r - 1)$ для чисел $a = 1,...,l$. Як степінь r полінома $X^r - 1$ вибираємо найменше r, що задовольняє умову $\mathrm{ord}_r(n) > \log^2 n$. Число рівностей, які перевіряємо, дорівнює $l = \lfloor \sqrt{\varphi(r)} \log n \rfloor$.

Припускаємо, що число n має нетривіальний простий дільник p. Розглядаємо підгрупу A групи Z_r^*, породжену елементами n та p. Нехай $|A| = t$. При подальших розглядах беремо наступний канонічний сюр'єктивний гомоморфізм

$$Z_n[X]/(X^r - 1) \to Z_p[X]/h(X),$$

де $h(X)$ – нерозкладний над Z_p дільник $X^r - 1$, та ототожнюємо елементи $X + a$, $a = 0,...,l$, з кільця $Z_n[X]/(X^r - 1)$ та їх образи при цьому гомоморфізмі в полі $Z_p[X]/h(X)$. Крім підгрупи A також беремо підгрупу G мультиплікативної групи $U = (Z_p[X]/h(X))^*$, породжену множиною елементів $X + a$, $a = 0,...,l$. Оскільки $l < t < \varphi(r)$, то утворюючи добутки щонайбільше $l+1$ поліномів виду $X + a$ та показуючи, що вони різні в U, ми отримуємо нижню границю $|G| \geq 2^{l+1}$.

Якщо n не є степенем p, можна отримати також верхню границю для $|G|$. З цією метою розглядаємо множину

$$I = \left\{ \left(\frac{n}{p} \right)^i p^j \mid 0 \leq i, j \leq \left\lfloor \sqrt{t} \right\rfloor \right\}.$$

Задана множина I містить $\left(\left\lfloor \sqrt{t} \right\rfloor + 1 \right)^2 > t$ різних чисел. Оскільки $|A| = t$, то принаймні два числа з I співпадають за модулем r: $\alpha \equiv \beta \bmod r$. Тоді справедливі такі порівняння:

$$(X + a)^\alpha \equiv X^\alpha + a \equiv X^\beta + a \equiv (X + a)^\beta.$$

Значить, для всіх твірних елементів $X + a$, $a = 0,...,l$, підгрупи G виконується рівність $(X + a)^{\alpha - \beta} = 1$. Так як кожен елемент підгрупи G можна записати у вигляді добутку цілих степенів твірних елементів, то вказана рівність виконується для всіх елементів з G. Оскільки мультиплікативна група $U = (Z_p[X]/h(X))^*$ скінченого поля циклічна, то її підгрупа G також циклічна. Вона має один твірний елемент, для якого справедлива наведена рівність. Це означає, що порядок цього елемента співпадає з $|G|$. Тоді, як наслідок теореми Лагранжа для скінченних груп, $|G|$ ділить $\alpha - \beta$. Отже, отримуємо наступний ланцюжок нерівностей:

$$|G| < \alpha - \beta < \alpha < \left(\frac{n}{p} \cdot p\right)^{\lfloor\sqrt{t}\rfloor} \le n^{\lfloor\sqrt{t}\rfloor}.$$

З іншого боку, так як $t > \log^2 n$, то

$$|G| \ge 2^{l+1} \ge 2^{\lfloor\sqrt{t}\log n\rfloor+1} > n^{\lfloor\sqrt{t}\rfloor},$$

і ми отримуємо суперечність з попередньою нерівністю.

Таким чином, ідея алгоритму AKS полягає в такому: показати, що множина елементів $X + a$ породжує "достатньо велику" підгрупу групи $(Z_p[X]/h(X))^*$. 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 з одного елемента $X - 1$, породжує достатньо велику підгрупу.

У даному підрозділі ми узагальнюємо твердження Х. Ленстри [95], яке показує, що множина $\{X-1\}$ дуже ймовірно не породжує достатньо велику підгрупу. Разом з тим ми показуємо, що ланцюг підгруп $\langle X\rangle \subset \langle X+1\rangle \subset \langle X-1\rangle \subset \langle X-1, X+2\rangle$ є строго зростаючим, і, виходячи з цього, формулюємо гіпотезу, що множина $\{X-1, X+2\}$ породжує достатньо велику підгрупу.

Нам буде надалі потрібний такий результат.

Лема 7.3. (1) *$n - p^i$ для будь-якого цілого i ділиться на $p-1$ тоді і тільки тоді, коли $p-1 \mid n-1$.*

(2) *$n - p^i$ для будь-якого цілого i ділиться на $p+1$ тоді і тільки тоді, коли $p+1 \mid n+1$.*

Доведення. (1) Справедлива рівність $n-p^i=(n-1)-(p^i-1)$. Оскільки $p-1 \mid p^i-1$, то $n-p^i$ ділиться на $p-1$ тоді і тільки тоді, коли $p-1 \mid n-1$.

(2) Справедлива рівність $n-p^i=(n+1)-(p^i+1)$. Оскільки $p+1 \mid p^i+1$, то $n-p^i$ ділиться на $p+1$ тоді і тільки тоді, коли $p+1 \mid n+1$.

Лему доведено.

Наведені далі дві теореми описують можливі підходи до побудови контрприкладів для гіпотези Агравала. 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

$$(X-1)^n = X^n-1 \,(\bmod n, X^r-1).$$

Доведення. Поліноми $X-1$ та $\Phi_r(X)=X^{r-1}+X^{r-2}+...+X+1$ взаємно прості в кільці поліномів $Z_n[X]$. Тому, щоб довести рівність $(X-1)^n = X^n-1 \,(\bmod n, X^r-1)$ досить довести, що

$$(X-1)^n = X^n-1 \,(\bmod n, \Phi_r(X)).$$

Згідно з китайською теоремою про залишки маємо такий ізоморфізм:

$$Z_n[X]/\Phi_r(X) \cong \prod_{i=1}^{k} Z_{p_i}[X]/\Phi_r(X).$$

Кожне фактор-кільце $R_i = Z_{p_i}[X]/\Phi_r(X)$ є полем, оскільки кожне просте число p_i примітивне за модулем r $(\mathrm{ord}_r(p_i) = p_i - 1)$, і, значить, поліном $\Phi_r(X)$ нерозкладний над $Z_{p_i}[X]$. Тобто досить довести рівність

$$(X-1)^n = X^n - 1 \,(\mathrm{mod}\, p_i, \Phi_r(X)) \qquad (7.6)$$

для кожного p_i.

За припущенням $n \equiv p_i^{a_i} (\mathrm{mod}\, 2r(p_i^{(r-1)/2} - 1))$ для деякого цілого числа a_i, і тому $n \equiv p_i^{a_i} (\mathrm{mod}\, r)$. Тоді $X^n \equiv X^{p_i^{a_i}}$ за модулем числа p_i і, отже, за модулем полінома $\Phi_r(X)$.

Оскільки R_i – поле, то виконується рівність

$$(X-1)^{p_i^{a_i}} \equiv X^{p_i^{a_i}} - 1 \,(\mathrm{mod}\, p_i, \Phi_r(X)). \qquad (7.7)$$

Так як число p_i – примітивне за модулем r, то $p_i^{r-1} \equiv 1 (\mathrm{mod}\, r)$ та $p_i^{(r-1)/2} \equiv -1 (\mathrm{mod}\, r)$ (бо r – просте число). Тоді $(X-1)^{p_i^{(r-1)/2}} \equiv X^{-1} - 1$ та $(X-1)^{p_i^{(r-1)/2}-1} \equiv -X^{-1}$ в полі R_i. Оскільки $(-X^{-1})^{2r} = 1$, то порядок $X-1$ в R_i ділить $2r(p_i^{(r-1)/2} - 1)$. За припущенням $n \equiv p_i^{a_i} (\mathrm{mod}\, 2r(p_i^{(r-1)/2} - 1))$ і тому $(X-1)^n \equiv (X-1)^{p_i^{a_i}}$.

