

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ЧЕРКАСЬКИЙ
ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова праця
на правах рукопису

Халявка Віктор Володимирович

ДИСЕРТАЦІЯ

МЕТОДИ ВИБОРУ ПАРАМЕТРІВ СКІНЧЕННИХ ПОЛІВ МАТРИЦЬ
ДРУГОГО ПОРЯДКУ ТА ЇХ ПРИМІТИВНИХ ЕЛЕМЕНТІВ ДЛЯ
КРИПТОГРАФІЧНИХ ЗАСТОСУВАНЬ У КОМП'ЮТЕРНИХ СИСТЕМАХ І
МЕРЕЖАХ

123 – Комп'ютерна інженерія

Подається на здобуття ступеня доктора філософії

Дисертація містить результати
власних досліджень. Використання
ідей, результатів і текстів інших
авторів мають посилання на
відповідне джерело

В.В. ХАЛЯВКА

Науковий керівник:

Фауре Еміль Віталійович

доктор технічних наук, професор

Черкаси – 2026

АНОТАЦІЯ

Халявка В.В. Методи вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для криптографічних застосувань у комп'ютерних системах і мережах. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія. – Черкаський державний технологічний університет, Черкаси, 2026.

Дисертацію присвячено розв'язанню актуального науково-прикладного завдання, що полягає в розробленні методів вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для подальшого використання в криптографічних протоколах комп'ютерних систем і мереж. Актуальність теми зумовлена постійним зростанням обсягів інформації, що передається, обробляється та зберігається в електронному вигляді, а також підвищенням вимог до криптографічної стійкості засобів захисту даних в умовах розвитку розподілених обчислювальних середовищ, хмарних сервісів, мобільних мереж, вбудованих систем та Інтернету речей. За таких умов особливого значення набуває побудова нових математичних платформ для криптографії, які, з одного боку, спираються на строгий алгебраїчний апарат, а з іншого – дають змогу розширити простір криптографічних параметрів і підвищити обчислювальну складність несанкціонованого відновлення ключової інформації.

У сучасній комп'ютерній криптографії скінченні поля є фундаментом багатьох класичних і сучасних алгоритмів, зокрема протоколів узгодження ключів, схем електронного цифрового підпису, симетричних шифрів та механізмів автентифікації. Водночас подальший розвиток криптографічних засобів потребує пошуку таких алгебраїчних конструкцій, які б дозволяли використовувати нові типи елементів і операцій без втрати математичної строгості. Одним із перспективних напрямів є використання матричних структур над простими полями. Проте практична цінність такого підходу

визначається не лише самим фактом використання матриць, а насамперед можливістю конструктивно обирати параметри відповідного матричного середовища та примітивні елементи, придатні для побудови криптографічних перетворень. Саме цій задачі й присвячено дисертаційне дослідження.

Об'єктом дослідження є процеси вибору параметрів скінченних полів матриць другого порядку та примітивних елементів у цих полях для криптографічного використання в комп'ютерних системах і мережах.

Предметом дослідження є методи, моделі та алгоритми вибору параметрів скінченних полів матриць другого порядку, пошуку їх примітивних елементів, а також способи використання отриманих результатів у криптографічних протоколах узгодження ключів і електронного цифрового підпису.

Метою дисертаційної роботи є підвищення криптографічної стійкості засобів захисту інформації в комп'ютерних системах і мережах за рахунок розроблення методів вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів, придатних для реалізації криптографічних протоколів. Для досягнення поставленої мети в роботі розв'язано такі основні завдання: проведено аналіз сучасного стану використання скінченних полів і матричних структур у криптографічних застосуваннях; визначено умови, яким мають задовольняти параметри матричних полів для їх практичного криптографічного використання; розроблено метод вибору примітивних елементів скінченних полів матриць другого порядку; розроблено метод вибору параметрів матричного поля та примітивного елемента в ньому; удосконалено реалізацію криптографічних протоколів узгодження ключів і електронного цифрового підпису шляхом перенесення відповідних операцій у матричне середовище; виконано дослідження статистичних властивостей і обчислювальної складності запропонованих рішень.

У дисертації показано, що задача вибору примітивних елементів у скінченних полях матриць другого порядку не може ефективно розв'язуватися

повним перебором усіх елементів, оскільки такий підхід є обчислювально витратним і малопридатним для практичних криптографічних застосувань. У зв'язку з цим розроблено метод вибору примітивних елементів, який базується на послідовній перевірці характеристик матриці-кандидата, аналізі її характеристичного полінома, умов досягнення максимального періоду та перевірці порядку визначника в базовому полі. Запропонований підхід дозволяє конструктивно формувати повну множину примітивних елементів без необхідності прямого перебору всіх можливих матриць. Такий результат має важливе прикладне значення, оскільки саме примітивні елементи є генераторами мультиплікативної групи та можуть бути використані як базові параметри у схемах узгодження ключів і підпису.

Сутність розробленого методу полягає в тому, що для матриці-кандидата аналізуються її інваріантні характеристики, зокрема слід, визначник, а також дискримінант характеристичного полінома. На цій основі визначається, чи може така матриця бути кандидатом на примітивний елемент у відповідному матричному полі. Якщо для мультиплікативної групи порядок дорівнює $p^2 - 1$, то примітивний елемент повинен мати саме цей порядок. Для цього в роботі використано критерії, що зводять завдання перевірки примітивності до аналізу періоду матриці та порядку її визначника в базовому полі \mathbb{Z}_p . Такий підхід дозволяє перейти від загальної постановки завдання до ефективної обчислювальної процедури.

Значну увагу приділено завданню одночасного вибору параметрів матричного поля та примітивного елемента в ньому. На відміну від традиційного підходу, коли спочатку фіксуються параметри поля, а потім окремо здійснюється пошук примітивних елементів, запропонований метод поєднує ці дві процедури. Це дозволяє отримувати параметри матричного поля й примітивний елемент у межах єдиної конструктивної схеми. Метод ґрунтується на використанні властивостей квадратичних лишків і нелишків у простому полі, аналізі нерозкладності характеристичного полінома, а також

урахуванні зв'язку між параметрами матриці та властивостями її власних значень. Виділено спеціальний важливий випадок, коли порядок мультиплікативної групи має сприятливу факторизацію, зокрема пов'язану з числами Мерсенна або простими множниками спеціального вигляду, а також досліджено загальний випадок вибору параметрів.

Наукова новизна одержаних результатів полягає в тому, що вперше розроблено та теоретично обґрунтовано методи вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для криптографічних застосувань у комп'ютерних системах і мережах. Уперше запропоновано цілісний підхід, у межах якого задача вибору параметрів матричного поля поєднується із задачею вибору генератора його мультиплікативної групи. Представлено підходи до використання матричних алгебраїчних структур у протоколах узгодження ключів Діффі–Хеллмана та електронного цифрового підпису Ель-Гамала.

Практичне значення одержаних результатів полягає в тому, що розроблені методи можуть бути безпосередньо використані під час створення програмних і апаратних засобів криптографічного захисту інформації. Запропоновані алгоритмічні процедури дають змогу формувати параметри матричного поля та відповідні примітивні елементи для подальшого застосування в протоколах узгодження ключів, схемах електронного цифрового підпису, а також в інших криптографічних механізмах, що базуються на складності дискретного логарифмування. У роботі показано, що перенесення обчислень із класичного скалярного середовища до матричного дає змогу розширити множину допустимих криптографічних параметрів і створює передумови для підвищення криптографічної стійкості без принципового ускладнення базових арифметичних операцій. Одержані результати можуть бути використані в системах захищеного мережевого обміну, вбудованих пристроях, IoT-рішеннях, а також у спеціалізованих програмно-апаратних комплексах захисту інформації.

У дисертації наведено приклади практичного застосування розроблених методів. Зокрема, досліджено реалізацію протоколу узгодження ключів у матричному середовищі, де відкриті та секретні параметри задаються елементами відповідного матричного поля. Розглянуто перенесення схеми електронного цифрового підпису Ель-Гамала на випадок використання примітивних елементів скінченних полів матриць другого порядку. Показано, що в такому підході зберігається загальна логіка класичних криптографічних схем, але при цьому використовується ширший клас алгебраїчних об'єктів. Це відкриває можливість побудови нових модифікацій криптографічних протоколів, у яких параметри можуть бути додатково варійовані за рахунок матричного подання.