Так як відповідно ліві та праві частини рівнянь (7.6), (7.7) співпадають і рівняння (7.7) виконується, то рівняння (7.6) також виконується. Теорему доведено.

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;*

(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) $p_i-1\,|\,n-1$ *для* $i=1,...,k$ *;*

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

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

Доведення. Парне число дільників p_i, які дорівнюють 2 або 3 за модулем 5, дають 1 або -1 за модулем 5. Дійсно, якщо $p_i(\mathrm{mod}\,5)\equiv 2$ та $p_j(\mathrm{mod}\,5)\equiv 2$, то $p_ip_j(\mathrm{mod}\,5)\equiv -1$. Якщо $p_i(\mathrm{mod}\,5)\equiv 2$ та $p_j(\mathrm{mod}\,5)\equiv 3$, то $p_ip_j(\mathrm{mod}\,5)\equiv 1$. Якщо $p_i(\mathrm{mod}\,5)\equiv 3$ та $p_j(\mathrm{mod}\,5)\equiv 3$, то $p_ip_j(\mathrm{mod}\,5)\equiv -1$.

Непарне число (принаймні три) дільників p_i, які дорівнюють 2 або 3 за модулем 5 дають 2 або 3 за модулем 5. Значить, $n^2\neq 1(\mathrm{mod}\,5)$. За теоремою 7.8 досить показати, що для кожного i існує таке ціле a_i, що рівність $n\equiv p_i^{a_i}(\mathrm{mod}\,10(p_i^2-1))$ справедлива.

Є два різних варіанти розкладу $10(p_i^2-1)$ на 4 попарно взаємно простих множники залежно від значення $p_i(\mathrm{mod}\,16)$:

- якщо $p_i(\mathrm{mod}\,16)\in\{3,11\}$, то $10(p_i^2-1)=5\cdot 16\cdot\frac{p_i-1}{2}\cdot\frac{p_i+1}{4}$;

- якщо $p_i(\mathrm{mod}\,16)\in\{5,13\}$, то $10(p_i^2-1)=5\cdot 16\cdot\frac{p_i-1}{4}\cdot\frac{p_i+1}{2}$.

В обидвох випадках досить показати існування такого цілого a_i, що рівність $n \equiv p_i^{a_i} (\mathrm{mod} 10(p_i^2 - 1))$ справедлива за модулем кожного дільника.

Розглянемо перший випадок.

Якщо $n \equiv p_i (\mathrm{mod} 5)$, то $a_i = 1$, $n \equiv p_i (\mathrm{mod} 16)$ за умовою (3) даної теореми 7.9, $n \equiv p_i (\mathrm{mod}(p_i - 1)/2)$ за лемою 7.3 та умовою (4), $n \equiv p_i (\mathrm{mod}(p_i + 1)/4)$ за лемою 7.3 та умовою (5).

Якщо $n \neq p_i (\mathrm{mod} 5)$, то $a_i = 3$ (оскільки $2 \equiv 3^3 \bmod 5$ та $3 \equiv 2^3 \bmod 5$), $n \equiv p_i^3 (\mathrm{mod} 5)$, $n \equiv p_i^3 (\mathrm{mod} 16)$ за умовою (3) ($11 \equiv 3^3 (\mathrm{mod} 16)$, $3 \equiv 11^3 (\mathrm{mod} 16)$, $13 \equiv 5^3 (\mathrm{mod} 16)$, $5 \equiv 13^3 (\mathrm{mod} 16)$), $n \equiv p_i^3 (\mathrm{mod}(p_i - 1)/2)$ за лемою 7.3 і умовою (4), $n \equiv p_i^3 (\mathrm{mod}(p_i + 1)/4)$ за лемою 7.3 та умовою (5).

У другому випадку доведення аналогічне.

Теорему доведено.

Зауваження 7.1. Теорема 7.9 також вірна у випадку, якщо умову (3) замінити на таку:

3') $p_1 (\mathrm{mod} 32) \in \{7,9,23,25\}$ та для $i = 2,...,k$ виконується: якщо $p_i \equiv p_1 (\mathrm{mod} 5)$, то $p_i \equiv p_1 (\mathrm{mod} 32)$, в іншому випадку $p_i \equiv p_1^3 (\mathrm{mod} 32)$.

Аналогічні умови можна записати, заміняючи 32 на більші степені двійки.

Зауваження 7.2. Порядок групи $(Z_{p_i}[X]/\Phi_r(X))^*$ дорівнює $(p_i^2 - 1)(p_i^2 + 1)$. Виконується умова $10 \mid p_i^2 + 1$. Порядок елемента $X - 1$ з теореми 7.9 в групі $(Z_{p_i}[X]/\Phi_r(X))^*$ ділить $10(p_i^2 - 1)$ для будь-якого простого дільника p_i натурального числа n.

Твердження Х.Ленстри з [95] є частковим випадком теореми 7.9. Згідно з теоремою 7.9 маємо евристику, яка припускає існування багатьох контрприкладів (див. [95]) для гіпотези Аграваля при $r = 5$. Виходячи з

теореми 7.8, можна будувати контрприклади також для $r > 5$. Проте ні один контрприклад поки що не знайдено.

Зокрема, гіпотезу перевірено в роботі [23] для малих чисел n та r.

Також гіпотезу перевірено нами з використанням комп'ютерних обчислень для випадку $r = 5$ та $10^{100} < n < 10^{100} + 10^{5}$ [119]. Программу реалізовано в середовищі Delphi 7.0 з використанням бібліотеки для роботи з великими цілими числами devlib (її можна вільно використовувати для наукових експериментів). Перевіряли лише числа n, для яких справедлива умова $n \bmod 5 \in \{2,3\}$. Якщо для такого числа виконувалася рівність, що описує гіпотезу Агравала, то перевіряли, чи є n простим числом. Як тест простоти взято реалізований T.Forbes алгоритм ARPL. Програма запам'ятовує до якого числа вона виконала перевірку і наступний раз продовжує від збереженого числа. При цьому у вказаному діапазоні знайдено 222 числа, для яких виявилася справедливою вказана рівність. Після цього для кожного з цих чисел було запущено тест простоти, який показав простоту випробовуваного числа. Наприклад, найменше з цих чисел дорівнює

N=1000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000267

*** N – просте число ! ,

а найбільше дорівнює

N=1000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000099457

*** N – просте число !

Оскільки, дуже ймовірно, гіпотеза Агравала не виконується, природно трохи змінити її, щоб отримати версію, яка все ще може бути справедливою. Наведені далі формулювання дозволяють пов'язати із гіпотезою Агравала певний ланцюг підгруп відповідної мультиплікативної групи скінченного поля. Описуємо отриманий ланцюг підгруп та його зв'язок з модифікованою

гіпотезою. Число n припускаємо примітивним за модулем r. Зауважимо, що елемент $X-1$ є одиницею в кільці $Z_p[X]/(\Phi_r(X))$.

Теорема 7.10. *Якщо*

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

то

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

строго зростаючий ланцюг підгруп групи $(Z_{p_i}[X]/\Phi_r(X))^*$ *для будь-якого простого дільника* p *числа* n.