Окрему увагу приділено дослідженню статистичних властивостей піднесення матриці до степеня та аналізу обчислювальної складності криптографічних перетворень у матричному полі. У роботі виконано порівняння запропонованих рішень із класичними реалізаціями над простим полем, проаналізовано вплив параметрів поля на кількість можливих примітивних елементів, а також показано, що коректний вибір параметрів має вирішальне значення для досягнення необхідного рівня криптографічної стійкості. Отримані результати підтверджують, що матричні поля можуть бути не лише теоретичною моделлю, а й практично придатною основою для розроблення криптографічних засобів.

Результати дисертаційної роботи мають значення для подальшого розвитку математичного апарату криптографії та для створення нових підходів до побудови захищених систем передавання, зберігання та автентифікації інформації. Запропоновані методи забезпечують можливість систематичного вибору параметрів і примітивних елементів у матричних полях другого порядку та створюють наукове підґрунтя для подальших досліджень у напрямі вдосконалення асиметричних криптографічних протоколів, орієнтованих на використання спеціальних алгебраїчних структур. Практична орієнтованість одержаних результатів полягає в їх

придатності до програмної реалізації, формалізації у вигляді алгоритмів та інтеграції в реальні системи захисту інформації.

Основні результати дисертаційної роботи оприлюднено в 5 наукових публікаціях, серед яких 2 статті у виданнях, що індексуються в Scopus та/або Web of Science (одна з них у квартилі Q2), а також 3 доповіді на міжнародних науково-практичних конференціях. Це підтверджує апробацію основних положень дисертації та науковий інтерес до отриманих результатів.

Ключові слова: кібербезпека, комп'ютерні системи, комп'ютерні мережі, криптографічний протокол, скінченне поле, матриця другого порядку, примітивний елемент, параметри поля, узгодження ключів, електронний цифровий підпис, дискретний логарифм, криптографічна стійкість.

SUMMARY

Khaliavka V.V. Methods for Selecting the Parameters of Finite Fields of Matrices of Order 2 and Their Primitive Elements for Cryptographic Applications in Computer Systems and Networks – Qualifying research work (manuscript).

Dissertation submitted for the degree of Doctor of Philosophy in Specialty 123 Computer Engineering. Cherkasy State Technological University, Cherkasy, 2026.

The dissertation is devoted to solving a relevant scientific and applied problem consisting in the development of methods for selecting the parameters of finite fields of matrices of order 2 and their primitive elements for subsequent use in cryptographic protocols of computer systems and networks. The relevance of the topic is due to the continuous growth in the volume of information transmitted, processed, and stored in electronic form, as well as by the increasing requirements for the cryptographic strength of data protection means under conditions of developing distributed computing environments, cloud services, mobile networks, embedded systems, and the Internet of Things. Under such conditions, the construction of new mathematical platforms for cryptography becomes particularly important; on the one hand, these platforms rely on a rigorous algebraic apparatus, and on the other hand, they make it possible to expand the space of cryptographic parameters and increase the computational complexity of unauthorized recovery of key information.

In modern computer cryptography, finite fields constitute the foundation of many classical and contemporary algorithms, including key agreement protocols, digital signature schemes, symmetric ciphers, and authentication mechanisms. At the same time, the further development of cryptographic means requires the search for algebraic constructions that would allow the use of new types of elements and operations without loss of mathematical rigor. One promising area is the use of matrix structures over prime fields. However, the practical value of this approach is determined not merely by the very fact of using matrices, but primarily by the possibility of constructively selecting the parameters of the corresponding matrix

environment and primitive elements suitable for building cryptographic transformations. It is precisely this problem that the dissertation research addresses.

The object of the research is the processes of selecting parameters of finite fields of matrices order 2 and primitive elements in these fields for cryptographic use in computer systems and networks.

The subject of the research is methods, models, and algorithms for selecting parameters of finite fields of matrices of order 2, finding their primitive elements, and determining ways to use the obtained results in cryptographic key agreement protocols and digital signature schemes.

The aim of the dissertation is to increase the cryptographic strength of information protection means in computer systems and networks through the development of methods for selecting the parameters of finite fields of matrices of order 2 and their primitive elements suitable for the implementation of cryptographic protocols. To achieve this aim, the following main tasks were solved in the study: an analysis of the current state of the use of finite fields and matrix structures in cryptographic applications was carried out; the conditions to be satisfied by the parameters of matrix fields for their practical cryptographic use were determined; a method for selecting primitive elements of finite fields of matrices of order 2 was developed; a method for selecting parameters of a matrix field and a primitive element in it was developed; the implementation of cryptographic key agreement protocols and digital signatures was improved by transferring the corresponding operations into the matrix environment; and a study of the statistical properties and computational complexity of the proposed solutions was performed.

The dissertation demonstrates that the problem of selecting primitive elements in finite fields of second-order matrices cannot be effectively solved by exhaustive enumeration of all elements, since such an approach is computationally expensive and of limited suitability for practical cryptographic applications. Accordingly, a method for selecting primitive elements was developed that is based on the successive verification of the characteristics of a candidate matrix, analysis of its characteristic polynomial, the conditions for attaining the maximum period, and

verification of the order of the determinant in the base field. The proposed approach makes it possible to constructively form the complete set of primitive elements without the need for direct exhaustive enumeration of all possible matrices. This result has important practical significance, since primitive elements are generators of the multiplicative group and may be used as basic parameters in key agreement and signature schemes.

The essence of the developed method lies in the fact that, for a candidate matrix, its invariant characteristics are analyzed, in particular the trace, determinant, and the discriminant of the characteristic polynomial. On this basis, it is determined whether such a matrix can be a candidate primitive element in the corresponding matrix field. If the order of the multiplicative group is equal to $p^2 - 1$, then the primitive element must have exactly this order. For this purpose, the study employs criteria that reduce the problem of verifying primitiveness to an analysis of the period of the matrix and the order of its determinant in the base field \mathbb{Z}_p . Such an approach makes it possible to move from a general formulation of the problem to an efficient computational procedure.

Considerable attention is paid to the problem of simultaneously selecting the parameters of the matrix field and a primitive element in it. Unlike the traditional approach, in which the field parameters are first fixed and the search for primitive elements is then carried out separately, the proposed method combines these two procedures. This makes it possible to obtain the parameters of the matrix field and a primitive element within a single constructive scheme. The method is based on the use of the properties of quadratic residues and non-residues in a prime field, analysis of the irreducibility of the characteristic polynomial, and consideration of the relationship between the matrix parameters and the properties of its eigenvalues. A special important case is distinguished, in which the order of the multiplicative group has a favorable factorization, in particular one associated with Mersenne numbers or prime factors of a special form; the general case of parameter selection is also investigated.

The scientific novelty of the obtained results lies in the fact that, for the first time, methods for selecting the parameters of finite fields of matrices of order 2 and their primitive elements for cryptographic applications in computer systems and networks have been developed and theoretically substantiated. For the first time, an integral approach has been proposed in which the problem of selecting the parameters of a matrix field is combined with the problem of selecting a generator of its multiplicative group. Approaches to the use of matrix algebraic structures in the Diffie–Hellman key agreement protocol and the ElGamal digital signature scheme are presented.

The practical significance of the obtained results lies in the fact that the developed methods may be directly used in the creation of software and hardware means for cryptographic information protection. The proposed algorithmic procedures make it possible to form the parameters of a matrix field and the corresponding primitive elements for further application in key agreement protocols, digital signature schemes, as well as in other cryptographic mechanisms based on the difficulty of the discrete logarithm problem. The study shows that transferring computations from the classical scalar environment to the matrix one makes it possible to expand the set of admissible cryptographic parameters and creates the prerequisites for increasing cryptographic strength without fundamentally complicating the basic arithmetic operations. The obtained results may be used in secure network exchange systems, embedded devices, IoT solutions, as well as in specialized software and hardware complexes for information protection.

The dissertation provides examples of the practical application of the developed methods. In particular, the implementation of a key agreement protocol in a matrix environment is investigated, where public and secret parameters are specified by elements of the corresponding matrix field. The transfer of the ElGamal digital signature scheme to the case of using primitive elements of finite fields of second-order matrices is considered. It is shown that, within this approach, the general logic of classical cryptographic schemes is preserved, while a broader class of algebraic objects is employed. This opens up the possibility of constructing new

modifications of cryptographic protocols in which parameters may be additionally varied through matrix representation.

Particular attention is paid to the study of the statistical properties of matrix exponentiation and to the analysis of the computational complexity of cryptographic transformations in a matrix field. The study compares the proposed solutions with classical implementations over a prime field, analyzes the influence of field parameters on the number of possible primitive elements, and shows that the correct selection of parameters is of decisive importance for achieving the required level of cryptographic strength. The obtained results confirm that matrix fields can serve not only as a theoretical model but also as a practically suitable basis for the development of cryptographic means.

The results of the dissertation are significant for the further development of the mathematical apparatus of cryptography and for the creation of new approaches to the construction of secure systems for the transmission, storage, and authentication of information. The proposed methods provide the possibility of systematic selection of parameters and primitive elements in second-order matrix fields and create a scientific foundation for further research aimed at improving asymmetric cryptographic protocols oriented toward the use of special algebraic structures. The practical orientation of the obtained results lies in their suitability for software implementation, formalization in the form of algorithms, and integration into real information protection systems.

The main results of the dissertation have been published in 5 scientific publications, including 2 articles in journals indexed in Scopus and/or Web of Science (one of them in the Q2 quartile), as well as 3 papers presented at international scientific and practical conferences. This confirms the approbation of the main provisions of the dissertation and the scientific interest in the obtained results.

Keywords: cybersecurity, computer systems, computer networks, finite field, matrix of order 2, primitive element, field parameters, cryptographic protocol, key agreement, digital signature, discrete logarithm, cryptographic strength.

Список публікацій здобувача

- [1] A. Shcherba, E. Faure, T. Vartiainen, i V. Khaliavka, «Primitive Elements in the Finite Field of Square Matrices of Order 2 for Cryptographic Applications», Lecture Notes on Data Engineering and Communications Technologies, т. 222, Cham: Springer Nature Switzerland, 2024, С. 250-265. doi: [10.1007/978-3-031-71804-5_17](https://doi.org/10.1007/978-3-031-71804-5_17). (Scopus)
- [2] A. Baikenov, E. Faure, A. Shcherba, V. Khaliavka, S. Tynymbayev, i O. Abramkina, «A Unified Method for Selecting Parameters and Primitive Elements in 2×2 Matrix Fields for Cryptographic Protocols», Symmetry, т. 17, вип. 8, 1212, 2025, doi: [10.3390/sym17081212](https://doi.org/10.3390/sym17081212). (Scopus, Web of Science, Q2)
- [3] Щерба А.І., Фауре Е.В., Халявка В.В. Примітивні елементи скінченного поля квадратних матриць порядку 2 для криптографічних застосувань // Тези доповідей VII Міжнародної науково-практичної конференції «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2024), (Черкаси, 23-24 травня 2024 р.) [Електронний ресурс]. Черкаси : ЧДТУ, 2024. С. 183-185. [Online]. Доступний за: https://er.chdtu.edu.ua/bitstream/ChSTU/5863/1/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D1%82%D0%B5%D0%B7%D0%86%D0%A2%D0%9E%D0%9D%D0%A2-2024_%D0%BC%D0%B0%D0%BA%D0%B5%D1%82.pdf#page=183
- [4] Фауре Е. В., Халявка В. В. Метод вибору примітивних елементів у полях матриць 2×2 для криптографічних протоколів // Збірник тез доповідей IV Міжнар. наук.-практич. конфер. «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШІТ-2025)» (25 лист. 2025 р., м. Черкаси) [Електронний ресурс] / упоряд. : Т. О. Прокопенко, О. І. Підкуйко. М-во освіти і науки України, Черкас. держ. технол. ун-т. Черкаси : ЧДТУ, 2025. С. 273-275. [Online]. Доступний за: https://drive.google.com/file/d/1vfK7HzALRZHFTE8SKi6P_c-D3X4K3YPK/view

- [5] A. Baikenov, E. Faure, A. Shcherba, A. Lavdanskyi, S. Tynymbayev, V. Khaliavka, O. Abramkina. ElGamal Digital Signature Scheme in a Matrix Finite Field // 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), Paris, France, 2025. P. 1-6. DOI: [10.1109/ICECET63943.2025.11472340](https://doi.org/10.1109/ICECET63943.2025.11472340).

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	18
ВСТУП	19
РОЗДІЛ 1. АНАЛІЗ СУЧАСНОГО СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ.	
ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ	29
1.1. Вступ.....	29
1.2. Використання скінченних полів матриць у криптографічних застосуваннях	30
1.3. Комутативні сімейства матриць другого порядку	36
1.4. Комутативне сімейство матриць другого порядку з одиницею	41
1.5. Діагоналізація матриць групи $CGL_{b,k}(2, \mathbb{Z}_p)$	45
1.6. Мета та завдання дисертаційного дослідження	51
1.7. Висновки до розділу 1.....	52
РОЗДІЛ 2. МЕТОД ВИБОРУ ПРИМІТИВНИХ ЕЛЕМЕНТІВ СКІНЧЕННИХ ПОЛІВ КВАДРАТНИХ МАТРИЦЬ ДРУГОГО ПОРЯДКУ .	54
2.1. Вступ.....	54
2.2. Умови для генератора мультиплікативної групи скінченного поля матриць.....	54
2.3. Опис методу вибору примітивних елементів скінченних полів матриць другого порядку	71
2.4. Особливості застосування розробленого методу.....	73
2.5. Методика вибору примітивних елементів скінченних полів матриць другого порядку	76
2.6. Висновки до розділу 2.....	78
РОЗДІЛ 3. МЕТОД ВИБОРУ ПАРАМЕТРІВ ПОЛЯ КВАДРАТНИХ МАТРИЦЬ ДРУГОГО ПОРЯДКУ ТА ПРИМІТИВНОГО ЕЛЕМЕНТУ В НЬОМУ	81
3.1. Вступ.....	81

3.2. Задача вибору параметрів поля матриць.....	82
3.3. Пошук квадратичних лишків $q, r \in \mathbb{Z}_p$ таких, що $q + r = t^2 \in \mathbb{Z}_p$	89
3.4. Опис методу вибору параметрів b і k матричного поля $F_{b,k}$ і примітивного елементу в ньому	111
3.4.1. Спеціальний важливий випадок методу вибору параметрів b і k матричного поля $F_{b,k}$ і примітивного елементу в ньому, коли p є числом Мерсенна або $3 \leq \frac{p+1}{2} = \rho$ є простим числом.....	111
3.4.2. Загальний випадок методу вибору параметрів b і k матричного поля $F_{b,k}$ і примітивного елементу в ньому	122
3.5. Порівняльний аналіз методів вибору примітивних елементів	131
3.6. Висновки до розділу 3.....	133
РОЗДІЛ 4. КРИПТОГРАФІЧНІ ПРОТОКОЛИ В СКІНЧЕННИХ ПОЛЯХ КВАДРАТНИХ МАТРИЦЬ ДРУГОГО ПОРЯДКУ	136
4.1. Вступ.....	136
4.2. Протокол узгодження ключів.....	136
4.3. Приклад реалізації протоколу узгодження ключів	137
4.4. Протокол електронного цифрового підпису	137
4.5. Приклад реалізації ЕЦП.....	140
4.6. Статистичні властивості піднесення матриці до степеня	142
4.7. Імітаційні програмні моделі протоколу узгодження ключів і протоколу електронного цифрового підпису	146
4.8. Обчислювальна складність протоколів у матричному полі та порівняння з класичним випадком	149
4.9. Висновки до розділу 4.....	154
ВИСНОВКИ.....	156
СПИСОК ДЖЕРЕЛ.....	160
ДОДАТКИ.....	171
Додаток А. Лістинги експериментальних моделей	171

Додаток Б. Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації	177
---	-----

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AES – Advanced Encryption Standard;

ASCII – American Standard Code for Information Interchange;

DH – протокол Діффі–Хеллмана;

DLP – задача дискретного логарифмування;

DSS – Digital Signature Standard;

ECC – Elliptic Curve Cryptography;

ECDLP – задача дискретного логарифмування на еліптичній кривій;

EDS – електронний цифровий підпис;

ElGamal – криптографічна схема Ель-Гамаля;

GF – Galois Field;

IoT – Internet of Things;

NIST – National Institute of Standards and Technology;

RSA – Rivest–Shamir–Adleman.