Доведення. Оскільки маємо $(X-1)^n = X^n - 1\,(\mathrm{mod}\, n, X^r - 1)$, то вірне співвідношення $(X-1)^n = X^n - 1\,(\mathrm{mod}\, p, \Phi_r(X))$. Так як число n примітивне за модулем r, то існує таке натуральне число a, що $n^a \equiv 2\,(\mathrm{mod}\, r)$. Тоді $(X-1)^{n^a} = X^2 - 1 = (X-1)(X+1)$. Значить, $X+1 = (X-1)^{n^a-1} \in \langle X-1\rangle$ та $\langle X+1\rangle \subseteq \langle X-1\rangle$.

Так як $X+1 \in \langle X-1\rangle$ та $(X-1)^n = X^n - 1\,(\mathrm{mod}\, p, \Phi_r(X))$, то $(X+1)^n = X^n + 1\,(\mathrm{mod}\, p, \Phi_r(X))$.

Оскільки n примітивне за модулем r, існує таке натуральне число c, що $n^c \equiv r - 1(\mathrm{mod}\, r)$. Тоді

$$(X+1)^{n^c} = X^{n^c} + 1 = X^{r-1} + 1 = X^{-1} + 1 = X^{-1}(X+1).$$

Нагадаємо, що $X^r = 1$. Звідси, $(X+1)^{n^c-1} = X^{-1}(\mathrm{mod}\, p, C_r(X))$. Тоді $\langle X^{-1}\rangle \subseteq \langle X+1\rangle$. Оскільки групи $\langle X^{-1}\rangle$ та $\langle X\rangle$ співпадають, то $\langle X\rangle \subseteq \langle X+1\rangle$. Так як $\langle X\rangle = \{1, X, ..., X^{r-1}\}$, то зрозуміло, що $X+1 \notin \langle X\rangle$ та $\langle X\rangle \subset \langle X+1\rangle$.

Для доведення $\langle X+1\rangle \subset \langle X-1\rangle$ розглянемо автоморфізм σ кільця

$Z_p[X]/(\Phi_r(X))$, який відображає елемент X в X^{-1}. Припустимо, що $(X+1)^V = X-1 \pmod{p, \Phi_r(X)}$ для деякого цілого числа V. Скористаємось для $\alpha = (X+1)^V$ та $\beta = X-1$ тим фактом, що з $\alpha = \beta$ випливає $\alpha \cdot (\sigma(\alpha))^{-1} = \beta \cdot (\sigma(\beta))^{-1}$.

Зауважимо, що $X+1$ та $X-1$ є одиницями, і тому $[\sigma(X+1)]^{-1}$ та $[\sigma(X-1)]^{-1}$ існують. Маємо

$$(X+1)[\sigma(X+1)]^{-1} = (X+1)[X^{-1}(X+1)]^{-1} = X$$

та

$$(X-1)[\sigma(X-1)]^{-1} = (X-1)[-X^{-1}(X-1)]^{-1} = -X\ .$$

Тоді $X^V = -X$, і отримали суперечність.

Отже, ланцюг груп $\langle X \rangle \subset \langle X+1 \rangle \subset \langle X-1 \rangle$ є строго зростаючим. Теорему доведено.

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

Доведення. Припустимо, що $(X-1)^V = X + a \pmod{p, \Phi_r(X)}$. Знову розглянемо автоморфізм σ кільця $Z_p[X]/(\Phi_r(X))$, який переводить X в X^{-1}. Тоді отримуємо наступні три рівності:

$$(X+a)[\sigma(X+a)]^{-1} = (X-1)^V[\sigma((X-1)^V)]^{-1},$$

$$(X+a)[X^{-1}+a)]^{-1} = (-X)^V,$$

$$X + a = (-1)^V(-X)^{V-1} + (-1)^V aX^V\ .$$

Якщо $X = (-1)^V aX^V$, то $(-1)^V \neq a$, що неможливо. Тоді $X = (-1)^V X^{V-1}$, $V-1 \equiv 1 (\mathrm{mod}\, r)$, $V \equiv 2 (\mathrm{mod}\, r)$. З іншого боку $a = (-1)^V aX^V$, $V \equiv 0 (\mathrm{mod}\, r)$, і

маємо суперечність. Теорему доведено.

Виходячи з 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 така теорема.

Теорема 7.12. *Якщо просте число* p *не дорівнює* 2, 3, 5, 11, 19 *та* $p^2 \neq 1 \pmod 5$, *то порядок елемента* $X+2$ *в полі* $Z_p[X]/(\Phi_5(X))$ *не ділить* $10(p^2-1)$.

Доведення. Легко перевірити, що

$$(X+2)(X^3-X^2+3X-5) \equiv -11 \pmod{p, \Phi_5(X)},$$

тобто елемент $-11^{-1}(X^3-X^2+3X-5)$ є мультиплікативним оберненим для $X+2$ в полі

$$Z_p[X]/(\Phi_5(X)) = Z_p[X]/(X^4+X^3+X^2+X+1).$$

Маємо $(X+2)^{p^2} \equiv X^{-1}+2 = X^{-1}(2X+1)$ та

$$(X+2)^{p^2-1} \equiv -11^{-1}X^{-1}(2X+1)(X^3-X^2+3X-5) = \\ = -11^{-1}X^{-1}(-3X^3+3X^2-9X-7).$$

Тоді виконуються наступні порівняння:

$$(X+2)^{10(p^2-1)} \equiv 11^{-10}(-3X^3+3X^2-9X-7)^{10} \equiv$$

$$\equiv -11^{-10}(19486165920X^3+26683280040X^2+22802637960X+29275201379).$$

Розклад на прості множники коефіцієнтів полінома при ненульових степенях X є таким:

$$19486165920=2\cdot2\cdot2\cdot2\cdot2\cdot3\cdot5\cdot13\cdot19\cdot164357;$$
$$26683280040=2\cdot2\cdot2\cdot3\cdot5\cdot19\cdot167\cdot70079;$$
$$22802637960=2\cdot2\cdot2\cdot3\cdot3\cdot5\cdot19\cdot67\cdot49757.$$

Оскільки p не ділить найбільший спільний дільник коефіцієнтів (який дорівнює 2·2·2·3·5·19), то ці коефіцієнти одночасно не дорівнюють нулю за модулем числа p. Значить, поліном $(X+2)^{10(p^2-1)}$ не дорівнює 1. Теорему доведено.

Доведені теореми 7.10, 7.11 та 7.12 дозволяють припустити, що такий варіант гіпотези Аггравала може бути вірним:
якщо r *– просте число, яке не ділить* n,
якщо $(X-1)^n = X^n - 1 \pmod{n, X^r-1}$ *і якщо* $(X+2)^n = X^n + 2 \pmod{n, X^r-1}$,
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.

Використовуючи результати з розділу 3 далі отримуємо експоненційні нижні межі для порядків підгруп, пов'язаних з гіпотезою Аггравала, які утворюють такий ланцюг підгруп: $\langle\theta\rangle \subset \langle\theta+1\rangle \subset \langle\theta-1\rangle \subset \langle\theta-1, \theta+2\rangle$. При цьому вибираємо просте число r так, що для натурального числа n, яке хочемо тестувати на простоту, виконується умова $\mathrm{ord}_r n = r-1$. Очевидно, що тоді $\mathrm{ord}_r p = r-1$ хоча б для одного простого дільника p числа n. Також зрозуміло, що у цьому разі поліном $\Phi_r(x) = x^{r-1} + x^{r-2} + ... + x + 1$ нерозкладний над Z_p.