ВСТУП

Актуальність теми дослідження. Сучасний розвиток комп'ютерних систем і мереж супроводжується постійним зростанням обсягів даних, що передаються, обробляються та зберігаються в електронному вигляді. За таких умов особливого значення набуває криптографічний захист інформації, який має забезпечувати конфіденційність, цілісність, доступність даних і стійкість до сучасних обчислювальних загроз. Теоретичний фундамент більшості класичних криптографічних схем становлять скінченні поля та завдання, пов'язані з обчисленням дискретного логарифма. Це простежується вже в базових роботах Diffie і Hellman [1], ElGamal [2], Koblitz [3] та Miller [4], у стандартизованих симетричних алгоритмах, зокрема AES [5], де арифметика над скінченними полями є невід'ємною частиною перетворень. Фундаментальні питання структури скінченних полів, побудови розширень, примітивних елементів і поліномів детально розглянуто в працях Lidl і Niederreiter [6], Mullen і Panario [7], Lenstra і Schoof [8], Hansen і Mullen [9], Cao і Wang [10], Cohen [11], Fan і Han [12], [13], Gao [14], von zur Gathen і Panario [15], Jungnickel і Vanstone [16]. Ці результати формують математичну базу для подальшого розвитку криптографічних платформ, орієнтованих на використання спеціальних алгебраїчних структур.

Підходам до використання матриць і розвитку матричного кодування присвячено праці D. Bigatti [17], A. Hock [18], D. Serre [19], W. P. Wardlaw [20], L. Brickman [21], R. Bellman [22], R.J. McEliece [23], [24], M.K. Singh [25], О.П. Стахова [26], [27]. Криптографічним схемам кодування на узагальнених матрицях Фібоначчі, матричних перестановках і полях Галуа належать праці A. Naseri [28], M. Durcheva [29], M. Maxrizal [30], M. Abu-Faraj [31], F. Al-Shaarani і A. Gutub [32], T. Kumar і S. Chauhan [33], А. Білецького [34].

У сучасній криптографії важливим напрямом є пошук нових алгебраїчних середовищ, які, з одного боку, зберігають строгість класичного апарату скінченних полів, а з іншого – розширюють простір криптографічних параметрів. Значна кількість досліджень у цьому напрямі присвячена

існуванню та властивостям примітивних елементів, нормальних і примітивно-нормальних базисів, а також елементів із додатковими обмеженнями на слід чи координати. Такі питання розглядали Lenstra і Schoof [8], Cohen і Huczynska [35], Cohen і Kapetanakis [36], Fernandes і Reis [37], а також Cao і Wang [10]. Практичне значення цих результатів полягає в тому, що примітивні елементи є генераторами мультиплікативних груп і безпосередньо пов'язані з побудовою протоколів узгодження ключів, схем електронного цифрового підпису та інших криптографічних механізмів. Водночас у класичному скалярному випадку простір допустимих параметрів визначається властивостями поля \mathbb{Z}_p або F_q , що стимулює пошук конструкцій, у яких можна одержати більшу гнучкість вибору параметрів без відмови від апарату теорії полів.

Одним із перспективних напрямів такого розширення є використання матричних алгебраїчних структур у криптографії. У роботах Zhao, Huang і Jiang [38] запропоновано схему відкритого ключа на основі ергодичних матриць над скінченними полями, а в праці Ding та ін. [39] показано, що матричні криптосистеми без належно контрольованої алгебраїчної структури можуть виявитися вразливими до криптоаналізу. Подібні висновки підтверджують і праці Sakalauskas, Mihalkovich, Venčkauskas [40], Mihalkovich, Zitkevicius, Sakalauskas [35], Sakalauskas, Dindienė, Kilčiauskas, Lukšys [41], Dindienė, Mihalkovich, Luksys, Sakalauskas [42], Ali та ін. [43], у яких матричні перетворення, matrix power function, MDS-матриці та матриці над комутативними кільцями розглядаються як основа нових криптографічних або дифузійних механізмів. Сукупно ці праці засвідчують, що сам по собі перехід до матричного подання є недостатнім: критично важливим є існування строго визначеної алгебраїчної структури, на якій можна конструктивно обирати параметри та генератори великого порядку.

Саме тому особливий науковий інтерес становлять праці, у яких досліджуються не довільні множини матриць, а саме скінченні поля

квадратних матриць другого порядку. У роботі Faure, Skutskyi, Shcherba, Lavdanskyi [44] виділено комутативні сімейства квадратних 2×2 матриць, придатні для криптографічних застосувань. У праці Faure, Skutskyi, Shcherba, Lavdanskyi [45] побудовано скінченне поле квадратних матриць другого порядку, що створює математичний фундамент для використання матричних елементів у задачах узгодження ключів і цифрового підпису. Однак, попри наявність зазначених результатів, задача конструктивного вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для практичної реалізації криптографічних протоколів у комп'ютерних системах і мережах залишається актуальною. Її розв'язання дає змогу поєднати строгість теорії скінченних полів із розширеним простором матричних параметрів, що створює передумови для підвищення криптографічної стійкості протоколів узгодження ключів і електронного цифрового підпису.

Виходячи з цього, тема дисертаційної роботи «Методи вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для криптографічних застосувань у комп'ютерних системах і мережах» є актуальною.

Зв'язок роботи з науковими програмами, планами, темами.

Дослідження, результати яких представлено в дисертаційній роботі, відповідають пріоритетному напрямку розвитку науки і техніки України «Інформаційні та комунікаційні технології» і виконувалися відповідно до програм і планів науково-дослідних робіт Черкаського державного технологічного університету.

Метою дослідження є підвищення криптографічної стійкості засобів захисту інформації в комп'ютерних системах і мережах за рахунок розроблення методів вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів, придатних для реалізації криптографічних протоколів.

Виходячи з зазначеної мети, задачами роботи є:

- провести аналіз сучасного стану використання скінченних полів і матричних структур у криптографічних застосуваннях;
- розробити метод вибору примітивних елементів скінченних полів матриць другого порядку;
- розробити метод вибору параметрів скінченних полів матриць другого порядку;
- удосконалити реалізацію криптографічних протоколів узгодження ключів і електронного цифрового підпису шляхом перенесення відповідних операцій у матричне середовище; виконати дослідження статистичних властивостей і обчислювальної складності запропонованих рішень.

Об'єктом дослідження є процеси вибору параметрів скінченних полів матриць другого порядку та примітивних елементів у цих полях для криптографічного використання в комп'ютерних системах і мережах.

Предметом дослідження є методи, моделі та алгоритми вибору параметрів скінченних полів матриць другого порядку, пошуку їх примітивних елементів, а також способи використання отриманих результатів у криптографічних протоколах узгодження ключів і електронного цифрового підпису.

Методи дослідження. У дисертації використано: аналітичний метод – для аналізу сучасного стану застосування скінченних полів і матричних структур у криптографії, виявлення обмежень відомих підходів і обґрунтування доцільності використання скінченних полів квадратних матриць другого порядку; алгебраїчні методи теорії скінченних полів і лінійної алгебри – для встановлення еквівалентних умов, за яких матриця є генератором мультиплікативної групи скінченного поля матриць, а також для одержання критеріїв перевірки максимального періоду й примітивності визначника; алгоритмічний метод – для розроблення методу вибору примітивних елементів, методу вибору параметрів матричного поля і

примітивного елемента в ньому, а також для побудови покрокових процедур і алгоритмів їх програмної реалізації; метод порівняльного аналізу – для зіставлення запропонованих підходів із класичними реалізаціями над простим полем, а також для порівняння методів вибору примітивних елементів і оцінювання їх ефективності; методи обчислювального експерименту та статистичного аналізу – для дослідження статистичних властивостей піднесення матриці до степеня, зокрема за результатами тестування послідовностей, і для перевірки придатності матричних перетворень у криптографічних схемах; метод аналізу обчислювальної складності – для оцінювання часових витрат алгоритмів вибору параметрів, факторизації, підготовки параметрів і виконання криптографічних операцій у матричному полі; метод криптографічного моделювання – для перенесення протоколу узгодження ключів Діффі–Хеллмана та схеми електронного цифрового підпису Ель-Гамала в середовище скінченних полів матриць другого порядку та перевірки працездатності запропонованих рішень.

Наукова новизна отриманих результатів:

- *вперше розроблено* метод вибору примітивних елементів скінченного поля квадратних матриць другого порядку над простим скінченним полем цілих чисел, який за рахунок послідовної перевірки дискримінанта характеристичного рівняння, максимального періоду матриці в квадратичному розширенні та примітивності її визначника в базовому полі дозволяє конструктивно формувати множину примітивних елементів поля матриць без повного перебору всіх його елементів;
- *вперше розроблено* метод вибору параметрів скінченного поля квадратних матриць другого порядку над простим скінченним полем цілих чисел \mathbb{Z}_p і примітивного елемента в цьому полі матриць для довільного простого p , який за рахунок детального дослідження й використання властивостей суми квадратичних лишків і нелишків у \mathbb{Z}_p дозволяє перейти від окремого розв’язання завдання вибору поля та завдання пошуку

примітивного елемента в цьому полі до їх узгодженого алгоритмічного розв'язання в межах єдиної процедури, а також суттєво звузити множину пошуку допустимих параметрів поля й забезпечити можливість знаходження примітивного елемента без повного перебору всіх елементів поля матриць;

– *удосконалено* метод вибору параметрів скінченного поля квадратних матриць другого порядку над простим скінченним полем цілих чисел \mathbb{Z}_p і примітивного елемента в цьому полі матриць для випадку, коли p є числом Мерсенна або $(p+1)/2$ є простим числом, який за рахунок обчислення символу Лежандра замість процедури розв'язання квадратичного рівняння в \mathbb{Z}_p дає змогу точно знаходити параметричне сімейство примітивних елементів поля матриць.

Практичне значення результатів дослідження.

1. Розроблено методику вибору примітивних елементів скінченних полів матриць другого порядку, орієнтовану на практичну й програмну реалізацію. Методика охоплює формування множини матриць-кандидатів, обчислення їх сліду, визначника та дискримінанта, перевірку умови максимального періоду, визначення порядку визначника та побудову примітивних елементів за допомогою скалярних коефіцієнтів із базового поля. Встановлено співвідношення, які дозволяють контролювати повноту сформованої множини примітивних елементів і уникати дублювання результатів під час обчислень. Розроблена методика дає змогу формувати всі примітивні елементи скінченного поля матриць другого порядку для їх подальшого використання в криптографічних алгоритмах комп'ютерних систем і мереж. Використання поля матриць порядку 2 над \mathbb{Z}_p забезпечує збільшення порядку мультиплікативної групи з $p-1$ до p^2-1 порівняно з базовим полем, що створює передумови для розширення можливостей криптографічних перетворень і потенційного підвищення їх криптографічної стійкості.

2. Розроблено алгоритми вибору параметрів скінченного поля квадратних матриць другого порядку над простим скінченним полем цілих чисел \mathbb{Z}_p і примітивного елементу в цьому полі матриць. Для спеціального випадку, коли p є числом Мерсенна або $(p+1)/2$ є простим числом, побудовано алгоритм, у якому основні обчислювальні кроки зводяться до знаходження первісного кореня, перевірки квадратичної нелишковості за символом Лежандра, розв'язання допоміжного рівняння та обчислення параметрів матриці. Для загального випадку побудовано алгоритмічну процедуру, що включає факторизацію чисел $p-1$ та p^2-1 , перевірку умов максимального порядку циклічної підгрупи та примітивності визначника, внаслідок чого забезпечується конструктивний вибір параметрів поля і примітивного елементу в ньому.

Отримані оцінки складності підтверджують, що визначальним чинником часу виконання є факторизація відповідних чисел, а самі алгоритми придатні до використання в задачах комп'ютерної інженерії, пов'язаних із математичним моделюванням обчислювальних процесів, програмною реалізацією криптографічних перетворень і захистом інформації в комп'ютерних системах і мережах.

Модельний приклад застосування алгоритмів вибору параметрів скінченного поля квадратних матриць другого порядку свідчить, що ймовірність вибору потрібної примітивної матриці збільшується порівняно з випадком повного перебору: 0,667 проти 0,132 для $p = 11$; 0,75 проти 0,166 для $p = 17$; 0,8 проти 0,133 для $p = 19$.

3. Розроблено імітаційні програмні моделі запропонованих схем узгодження ключів Діффі-Хеллмана та електронного цифрового підпису Ель-Гамала на скінченних полях квадратних матриць другого порядку, що забезпечує відтворення всіх основних етапів роботи криптографічних схем: генерації ключів, формування відкритих параметрів, узгодження спільного

ключа, створення електронного цифрового підпису та його перевірки – і можуть бути використані для переносу в програмне середовище.

Особистий внесок здобувача. Дисертація є самостійно виконаною завершеною роботою здобувача. Наукові результати і практичні розробки, що містяться в дисертаційній роботі, отримані автором самостійно.

У роботах, опублікованих у співавторстві, автором: [46], [47] – розроблено та теоретично обґрунтовано підходи до вибору примітивних елементів скінченного поля квадратних матриць другого порядку над простим скінченим полем цілих чисел, встановлено критерії примітивності елементу поля; [48] – розроблено методику вибору примітивних елементів у полях матриць 2×2 ; [49] – розроблено метод і алгоритми вибору параметрів скінченного поля квадратних матриць другого порядку і примітивного елемента в ньому; [50] – розроблено імітаційну програмну модель схеми електронного цифрового підпису Ель-Гамала на скінченному полі квадратних матриць другого порядку.

З робіт, опублікованих у співавторстві, для вирішення задач, поставлених у дисертаційному дослідженні, використано результати, отримані здобувачем особисто.

Апробація результатів дисертації. Основні результати дисертаційної роботи доповідалися та обговорювалися на:

- VII Міжнародній науково-практичній конференції «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2024), (Черкаси, 23-24 травня 2024 р.);
- IV Міжнародній науково-практичній конференції «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2025)» (25 лист. 2025 р., м. Черкаси);
- V International Conference on Electrical, Computer and Energy Technologies (ICECET 2025), (3-6 July 2025, Paris-France).

Публікації. Результати дослідження опубліковано в 5 наукових публікаціях, серед яких 2 статті [46], [49] у виданнях, що індексуються в Scopus та/або Web of Science (одна [49] з них у квартилі Q2), а також 3 доповіді [47], [48], [50] на міжнародних науково-практичних конференціях.

Структура і обсяг дисертаційної роботи. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 178 сторінок машинописного тексту, включає 6 рисунків, 22 таблиці та 101 найменування в списку використаних джерел.

У **першому розділі** проведено аналіз сучасного стану предметної області, розглянуто використання скінченних полів і матричних структур у криптографічних застосуваннях комп'ютерних систем і мереж, досліджено сімейства квадратних матриць другого порядку над полем простих лишків; сформульовано мету і завдання дисертаційного дослідження.

У **другому розділі** розроблено метод вибору примітивних елементів скінченних полів матриць другого порядку. Встановлено умови, за яких матриця є генератором мультиплікативної групи скінченного поля матриць, наведено опис методу вибору примітивних елементів, досліджено особливості його застосування та сформовано методику, орієнтовану на практичну і програмну реалізацію.

У **третьому розділі** розроблено метод вибору параметрів поля матриць другого порядку і примітивного елемента в ньому. Досліджено задачу вибору параметрів поля матриць, виконано аналіз властивостей квадратичних лишків і нелишків у простому полі, побудовано алгоритмічні процедури для спеціального та загального випадків вибору параметрів скінченного поля квадратних матриць другого порядку і примітивного елемента в ньому, а також проведено порівняльний аналіз запропонованих підходів.

У **четвертому розділі** розглянуто криптографічні протоколи в скінченних полях матриць другого порядку. Наведено реалізацію протоколу узгодження ключів та протоколу електронного цифрового підпису в

матричному полі, досліджено статистичні властивості піднесення матриці до степеня, а також проаналізовано обчислювальну складність запропонованих криптографічних протоколів і виконано їх порівняння з класичним випадком.