Таким чином, якщо покладемо $q = p$, то отримуємо конструкцію, розглянуту в розділі 3. Дійсно, q – примітивний корінь за модулем r, тобто мультиплікативний порядок q за модулем r дорівнює $r-1$, а кільце $F_q[x]/\Phi_r(x)$ є полем. Як і раніше, будемо притримуватися позначення $\theta = x \pmod{\Phi_r(x)}$.

Покладаємо до кінця підрозділу, що $q = p > 3$ – просте число та $r < p$. Очевидно, що $|\langle\theta\rangle| = r$.

Лема 7.4. *Справедлива така рівність для підгруп:*

$$\langle\theta+1\rangle = \langle\theta\rangle \times \langle\theta+\theta^{-1}\rangle.$$

Доведення. Покажемо спочатку, що $\langle\theta^2+1\rangle = \langle\theta+1\rangle$. Оскільки число p – примітивне за модулем r, то існує таке натуральне число i, що виконується умова $p^i \equiv 2 \bmod r$. Тоді $(\theta+1)^{p^i} = \theta^2+1 (\text{mod } p, \Phi_r(\theta))$. Аналогічно існує таке натуральне число j, що виконується порівняння $p^j \equiv 2^{-1} \bmod r$. Тоді маємо $(\theta^2+1)^{p^j} = \theta+1 (\text{mod } p, \Phi_r(\theta))$.

Тепер покажемо, що $\langle\theta\rangle \cdot \langle\theta+\theta^{-1}\rangle = \langle\theta^2+1\rangle$. Дійсно, $\theta(\theta+\theta^{-1}) = \theta^2+1$ і включення $\langle\theta\rangle \cdot \langle\theta+\theta^{-1}\rangle \supseteq \langle\theta^2+1\rangle$ очевидне. Так як $\theta \in \langle\theta+1\rangle = \langle\theta^2+1\rangle$, $\theta^{-1}(\theta^2+1) = \theta+\theta^{-1} \in \langle\theta^2+1\rangle$ і маємо включення $\langle\theta\rangle \cdot \langle\theta+\theta^{-1}\rangle \subseteq \langle\theta^2+1\rangle$.

Щоб довести, що перетин підгруп $\langle\theta\rangle$ та $\langle\theta+\theta^{-1}\rangle$ дорівнює тривіальній підгрупі, розглянемо автоморфізм σ поля $F_p(\theta)$, який переводить елемент θ в θ^{-1}. Для будь-якого $a \in F_p(\theta)$ беремо $t(a) = a \cdot (\sigma(a))^{-1}$. Зрозуміло, що t володіє властивостями: $t(ab) = t(a)t(b)$ та $t(a^i) = [t(a)]^i$. Тоді легко отримати $t((\theta+\theta^{-1})^u) = 1$ і $t(\theta^c) = \theta^{2c}$. Припустимо,

що $\theta^c = (\theta + \theta^{-1})^u$ для деяких натуральних чисел c, u. Скористаємось для $\alpha = \theta^c$ та $\beta = (\theta + \theta^{-1})^u$ тим фактом, що з $\alpha = \beta$ випливає $t(a) = t(b)$. Тоді $\theta^{2c} = 1$, а, значить, c ділиться на r та $\theta^c = 1$.

Отже, отримуємо бажану рівність для підгруп. Лему доведено.

Як наслідок леми 7.4, маємо наступний точніше визначений ланцюг підгруп:

$$\langle\theta\rangle \subset \langle\theta\rangle \times \langle\theta + \theta^{-1}\rangle = \langle\theta + 1\rangle \subset \langle\theta - 1\rangle \subset \langle\theta - 1, \theta + 2\rangle.$$

Таким чином, нами пов'язано із задачею тестування простоти великих натуральних чисел певний ланцюг підгруп мультиплікативної групи скінченного поля.

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

Враховуючи лему 7.4 та той факт, що згідно з наслідком 3.5, пункт (а) гауссовий період $\beta = \theta + \theta^{-1} = \theta^{-1}(\theta^2 + 1)$ має мультиплікативний порядок більший, ніж величина

$$\frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right)}{13(r-2)},$$

отримуємо такий наслідок.

Наслідок 7.1. *Виконується наступна нерівність:*

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

Оскільки маємо включення $\langle\theta+1\rangle \subset \langle\theta-1\rangle$, то наступний результат є очевидним.

Лема 7.5. *Справедлива така нерівність для порядків підгруп:*

$$|\langle\theta-1\rangle| \geq 2|\langle\theta+1\rangle|.$$

Зауваження 7.3. Порядок елемента $\theta+1$ у випадку $r=5$ та $p \equiv 2 \bmod r$ ділить число $2r(p+1)$, бо справедливі співвідношення:

$$(\theta+1)^{p+1} = (\theta^p+1)(\theta+1) = (\theta^2+1)(\theta+1) = \theta^3+\theta^2+\theta+1 = -\theta^4,$$

а порядок елемента $-\theta^4$ дорівнює $2r$. З іншого боку, можна показати, що $(\theta-1)^{2r(p+1)} \neq 1$.

Беручи до уваги наслідок 7.1 та лему 7.5, маємо таку нижню межу.

Наслідок 7.2. *Справедлива наступна нерівність:*

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

Тепер ми можемо отримати нижню межу для порядку підгрупи $\langle\theta-1,\theta+2\rangle$.

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

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

Доведення. Нагадаємо, що порядок групи $F^*_{p^{r-1}} = (F_q[x]/\Phi_r(x))^*$ дорівнює $p^{r-1}-1=(p^{(r-1)/2}-1)(p^{(r-1)/2}+1)$. Співмножники $p^{(r-1)/2}-1$ та $p^{(r-1)/2}+1$ мають найбільший спільний дільник рівний 2, оскільки їх сума дорівнює $2p^{(r-1)/2}$.

Розглянемо підгрупу групи $F^*_{p^{r-1}}$, породжену елементами $\theta-1$ та $\theta+2$. Ця підгрупа включає дві підгрупи: перша підгрупа породжена елементом $\beta=\theta+\theta^{-1}$ (бо $\langle\theta-1\rangle$ містить $\langle\theta+1\rangle$, а $\langle\theta+1\rangle$ містить $\langle\theta+\theta^{-1}\rangle$), а друга підгрупа породжена елементом $\gamma=(\theta-2)^{p^{(r-1)/2}-1}=(\theta^{-1}-2)(\theta-2)^{-1}$.

Згідно з наслідком 3.1 елемент β має порядок, який ділить величину $p^{(r-1)/2}-1$, а згідно з наслідком 3.5, пункт (a) цей порядок є принаймні величина

$$\frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right)}{13(r-2)}.$$

Так як $2^2\neq 1 \pmod p$, то згідно з теоремою 3.1, пункт (c) (якщо покласти $e=0$, $f=1$), елемент γ має порядок, який ділить $p^{(r-1)/2}+1$ і є принаймні $U((r-3)/2, p-1)$.

Визначимо наступним чином елемент

$$\delta=\begin{cases}\beta^2\gamma, \text{ якщо } \rho_2(p^{(r-1)/2}-1)=2\\ \beta\gamma^2, \text{ якщо } \rho_2(p^{(r-1)/2}+1)=2\end{cases}.$$

Очевидно, що підгрупа $\langle\theta-1,\theta+2\rangle$ включає підгрупу, породжену елементом δ. Якщо виконується умова $\rho_2(p^{(r-1)/2}-1)=2$, то число $(p^{(r-1)/2}-1)/2$ є непарним і взаємно простим з числом $p^{(r-1)/2}+1$. Зрозуміло, що мультиплікативний порядок елемента β^2 є дільником числа $(p^{(r-1)/2}-1)/2$. Таким чином, у цьому випадку, ми маємо наступний внутрішній прямий

добуток підгруп групи, породженої елементом $\theta-1$ та елементом $\theta+2$: $<\delta>=<\beta^2>\times<\gamma>$.