У **висновках** узагальнено результати дисертаційного дослідження, сформульовано основні наукові й практичні результати та визначено напрями подальших досліджень.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНОГО СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ. ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ

1.1. Вступ

Сучасний розвиток комп'ютерних систем і мереж супроводжується постійним зростанням обсягів інформації, що передається, обробляється та зберігається в електронному вигляді. За таких умов особливого значення набуває забезпечення криптографічного захисту даних, який має поєднувати високий рівень стійкості з можливістю ефективної практичної реалізації. Одним із перспективних напрямів удосконалення криптографічних засобів є використання алгебраїчних структур, здатних розширити простір параметрів криптографічних перетворень без відмови від класичних математичних підходів.

У сучасній криптографії скінченні поля становлять фундамент більшості відомих асиметричних і симетричних схем. Водночас подальший розвиток криптографічних механізмів потребує пошуку таких алгебраїчних конструкцій, які, з одного боку, зберігали б строгість і передбачуваність математичного апарату, а з іншого – надавали б нові можливості для побудови більш складних і стійких перетворень. У цьому контексті особливий інтерес становлять скінченні поля квадратних матриць другого порядку, які дають змогу поєднати переваги теорії скінченних полів із додатковими властивостями матричного подання.

Аналіз наукових праць показує, що використання матричних структур у криптографії є актуальним і водночас складним напрямом досліджень. З одного боку, матриці над скінченними полями вже широко застосовуються в симетричних криптографічних перетвореннях, зокрема для забезпечення дифузії та побудови ефективних лінійних перетворень. З іншого боку, спроби використання загальних матричних платформ у криптографії з відкритим ключем не завжди приводили до належного рівня стійкості, оскільки за

відсутності чітко визначеної алгебраїчної структури такі системи можуть містити приховану лінійність і допускати ефективний криптоаналіз.

Саме тому науковий інтерес становить не просто використання множин матриць над скінченними полями, а побудова таких сімейств матриць, які зі звичайними операціями додавання та множення утворюють скінченне поле. За такого підходу стає можливим перенесення на матричні елементи класичних результатів теорії скінченних полів, зокрема властивостей циклічності мультиплікативної групи, існування примітивних елементів і побудови перетворень з великим періодом. Це відкриває перспективу використання матричних полів як математичної основи для вдосконалення відомих криптографічних схем, зокрема протоколів узгодження ключів та електронного цифрового підпису.

У першому розділі дисертації проведено аналіз сучасного стану досліджень у галузі застосування скінченних полів і матричних структур у криптографії, розглянуто комутативні сімейства квадратних матриць другого порядку над полем простих лишків, досліджено умови побудови на їх основі скінченного поля, а також обґрунтовано доцільність використання таких алгебраїчних структур для подальшого розроблення криптографічних методів і засобів захисту інформації.

1.2. Використання скінченних полів матриць у криптографічних застосуваннях

Скінченні поля посідають центральне місце в сучасній криптографії, оскільки саме в них вдається поєднати строгі алгебраїчні властивості з високою ефективністю реалізації обчислень у комп'ютерних системах і мережах. Класичні криптографічні побудови, зокрема протокол Діффі-Хеллмана [1], схема Ель-Гамала [2], криптографія на еліптичних кривих [3], [51], а також значна частина симетричних перетворень, безпосередньо або опосередковано спираються на арифметику скінченних полів. Відомо, що для

поля $GF(q)$, де $q = p^m$, мультиплікативна група ненульових елементів має порядок $q - 1$ і є циклічною, а тому для неї існують примітивні елементи, тобто генератори всієї мультиплікативної групи. Саме ця властивість є однією з ключових у криптографічних застосуваннях, оскільки дозволяє формувати великі циклічні підгрупи, на яких будуються задачі дискретного логарифмування, узгодження ключів й інші криптографічні механізми.

У симетричній криптографії роль скінченних полів також є фундаментальною. Так, у шифрі AES [5] арифметика над $GF(2^8)$ використовується як під час побудови нелінійного перетворення SubBytes, так і в лінійному перетворенні MixColumns. Для вектору стану операція MixColumns задається множенням на MDS-матрицю над $GF(2^8)$. Використовують оборотну матрицю з високими дифузійними властивостями. Хоча в такому випадку матриця використовується не як елемент поля матриць, а як інструмент лінійного перетворення над полем, уже тут проявляється важливий факт: матричні структури над скінченними полями мають самостійну криптографічну цінність. Саме тому в подальших роботах [52], [53], [54] розглядалися різні класи MDS-матриць, зокрема легковагові, циркулянтні та динамічні, орієнтовані на покращення апаратної та програмної реалізації криптографічних алгоритмів.

Разом з тим, для криптографії з відкритим ключем виявився недостатнім сам факт використання класичних полів $GF(q)$. У зв'язку з цим у літературі з'явився окремий напрям, спрямований на застосування матриць над скінченними полями як носіїв нових обчислювально складних задач. За такого підходу замість елемента $a \in GF(q)$ розглядається матриця $A \in M_n(GF(q))$ або $A \in GL_n(GF(q))$, а замість звичайного степеневого перетворення a^x – матричні степені A^x , матричні добутки та двосторонні степеневі конструкції. Якщо для скалярного випадку порядок елемента визначається найменшим

числом t , для якого $a^t = 1$, то для матриці аналогічно розглядається умова $A^t = I$.

Тоді криптографічний інтерес становлять такі матриці, для яких значення t є максимальним або достатньо великим, а задача відновлення показника степеня або прихованих параметрів не зводиться до простої системи лінійних рівнянь.

Одними з перших робіт цього напрямку стали праці, присвячені ергодичним матрицям над скінченними полями [38], [39], [55], [56], [57]. У роботі [38] запропоновано схему з відкритим ключем, побудовану на так званих ергодичних матрицях над полем $GF(p)$. У цьому підході матриця Q вважається ергодичною, якщо її степені породжують послідовність максимальної довжини, а криптографічна стійкість пов'язується з важкістю спеціально введених задач TEME та SEME. Ідея цих задач полягає у відновленні степеневих параметрів за відомими матричними образами, причому передбачалося, що така задача є складнішою, ніж класична задача дискретного логарифмування. Сам підхід виглядав перспективним, оскільки дозволяв перейти від одномірної арифметики до багатовимірної матричної платформи.

Проте подальші дослідження показали, що не будь-яка матрична конструкція є придатною для криптографічного використання. Уже в [55] продемонстровано, що одна зі схем на ергодичних матрицях допускає ефективний криптоаналіз шляхом зведення до системи лінійних рівнянь. У [39] та [56] безпеку таких систем проаналізовано глибше, і встановлено, що TEME-проблема в низці випадків розв'язується за поліноміальний час, а SEME-проблема за неправильного вибору параметрів зводиться до дискретного логарифмування над базовим полем. Як наслідок, сам перехід до матриць не усуває структурної вразливості, якщо матрична платформа містить приховану лінійність. Цей висновок має принципове значення, оскільки він вказує на необхідність не просто використовувати матриці над скінченними

полями, а добирати такі їх сімейства, для яких структура поля та примітивність елементів контролюються строгими теоретичними критеріями. Огляд сучасних робіт з криптоаналізу матричних схем також прямо підкреслює, що побудова безпечної та практичної системи шифрування на матрицях над скінченними полями залишається складною науковою проблемою.

Інший важливий напрям представлено роботами, присвяченими *matrix power function* [58], [59], [60], [61], [62]. У цих працях розглядається двостороння матрична степенева функція, яка в загальному вигляді може бути записана як

$$F_{X,Y}(W) = X^m W Y^n,$$

де X , Y , W – матриці над відповідною алгебраїчною структурою. Перевагою такого підходу є значне розширення простору параметрів і можливість побудови нетрадиційних задач інверсії. У ранніх роботах цього напрямку було запропоновано нові асиметричні шифри та протоколи узгодження ключів. Проте згодом у [59] було знайдено атаку лінійної алгебри на одну з базових схем, після чого в [60], [61] запропоновано вдосконалені модифікації, стійкі до зазначеної атаки. У новіших дослідженнях *matrix power function* розглядається також у контексті постквантових узгоджувальних протоколів та симетричних конструкцій [62]. Водночас, загальний висновок цих джерел збігається з наведеним вище: складність матричного перетворення має бути підкріплена належно обраною алгебраїчною структурою; інакше зовнішньо складна схема може мати внутрішньо лінійний характер. Сучасні праці про *matrix power function* дійсно фіксують як появу атаки лінійної алгебри на ранні варіанти, так і подальші спроби модифікувати схеми, зберігаючи їх ефективність.

Поряд із некомутативними матричними платформами в літературі простежується ще один, значно важливіший напрям: побудова саме скінченних полів матриць, а не лише множин або груп матриць. У загальному випадку множина всіх квадратних матриць порядку n над $GF(p)$ не є полем,

оскільки містить необоротні елементи й не є комутативною відносно множення. Проте для окремо побудованих сімейств матриць можливо забезпечити виконання аксіом поля. У такому випадку відкривається можливість перенести на матричні елементи класичні результати теорії скінченних полів: циклічність мультиплікативної групи, існування примітивних елементів, опис степеневих ланцюгів, умови максимального періоду тощо. Саме ця ідея є концептуально важливою, оскільки дозволяє поєднати переваги матричного подання з математичною визначеністю теорії $GF(p^m)$.

Для матриці другого порядку

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

над $GF(p)$ її характеристичний багаточлен має вигляд

$$\lambda^2 - \text{tr}(A)\lambda + \det(A),$$

де

$$\text{tr}(A) = a + d,$$

$$\det(A) = ad - bc.$$

Саме аналіз значення $\Delta(A)$ дозволяє розрізнити випадок, коли характеристичний багаточлен розкладається над $GF(p)$, і випадок, коли його корені належать лише квадратичному розширенню $GF(p^2)$. Для криптографічних застосувань це принципово, оскільки від характеру власних значень матриці залежать її порядок, період степеневі послідовності та можливість бути генератором великої мультиплікативної групи. Якщо власні значення матриці належать базовому полю, то порядок матриці часто зводиться до порядків відповідних скалярних елементів і не перевищує $p-1$ або найменшого спільного кратного цих порядків. Якщо ж характеристичний многочлен є нерозкладним над $GF(p)$, тоді матриця природно

інтерпретується як елемент квадратичного розширення, і її порядок може досягати $p^2 - 1$.

Це безпосередньо зближує задачу вибору матриць для криптографії із задачею вибору примітивних елементів поля. Для поля $GF(p^2)$ мультиплікативна група має порядок $p^2 - 1$, а отже матриця A , що представляє елемент цього поля, є примітивною тоді і тільки тоді, коли

$$\text{ord}(A) = p^2 - 1.$$

Кількість таких елементів визначається функцією Ейлера:

$$\varphi(p^2 - 1)$$

У криптографічному сенсі це означає, що правильно побудоване поле матриць другого порядку дає можливість використовувати генератори мультиплікативної групи більшого порядку, ніж у базовому полі $GF(p)$, де порядок групи дорівнює лише $p - 1$. Таким чином, навіть за незмінного простого модуля p перехід до поля матриць дозволяє суттєво збільшити розмір циклічної групи, а відтак – розширити простір допустимих криптографічних параметрів.

Варто також зазначити, що в окремих джерелах [63], [64], [65] розглядалися суміжні питання, пов'язані із застосуванням спеціальних класів матриць над полями у криптографії. Так, досліджувалися сингулярні матриці, матричні добутки, а також криптографічні побудови, в яких матриці виступають носіями параметризованих перетворень. Такі результати є корисними для загального розуміння потенціалу матричних методів, проте вони ще раз підтверджують, що універсальною проблемою залишається керованість алгебраїчної структури. Без чіткого опису множини допустимих матриць, без критерію їх примітивності та без способу конструктивного вибору генераторів криптографічна платформа залишається теоретично неповною.

З огляду на це в сучасних дослідженнях привертають увагу роботи, у яких безпосередньо побудовано поле квадратних матриць порядку 2 та розглянуто питання примітивних елементів такого поля. У праці [44] показано існування сімейства квадратних матриць другого порядку над полем простих лишків, яке зі звичайними операціями додавання та множення матриць утворює скінченне поле порядку p^2 . Це прямо відповідає завданню побудови матричної криптографічної платформи зі строго визначеними властивостями поля. Праця [45] уточнює клас комутативних матриць другого порядку, придатних для такого конструювання.

Подальше дослідження зосередимо на полях квадратних матриць другого порядку, які поєднують порівняно просту структуру з можливістю одержання поля порядку p^2 і мультиплікативної групи порядку $p^2 - 1$. У зв'язку з цим особливий інтерес становлять праці [44], [45], які розглянемо детальніше.

1.3. Комутативні сімейства матриць другого порядку

Позначимо повну загальну групу порядку n над полем F через $GL(n, F)$.

Квадратна матриця A є оборотною тоді і тільки тоді, коли її визначник $|A| \neq 0$ [66].

Нехай група $\Gamma = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}_p, |A| \neq 0 \right\}$, де \mathbb{Z}_p – просте поле

лишків за модулем p . Тоді $\Gamma = GL(2, \mathbb{Z}_p)$.

Твердження 1.1 (з [44]). Операція множення є комутативною для наступних сімейств матриць групи $\Gamma = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}_p, |A| \neq 0 \right\}$:

$$\Gamma_1 = \left\{ t \cdot \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}, t, a \in \mathbb{Z}_p, t \neq 0, a \neq 0 \right\},$$

$$\Gamma_2 = \left\{ t \cdot \begin{pmatrix} 1 & 0 \\ a & ak+1 \end{pmatrix}, t, a, k \in \mathbb{Z}_p, t \neq 0, ak+1 \neq 0 \right\}, k - \text{фіксоване};$$

$$\Gamma_3 = \left\{ t \cdot \begin{pmatrix} 1 & a \\ 0 & ak+1 \end{pmatrix}, t, a, k \in \mathbb{Z}_p, t \neq 0, ak+1 \neq 0 \right\}, k - \text{фіксоване};$$

$$\Gamma_4 = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}, t, a, b \in \mathbb{Z}_p, t \neq 0, b \neq 0 \right\}, a \text{ і } b - \text{фіксовані};$$

$$\Gamma_5 = \left\{ t \cdot \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}, t, a, b \in \mathbb{Z}_p, t \neq 0, b \neq 0 \right\}, a \text{ і } b - \text{фіксовані};$$

$$\Gamma_6 = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, t, a, b, k \in \mathbb{Z}_p, t \neq 0, b \neq 0, a(a+k)-b \neq 0 \right\}, b \text{ і } k -$$

фіксовані.

Доведення (з [44]). У загальному випадку група Γ неабелева.

Розглянемо наступні випадки для $|A| \neq 0$:

- 1) $b = c = 0, ad \neq 0$;
- 2) $b = 0$ або $c = 0, ad \neq 0$;
- 3) $bc \neq 0, ad = 0$;
- 4) $ad \neq 0, bc \neq 0$.

1. Випадок 1: $b = c = 0$ і $ad \neq 0$. Тоді $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & d/a \end{pmatrix}$.

Множина таких діагональних невідроджених матриць еквівалентна множині

$\Gamma_1 = \left\{ t \cdot \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}, t, a \in \mathbb{Z}_p, t \neq 0, a \neq 0 \right\}$, яка утворює абелеву групу [67]: для

$\forall A, B \in \Gamma_1$ справедливо $AB = BA$.

2. Випадок 2: $b = 0$ або $c = 0, ad \neq 0$.

Нехай $b = 0$ і $ad \neq 0$. Тоді матриця $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ c/a & d/a \end{pmatrix}$.

Множина таких матриць є сімейством невироджених нижньотрикутних матриць $\Upsilon = \left\{ t \cdot \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}, t, a, b \in \mathbb{Z}_p, t \neq 0, b \neq 0 \right\}$, яка відповідно до [67] утворює групу за множенням.

Нехай $A, B \in \Upsilon$ і $A = \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ x & y \end{pmatrix}$. Добуток $A \cdot B = \begin{pmatrix} 1 & 0 \\ a + bx & by \end{pmatrix}$.

Добуток $B \cdot A = \begin{pmatrix} 1 & 0 \\ x + ay & by \end{pmatrix}$.