Якщо ж справедлива рівність $\rho_2(p^{(r-1)/2}+1)=2$, то число $(p^{(r-1)/2}+1)/2$ є непарним і взаємно простим з числом $p^{(r-1)/2}-1$. Очевидно, що мультиплікативний порядок елемента γ^2 є дільником числа $(p^{(r-1)/2}+1)/2$. Значить, у цьому разі, отримуємо такий внутрішній прямий добуток підгруп $<\delta>=<\beta>\times<\gamma^2>$.

Отже, в обидвох розглянутих випадках, порядок елемента δ дорівнює добутку мультиплікативних порядків елемента β та елемента γ, поділеним на число 2.

Оскільки виконується умова $(r-3)/2<p$, то маємо $U((r-3)/2, p-1)=U((r-3)/2)$. Застосовуючи до величини $U((r-3)/2)$ нерівність (2.3), отримуємо, що мультиплікативний порядок елемента δ задовольняє наступну нерівність:

$$\operatorname{ord}\delta \geq \frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right)}{13(r-2)}\cdot U((r-3)/2)/2>$$

$$>\frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot\sqrt{r-2}\right)}{13(r-2)}U((r-3)/2)/2>\frac{\exp\left(\pi\sqrt{\frac{2}{3}}\cdot(1+\frac{\sqrt{2}}{2})\sqrt{r-3}\right)}{169(r-2)(r-3)}.$$

Таким чином, отримуємо потрібний результат. Теорему доведено.

Зауважимо, що усі отримані в даному підрозділі нижні межі для порядків підгруп, пов'язаних з тестуванням простоти великого натурального числа n, залежать лише від числа r. Це число r вибираємо на початкових

кроках алгоритму й воно відоме при здійсненні тестування, і не залежать від гіпотетичного простого дільника p числа n, якого не знаємо.

7.4. Висновки до розділу

У даному розділі даємо нижню межу для мультиплікативного порядку деяких елементів у загальних розширеннях скінченних полів.

В першому підрозділі розглянуто побудову елементів великого порядку в скінченних полях загального вигляду на основі гіпотези Гао. У результаті отримано підсилення нижньої межі Гао-Конфлітті для мультиплікативного порядку елементів у скінченних полях загального вигляду.

У другому підрозділі з використанням наслідку з ABC теореми для поліномів побудовано елементи мультиплікативного великого порядку в скінченних полях загального вигляду, не спираючись на гіпотезу Гао.

Останній підрозділ присвячений вивченню зв'язку між елементами великого порядку та доведенням простоти великих натуральних чисел. Проаналізовано, що ідея поліноміального детермінованого алгоритму AKS тестування простоти полягає в такому: показати, що множина елементів, для яких виконують пробні обчислення, породжує "достатньо велику" підгрупу мультиплікативної групи відповідного скінченого поля. З цієї ж точки зору можна трактувати гіпотезу Аггравала в такий спосіб: множина, що складається з одного елемента, породжує достатньо велику підгрупу цієї групи. Доведено, що твердження Х. Ленстри, яке припускає існування багатьох контрприкладів для гіпотези Аггравала, є вірним у більш загальному випадку. Разом з тим, отримано строго зростаючий ланцюг підгруп мультиплікативної групи відповідного скінченного поля і сформульовано модифіковану гіпотезу про те, що множина з двох елементів породжує

досить велику підгрупу цієї групи. Використовуючи результати з третього розділу, отримано експоненційні нижні межі для порядків підгруп, які утворюють вказаний строго зростаючий ланцюг підгруп відповідної мультиплікативної групи.

Результати цього розділу опубліковано в роботах [11, 14, 20, 21, 110, 112, 115, 119, 124].

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.

В роботі одержано 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 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. У цій ситуації ефективним є запропонований метод комбінування двох підходів. Підсилено дану 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, 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.

Підсилено нижню межу 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 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 використаних джерел

[1] Варден Б. Л. ван дер. Алгебра / Б. Л. ван дер Варден. – М.: Наука, 1976. – 648 с.

[2] Глазунов Н.М. Вопросы развития алгебраических исследований с применением ЭВМ / Н.М. Глазунов, Л.А. Калужнин, А.А. Стогний, В.И. Сущанский // Кибернетика. – 1983. – № 2. – С. 1–10.

[3] Глазунов Н. М. Доказательство гипотезы Минковского о критическом определителе области |*x*|^*p* + |*y*|^*p* < 1 в окрестности *p*=2 / Н. М. Глазунов, А. В. Малышев // Доклади АН УССР. – 1986. – Серия А, № 7. – С. 8–11.

[4] Глазунов Н.М. Вычислительные эксперименты в арифметической геометрии над конечными полями и их компъютерная поддержка / Н. М. Глазунов, Ю.В. Капитонова // Кибернетика и системный анализ. – 2000. – № 4. – С. 12–25.

[5] Глазунов Н.М. О пространствах модулей, равнораспределенности, оценках и рациональных точках алгебраических кривых / Н.М. Глазунов // Укр. мат. журнал. – 2001. – Т.53, № 9. – С. 1174–1183.

[6] Дрозд Ю. А. Конечномерные алгебры / Ю. А. Дрозд, В. В. Кириченко – Київ: Вища школа, 1980. – 192 с.

[7] Попович Р. Елементи великого порядку в розширеннях Артіна-Шраєра скінченних полів / Р. Попович // Математичні студії. – 2013. – Т. 39, № 2. – С. 115–118.

[8] 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.

[9] Попович Р. Покращення нижньої оцінки для порядку елементів одного класу скінченних полів / Р. Попович // Математичний вісник НТШ. – 2013. – Т. 10. – С. 39–44.

[10] Попович Р. Про оцінки для мультиплікативних порядків елементів скінченних полів на основі циклотомічних поліномів / Р. Попович // Вісник Національного ун-ту “Львівська політехніка”, фіз.-мат. науки. – 2013. –№ 768. – С. 59–62.

[11] 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.

[12] 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. 120–126.

[13] 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.

[14] Попович Р. Про підгрупи мультиплікативної групи одного класу скінченних полів / Р. Попович // Вісник Національного ун-ту “Львівська політехніка”, фіз.-мат. науки. – 2014. –№ 804. – С. 108–111.

[15] Попович Р. Про ізоморфізм скінченних полів характеристики два / Р. Попович // Математичний вісник Наук. Товариства ім. Т. Шевченка – 2014. – Т. 11. – С. 12–20.

[16] 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.

[17] 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.

[18] 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.

[19] 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).

[20] Попович Р. Деякі зауваження відносно реалізації AKS тесту простоти / Р. Попович // Вісник Національного ун-ту "Львівська політехніка", комп'ютерні системи та мережі. – 2006. –№ 573. – С. 157–160.

[21] Попович Р. Удосконалення алгоритму AKS доведення простоти цілих чисел / Р. Попович // Вісник Національного ун-ту "Львівська політехніка", комп'ютерні системи та мережі. – 2007. –№ 603. – С. 112–116.

[22] 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.

[23] Agrawal M. PRIMES is in P / M. Agrawal, N. Kayal, N. Saxena // Annals of Mathematics. – 2004. – Vol. 160, no. 2. – P. 781–793.

[24] Andrews G. E. The theory of partitions / G. E. Andrews. – Encyl. of Math. and Its Appl., Vol. 2, London-Amsterdam-Don Mills-Sydney-Tokyo: Addison-Wesley, 1976. – 255 p.

[25] Arnault F. Construction of self-dual normal bases and their complexity / F. Arnault, E. J. Pickett, S. Vinatier // Finite Fields Appl. – 2012. – Vol. 18, no. 2. – P. 458-472.

[26] Ash D. W. Low complexity normal bases / D. W. Ash, I. F. Blake, S. A. Vanstone // Discrete Applied Mathematics – 1989. – Vol. 25, no. 3. – P. 191-210.

[27] Bach E. Comments on search procedures for primitive roots / E. Bach // Math. Comp. – 1997. – Vol. 66, no. 220. – P. 1719–1727.

[28] Benger N. Constructing tower extensions of finite fields for implementation of pairing-based cryprography / N. Benger, M. Scott // Proc. 3rd International Workshop on Arithmetic of Finite Fields, Istanbul, Turkey, June 27-30, 2010.– Lecture Notes in Computer Sciences, Vol. 6087, Springer, Berlin, 2010. – P. 180–195.

[29] Bernstein D. Sharper ABC-based bounds for congruent polynomials / D. Bernstein // J. Theor. Nombres de Bordeaux. – 2005. – Vol. 17, no. 3. – P. 721–725.

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

[31] Bernstein D.J. Type-II optimal polynomial bases / D.J. Bernstein, T. Lange // Proc. 3d Int. Workshop on Arithmetic of Finite Fields, Istanbul, Turkey, June 27-30, 2010.– Lecture Notes in Comput. Sci., Vol. 6087, Springer, Berlin, 2010. – P. 41–61.

[32] Berrizbeitia P. Sharpening Primes is in P for a large family of numbers / P. Berrizbeitia // Math. Comp. – 2005. – Vol. 74, no. 252. – P. 2043–2059.

[33] Beth T. Finding (good) normal bases in finite fields / T. Beth, W. Geiselmann, F. Meyer // Proc. Int. Symposium on Symbolic and Algebraic Computation – ACM, New York, NY, USA, 1991. – P. 173–178.

[34] Blake I. F. Specific irreducible polynomials with linearly independent roots over finite fields / I. F. Blake, S. Gao, R.C. Mullin // Linear Algebra Appl. – 1997. – Vol. 253, no. 1–3. – P. 227–249.

[35] Bruyn L. The-odd-knights-of-the-round-table [Електронний ресурс] / L. l Bruyn // 2010. – Режим доступу: http://www.neverendingbooks.org/the-odd-knights-of-the-round-table, http://www.neverendingbooks.org/seating-the-first-few-thousand-knights, http://www.neverendingbooks.org/seating-the-first-few-billion-knights.

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

[37] Car M. About the period of Bell numbers modulo a prime / M. Car, L. H. Gallardo, O. Rahavandrainy, L. N. Vaserstein // Bull. Korean Math. Soc. – 2008. – Vol. 45, no. 1. – P. 143–155.

[38] Carlitz L. Primitive roots in finite fields / L. Carlitz // Trans. Amer. Math. Soc. – 1952. – Vol. 73, no. 3. – P. 373–382.

[39] Carlitz L. Some problems involving primitive roots in a finite field / L. Carlitz // Proc. Nat. Acad. Sci. U.S.A. – 1952. – Vol. 38, no. 4. – P. 314–318.

[40] Carlitz L Distribution of primitive roots in a finite field, / L. Carlitz // Quart. J. Math. Oxford – 1953. – Vol. 4, no. 2. – P. 4–10.

[41] Castro F. N. Mixed exponential sums over finite fields. / F. N. Castro, C. J. Moreno // Proc. Amer. Math. Soc. – 2000. – Vol. 128, no. 9. – P. 2529–2537.

[42] Chang M.-C. Order of Gauss periods in large characteristic / M.-C. Chang // Tawanise J. Math. – 2013. – Vol. 17, no. 2. – P. 621–628.

[43] Chang M.-C. Elements of large order in prime finite fields / M.-C. Chang // Bull. Austral. Math. Soc. – 2013. – Vol. 88, no. 1. – P. 169–176.

[44] 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.

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

[46] Cheng Q. Constructing finite field extensions with large order elements / Q. Cheng // Proc. 15th ACM-SIAM Symp. on Discrete algorithms, New Orleans, LA, USA; 11–13 January 2004. – 2004. – P. 1123–1124.

[47] Cheng Q. Constructing high order elements through subspace polynomials /

Cheng Q., Gao S., Wan D. // Discrete algorithms: Proc. 23rd ACM-SIAM Symp. (Kyoto, Japan, 17–19 January 2012). – Omnipress, Philadelphia, USA, 2011 – P. 1457–1463.

[48] Christopoulou M. The trace of an optimal normal element and low complexity normal bases / M. Christopoulou, T. Garefalakis, D. Panario, D. Thomson // Des. Codes Cryptogr. – 2008. – Vol. 49, no. 1–3. – P. 199–215.

[49] Christopoulou M. Gauss periods as constructions of low complexity normal bases / M. Christopoulou, T. Garefalakis, D. Panario, D. Thomson // Des. Codes Cryptogr. – 2012. – Vol. 62, no. 1. – P. 43–62.

[50] Clausen M. On zero testing and interpolation of k-sparse multivariate polynomials over finite field / M. Clausen, A. Dress, J. Grabmeier, M. Karpinski // Theor. Comp. Sci. – 1991. – Vol. 84, no. 3. – P. 151–164.

[51] Cochrane T. Using Stepanov's method for exponential sums involving rational functions. / T. Cochrane, C. Pinner // J. Number Theory. – 2006. – Vol. 116, no. 2. – P. 270–292.

[52] Cohen S.D. Primitive roots in the quadratic extension of a finite field. / S.D. Cohen // J. London Math. Soc. – 1983. – Vol. 27, no. 2. – P. 221–228.

[53] 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.

[54] Cohen S.D. Consecutive primitive roots in a finite field II. / S.D. Cohen // Proc. Amer. Math. Soc. – 1985. – Vol. 94, no. 2. – P. 605–611.

[55] Cohen S.D. Primitive elements in finite fields and Costas arrays. / S.D. Cohen, G.L. Mullen // App. Alg. Engr. Comm. Comp. – 1992. – Vol. 2, no. 1. – P. 45–53.

[56] Cohen S.D. Primitive elements on lines in extensions of finite fields / S.D. Cohen // Proc. 9th Int. Conf. (Ireland, 13-17 July 2009). – Contemporary Mathematics, v. 518, Finite fields. Theory and applications, Amer. Math. Soc., Providence, RI, 2010. – P. 113–127.

[57] Cohen S.D. Primitive normal bases with prescribed trace / S.D. Cohen,

D. Hachenberger // App. Alg. Engr. Comm. Comp. – 1999. – Vol. 9, no. 5. – P. 383–403.

[58] Cohen S.D. Gauss sums and a sieve for generators of Galois fields / S.D. Cohen // Publ.Math. Debrecen. – 2000. – Vol. 56, no. 2–3. – P. 293–312.

[59] 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.

[60] Cohen S. D. The strong primitive normal basis theorem / S. D. Cohen, S. Huczynska // Acta Arith. – 2010. – Vol. 143, no. 4. – P. 299–332.

[61] Conflitti A. On elements of high order in finite fields / A. Conflitti // Cryptography and computational number theory: Proc. Workshop (Singapore, 22-26 November 1999). – Birkhauser, Basel, 2001. – P. 11–14.

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

[63] Conway J. H. Lexicographic codes: error-correcting codes from game theory / J. H. Conway, N. J. A. Sloane // IEEE Trans. Inform. theory – 1986. – Vol. 32, no. 3. – P. 337–348.

[64] Crandall R. Prime Numbers, A Computational Perspective / R. Crandall, C. Pomerance. – New York: Springer-Verlag, 2005. – 596 p.

[65] Dadayan Z. Divisor function $\tau_3(\omega)$ weighted by Kloosterman sum / Z. Dadayan, S. Sergeev, P. Varbanets // Int. J. Pure Appl. Math. – 2013. – Vol. 89, no. 5. – P. 731–741.

[66] Davenport H. On primitive roots in finite fields / H. Davenport // Quart. J. Math. Oxford – 1937. – Vol. 8. – P. 308–312.

[67] Davenport H. Bases for finite fields / H. Davenport // J. London Math. Soc. – 1968. – Vol. 43, no. 1. – P. 21–39.

[68] Fan S. Primitive normal polynomials with multiple coeficients prescribed: an asymptotic result / S. Fan, W. Han, K. Feng // Finite Fields Appl. – 2007. – Vol. 13, no. 4 – P. 1029–1044.

[69] Fan S. Primitive normal polynomials with a prescribed coeficient / S. Fan, X. Wang // Finite Fields Appl. – 2009. – Vol. 15, no. 6. – P. 682–730.

[70] Gao S. Optimal normal bases / S. Gao, H.W. Lenstra // Des. Codes Cryptogr. – 1992. – Vol. 2, no. 4. – P. 315–323.

[71] Gao S. Dickson Polynomials and Irreducible Polynomials over Finite Fields / S. Gao, G.L. Mullen // J. Number Theory – 1994. – Vol. 49, no. 1. – P. 118–132.

[72] Gao S. On Orders of Optimum Normal Basis Generators / S. Gao, S.A. Vanstone // Math. Comp. – 1995. – Vol. 64, no. 211. – P. 1227–1233.

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

[74] Gao S. Gauss periods and fast exponentiation in finite fields / S. Gao, J. von zur Gathen, D. Panario // LATIN' 95: Theoretical Informatics. Proc. Second Latin American Symposium, Valparaiso, Chile, April 1995 – Lecture Notes in Comput. Sci., Vol. 911, Springer, Berlin, 1995. – P. 311–322.

[75] Gathen J. Orders of Gauss periods in finite fields / J. von zur Gathen, I.E. Shparlinski // Proc. 6th Intern. Symp. on Algorithms and Computation, Cairns, Australia, December 4–6, 1995. – Lecture Notes in Comput. Sci., Vol. 1004, Springer, Berlin, 1995. – P. 208–215.

[76] 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.

[77] Gathen J. Constructing elements of large order in finite fields / J. von zur Gathen, I. E. Shparlinski // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes – Lecture Notes in Comput. Sci., Vol. 1719, Springer, Berlin, 1999, – P. 404–409.

[78] Gathen J. Gauss periods in finite fields / J. von zur Gathen, I. E. Shparlinski // Proc. 5th Conf. of Finite Fields and their Applications, Augsburg, 1999 – Springer, 2001, – P. 162-177.

[79] Giudici R. E. A geometric characterization of the generators in a quadratic extension / R. E. Giudici, C. Margaglio // Rend. Sem. Mat. Univ. Padova – 1980. – Vol. 62. – P. 103–114.

[80] Granville A. It is easy to determine whether a given integer is prime / A. Granville // Bull. Amer. Math. Soc. – 2005. – Vol. 42, no. 1. – P. 3–38.

[81] Hagis P. A problem on partitions with a prime modulus $p \geq 3$ / P. Hagis // Trans. Amer. Math. Soc. – 1962. – Vol. 102, no. 1. – P. 30–62.

[82] Heath-Brown D. R. Artin's conjecture for primitive roots / D. R. Heath-Brown // Quart. J. Math. – 1986. – Vol. 37, no. 2 – P. 27–38.

[83] Hooley C. On Artin's conjecture / C. Hooley // J. Reine Angew. Math. – 1967. – Vol. 225. – P. 209–220.

[84] Hsu C. A generalization of the primitive normal basis theorem / C. Hsu, T. Nan // J. Number Theory – 2011. – Vol. 131, no. 1 – P. 146–157.

[85] Huang M.-D. Finding primitive elements in finite fields of small characteristic / M.-D. Huang, A.K. Narayanan // Proc. 11th Int. Conf. Finite Fields and their Applications, July 22-26, 2013, Magdeburg, Germany – Contemporary Mathematics, Vol. 632, Topics in Finite Fields, American Mathematical Society, Providence, Rhode Island, 2015.– P. 215–228.

[86] Ito H. On the construction of huge finite fields / H. Ito, H. Song // Proc. Algebra and Computation 2009, December 2–4, 2009, Tokyo Metropolitan University, Japan. – 2009. – P. 1–7.

[87] Ito H. A Tower of Artin-Schreier extensions of finite fields and its applications / H. Ito, T. Kajiwara, H. Song // JP J. of Algebra, Number Theory and Applications – 2011. – Vol. 22, no. 2. – P. 111–125.

[88] Jungnickel D. A On the Number of Self-Dual Bases of $GF(q^m)$ over $GF(q)$ / D. Jungnickel, A. Menezes, S. Vanstone // Proc. Amer. Math. Soc. – 1990. – Vol. 109, no. 1. – P. 23–29.

[89] Kapetanakis G. An extension of the (strong) primitive normal basis theorem / G. Kapetanakis // Appl. Algebra Engrg. Comm. Comput. – 2014. – Vol. 25. – P. 311–337.

[90] Kapetanakis G. Normal bases and primitive elements over finite fields / G. Kapetanakis // Finite Fields Appl. – 2014. – Vol. 26. – P. 123–143.

[91] Lambe T. A. Bounds on the Number of Feasible Solutions to a Knapsack Problem / T. A. Lambe // SIAM Journal on Applied Mathematics. – 1974. – Vol. 26, no. 2. – P. 302–305.

[92] Lang S. Algebra / S. Lang. – Graduate Texts in Mathematics, Vol. 211, New York: Springer-Verlag, 2002. – 866 p.

[93] Lazebnik F. A new series of dense graphs of high girth / F. Lazebnik, V. Ustimenko, A.J. Woldar // Bull. Amer. Math. Soc. – 1996. – Vol. 32, no. 1. – P. 73–79.

[94] Lenstra H.W. Nim multiplication / H. W. Lenstra // Seminaire de Théorie des Nombres de Bordeaux – 1977-1978. – Vol. 48, no. 7 – P. 1–24.

[95] Lenstra H.W. Remarks on Agrawal's conjecture / H.W. Lenstra, C. Pomerance // Advancing Research Computing on Campuses workshop: Future directions in algorithmic number theory , Palo Alto, USA, March 24-28, 2003. − American Institute of Mathematics, 2003, − P. 30−32.

[96] Lenstra H.W. Primitive normal bases for finite fields / H. W. Lenstra, R. J. Schoof // Math. Comp. – 1987. – Vol. 48, no. 177 – P. 217–231.

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

[98] Maroti A. On elementary lower bounds for the partition function / A. Maroti // Integers: Electronic J. Comb. Number Theory – 2003. –no. 3. – A10.

[99] Menezes A. Handbook of Applied Cryptography / A. Menezes, P. Van Oorschot, S. Vanstone. – London: CRC Press, 1996. – 794 p.

[100] Mills D. Primitive Roots in Cubic Extensions of Finite Fields / D. Mills, G. McNay // Finite Fields with Applications to Coding Theory,

Cryptography and Related Areas: Proc. 6th Int. Conf. Finite Fields and Applications, Oaxaca, México, May 21–25, 2001. – Springer, Berlin, 2002. – P.239–250.

[101] Montgomery P. L. The period of the Bell numbers modulo a prime / P. L. Montgomery, S. Nahm, S. S. Wagstaff Jr. // Math. Comp. – 2010. – Vol. 79, no. 271. – P. 1793–1800.

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

[103] Mullen G. L. Open problems and conjectures in finite fields / G. L. Mullen, I. E. Shparlinski // Finite Fields and Applications, Vol. 233 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 1996. – P. 243–268.

[104] Mullin R.C. Optimal normal bases in GF(p^n) / R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone, R.M.Wilson // Discrete Appl. Math. – 1988-1989. – Vol. 22, no. 2. – P. 149–161.

[105] Panario D. Efficient pth root computations in finite fields of characteristic p / D. Panario, D. Thomson // Des. Codes Cryptogr. – 2009. – Vol. 50, no. 3. – P. 351–358.

[106] Perel'muter G. I. Estimate of a sum along an algebraic curve / G. I. Perel'muter // Mat. Zametki. – 1969. – Vol. 5, no. 3. – P. 373–380.

[107] Pincin A. Bases for finite fields and a canonical decomposition for a normal basis generator / A. Pincin // Comm. Algebra. – 1989. – Vol. 17, no. 6. – P. 1337–1352.

[108] Popovych R. Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$ / R. Popovych // Finite Fields and Their Applications – 2013. – Vol. 19, no. 1. – P. 86–92.

[109] Popovych R. Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$ / R. Popovych // Finite Fields and Their Applications – 2012. – Vol. 18, no. 4. – P. 700–710.

[110] 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.

[111] 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.

[112] 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.

[113] 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.

[114] 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.

[115] 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.

[116] 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.

[117] 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.

[118] 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.

[119] Popovych R. On Agrawal conjecture / R. Popovych, B. Popovych // International Conference dedicated to 120th anniversary of S. Banach International Conference on Algebra dedicated to 100th anniversary of S.M. Chernikov (17–21 вересня 2012 р., Львів): зб. тез доп. – Львів, 2012. – С. 261.

[120] 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.

[121] 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.

[122] 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.

[123] 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.

[124] 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.

[125] Prachar K. Primzahlverteilung (Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete) / K. Prachar. – Berlin: Springer, 1957. – 415 s.

[126] Raievska M. On local near-rings with Miller-Moreno multiplicative group / M. Raievska, Ya. P. Sysak // Ukrainian Math. J. – 2012. – Vol. 64, no. 6. – P. 930–937.

[127] Raievska I. Finite local nearrings on metacyclic Miller–Moreno p-groups / I. Raievska, Ya. P. Sysak // Algebra Discrete Math. – 2012. – Vol. 13, Issue 1. – P. 111–127.

[128] Schleicher D. An introduction to Conway's games and numbers / D. Schleicher, M. Stoll // Mosc. Math. J. – 2006. – Vol. 6, no. 2. – P. 359–388.

[129] Shoup V. Searching for primitive roots in finite fields / V. Shoup // Math. Comp. – 1992. – Vol. 58, no. 197. – P. 369–380.

[130] Shparlinski I. E. On finding primitive roots in finite fields / I. E. Shparlinski // Theoret. Comput. Sci. – 1996. – Vol. 157, no. 2. – P. 273–275.

[131] Shparlinski I. E. Finite fields: theory and computation / I. E. Shparlinski. – Dordrecht: Kluwer Academic Publichers, 1999.

[132] Stănică P. Good lower and upper bounds on binomial coefficients / P. Stănică // Journal Inequalities Pure Applied Mathematics. – 2001. – Vol. 2, no. 3. – Article 30.

[133] Tian T. Primitive normal element and its inverse in finite fields / T. Tian, W. F. Qi // Acta Math. Sinica – 2006. – Vol. 49, no. 3. – P. 657–668.

[134] Ustimenko V. On the varieties of parabolic subgroups, their generalisations and combinatorial applications / V. Ustimenko // Acta Applicandae Mathematicae. – 1998. – Vol. 52, no. 1. – P. 223–238.

[135] Ustimenko V. Graphs with special arcs and cryptography / V. Ustimenko // Acta Applicandae Mathematicae. – 2002. – Vol. 74, no. 2. – P. 117–153.

[136] Ustimenko V. Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography / V. Ustimenko // Journal of Mathematical Sciences. – 2007. – Vol. 140, no. 3. – P. 412–434.

[137] Ustimenko V. On the extremal graph theory for directed graphs and its cryptographical applications / V. Ustimenko // Advances in Coding Theory and

Cryptography, World Scientific, Series on Coding and Cryptology, Vol. 3, 2007. – P. 181–200.

[138] Ustimenko V. Algebraic graphs and security of digital communications / V. Ustimenko. – Institute of Computer Science, University of Maria Curie Sklodowska in Lublin, 2011. – 151 p.

[139] Varbanets P. Divisors of the Gaussian Integers in an Arithmetic Progression / P. Varbanets, P. Zarzycki // J. Number Theory. – 1989. – Vol. 33, no. 2. – P. 152–169.

[140] Varbanets P. On divisor function over Z[i] / P. Varbanets, S. Varbanets // Annales University Sci. Budapest, Section of Computing – 2007. – Vol. 27. – P. 75–90.

[141] Varbanets P. Generalizations of Inversive Congruential Generator / P. Varbanets, S. Varbanets // Analytic and Probabilistic Methods in Number Theory: Proc. of the International Conference in Honour of J. Kubilius, Palanga, Lithuania, 4-10 September 2011. – 2012. – P. 265–282.

[142] Varbanets P. Linear inversive generator of PRN's / P. Varbanets, S. Varbanets // 8th International Algebraic Conference in Ukraine (5–12 липня 2011 р., Луганськ): зб. тез доп. – Луганськ, 2011. – С. 84.

[143] Voloch J. F. On the order of points on curves over finite fields / J. F. Voloch // Integers: Electronic J. Comb. Number Theory – 2007. –no. 7. – A49.

[144] Voloch J. F. Elements of high order on finite fields from elliptic curves / J. F. Voloch // Bull. Australian Math. Society – 2010. – Vol. 81, no. 3. – P. 425–429.

[145] Voloch J. F. On some subgroups of the multiplicative group of finite rings / J. F. Voloch // J. Theor. Nombres de Bordeaux. – 2004. – Vol. 16, no. 1. – P. 233–239.

[146] Wagstaff S. Jr. Aurifeuillian factorizations and the period of the Bell numbers modulo a prime / S. Wagstaff Jr. // Math. Comp. – 1996. – Vol. 65, no. 213. – P. 383–391.

[147] Wang P. On the existence of some specific elements in finite fields of characteristic 2 / P. Wang, X. Cao, R. Feng // Finite Fields Appl. – 2012. – Vol. 18, no. 4. – P. 800–813.

[148] Wang Y. On the least primitive root of a prime / Y. Wang // Sci. Sinica. – 1961. – Vol. 10. – P. 1–14.

[149] Werther K. The complexity of sparse polynomials interpolation over finite fields / K. Werther // Appl. Algebra Engrg. Comm. Comput.– 1994. – Vol. 5, no. 2 – P. 91–103.

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