Значення $AB = BA$, якщо $a + bx = x + ay$ або $x(b - 1) = a(y - 1)$. Якщо $a = x = 0$, Υ вироджується в Γ_1 , яка є абелевою. Якщо ж $a, x \neq 0$, прийнемо

$\frac{b-1}{a} = \frac{y-1}{x} = k$, $k \in \mathbb{Z}_p$. Тоді $\begin{cases} b = ak + 1; \\ y = xk + 1; \end{cases}$ а матриці $A = \begin{pmatrix} 1 & 0 \\ a & ak + 1 \end{pmatrix}$,

$B = \begin{pmatrix} 1 & 0 \\ x & xk + 1 \end{pmatrix}$, де $a \neq 0$, $x \neq 0$, $ak + 1 \neq 0$, $xk + 1 \neq 0$, $\forall k \in \mathbb{Z}_p$.

Тоді $\Gamma_2 = \left\{ t \cdot \begin{pmatrix} 1 & 0 \\ a & ak + 1 \end{pmatrix}, t, a, k \in \mathbb{Z}_p, t \neq 0, ak + 1 \neq 0 \right\}$ є абелевою групою,

причому значення a і t можуть бути довільними, а значення k є фіксованим параметром групи Γ_2 .

Прийнявши $c = 0$, $ad \neq 0$, за аналогією можна показати, що група невироджених верхньотрикутних матриць виду $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ є абелевою, якщо

утворює групу $\Gamma_3 = \left\{ t \cdot \begin{pmatrix} 1 & a \\ 0 & ak + 1 \end{pmatrix}, t, a, k \in \mathbb{Z}_p, t \neq 0, ak + 1 \neq 0 \right\}$.

3. Випадок 3: $bc \neq 0$, $ad = 0$.

Нехай $bc \neq 0$, $d = 0$. Тоді матриця $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} = a \begin{pmatrix} a/b & 1 \\ c/b & 0 \end{pmatrix}$.

Такі матриці задають множину $\Xi = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}, t, a, b \in \mathbb{Z}_p, t \neq 0, b \neq 0 \right\}$.

Нехай $A, B \in \Xi$ і $A = t \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}$, $B = s \begin{pmatrix} x & 1 \\ y & 0 \end{pmatrix}$. Рівність $A \cdot B = B \cdot A$ означає

$$\begin{pmatrix} ax + y & a \\ bx & b \end{pmatrix} = \begin{pmatrix} ax + b & x \\ ay & y \end{pmatrix} \text{ або } \begin{cases} x = a; \\ y = b. \end{cases} \text{ Отже, для } bc \neq 0 \text{ і } d = 0 \text{ комутативним}$$

сімейством є множина $\Gamma_4 = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}, t, a, b \in \mathbb{Z}_p, t \neq 0, b \neq 0 \right\}$, де a і b –

фіксовані.

Прийнявши $bc \neq 0$, $a = 0$, за аналогією можна показати, що комутативним сімейством є множина $\Gamma_5 = \left\{ t \cdot \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}, t, a, b \in \mathbb{Z}_p, t \neq 0, b \neq 0 \right\}$,

де a і b – фіксовані.

Зауважимо, що сімейства Γ_4 , Γ_5 не замкнено відносно операції множення, тому не утворюють групу.

4. Випадок 4: $\begin{cases} ad \neq 0; \\ bc \neq 0. \end{cases}$ Оскільки $b \neq 0$, то $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = b \begin{pmatrix} a/b & 1 \\ c/b & d/b \end{pmatrix}$.

Множина таких матриць утворює множину невироджених матриць

$$\Psi = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & c \end{pmatrix}, t, a, b, c \in \mathbb{Z}_p, t \neq 0, b \neq 0, ac - b \neq 0 \right\}.$$

Нехай $A, B \in \Psi$ і $A = \begin{pmatrix} a & 1 \\ b & c \end{pmatrix}$, $B = \begin{pmatrix} x & 1 \\ y & z \end{pmatrix}$. Добуток

$$A \cdot B = \begin{pmatrix} ax + y & a + z \\ bx + cy & b + cz \end{pmatrix}. \text{ Добуток } B \cdot A = \begin{pmatrix} ax + b & x + c \\ ay + bz & y + cz \end{pmatrix}.$$

Рівність $AB = BA$ досягається, якщо
$$\begin{cases} ax + y = ax + b; \\ a + z = x + c; \\ bx + cy = ay + bz; \\ b + cz = y + cz. \end{cases} \quad \text{З цього слідує, що}$$

$$\begin{cases} y = b; \\ c - a = z - x. \end{cases}$$

Нехай $c - a = z - x = k$, $k \in \mathbb{Z}_p$. Тоді $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$, $B = \begin{pmatrix} x & 1 \\ b & x+k \end{pmatrix}$,

звідки комутативним сімейством є множина

$$\Gamma_6 = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, t, a, b, k \in \mathbb{Z}_p, t \neq 0, b \neq 0, a(a+k) - b \neq 0 \right\}, \text{ причому значення}$$

a і t можуть бути довільними, а значення b і k є фіксованими параметрами множини Γ_6 .

Запишемо всі сімейства $\Gamma_1 - \Gamma_6$ матриць з $\Gamma = GL(2, \mathbb{Z}_p)$, для яких операція множення є комутативною:

$$\Gamma_1 = \left\{ t \cdot \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}, t, a \in \mathbb{Z}_p, t \neq 0, a \neq 0 \right\},$$

$$\Gamma_2 = \left\{ t \cdot \begin{pmatrix} 1 & 0 \\ a & ak+1 \end{pmatrix}, t, a, k \in \mathbb{Z}_p, t \neq 0, ak+1 \neq 0 \right\}, k - \text{фіксоване};$$

$$\Gamma_3 = \left\{ t \cdot \begin{pmatrix} 1 & a \\ 0 & ak+1 \end{pmatrix}, t, a, k \in \mathbb{Z}_p, t \neq 0, ak+1 \neq 0 \right\}, k - \text{фіксоване};$$

$$\Gamma_4 = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix}, t, a, b \in \mathbb{Z}_p, t \neq 0, b \neq 0 \right\}, a \text{ і } b - \text{фіксовані};$$

$$\Gamma_5 = \left\{ t \cdot \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}, t, a, b \in \mathbb{Z}_p, t \neq 0, b \neq 0 \right\}, a \text{ і } b - \text{фіксовані};$$

$$\Gamma_6 = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, t, a, b, k \in \mathbb{Z}_p, t \neq 0, b \neq 0, a(a+k) - b \neq 0 \right\}, b \text{ і } k -$$

фіксовані.

Твердження доведено.

Потужності $\Gamma_1 - \Gamma_3$ дорівнюють $(p-1)^2$, а $\Gamma_4 - \Gamma_5 - p-1$. Потужність Γ_6 дорівнює $(p-1)(p-l)$, де $l = \{0; 1; 2\}$ – кількість цілих коренів рівняння $a^2 + ka - b = 0 \pmod{p}$ відносно a . Значення l визначається значеннями b і k .

1.4. Комутативне сімейство матриць другого порядку з одиницею

Розглянемо сімейство матриць Γ_6 , доповнене одиничною матрицею, а також випадком, коли $b = 0$, оскільки він не впливає на комутативність матриць множини Γ_6 . Позначимо це сімейство через

$$CGL_{b,k}(2, \mathbb{Z}_p) = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, t, s, a, b, k \in \mathbb{Z}_p, t, s \neq 0, a(a+k) - b \neq 0 \right\}$$

Твердження 2 (з [44]). Сімейство матриць $CGL_{b,k}(2, \mathbb{Z}_p)$ є комутативною (абелевою) групою за множенням.

Доведення (з [44]).

Доведення передбачає підтвердження виконання аксіом групи для $CGL_{b,k}(2, \mathbb{Z}_p)$, а також, що операція множення у $CGL_{b,k}(2, \mathbb{Z}_p)$ є комутативною.

1. У $CGL_{b,k}(2, \mathbb{Z}_p)$ існує єдиний нейтральний (одиничний) елемент:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

2. Операція множення елементів у $CGL_{b,k}(2, \mathbb{Z}_p)$ є асоціативною, оскільки це є загальною властивістю матриць.

3. Для кожної матриці $A \in CGL_{b,k}(2, \mathbb{Z}_p)$ існує обернена матриця $A^{-1} \in CGL_{b,k}(2, \mathbb{Z}_p)$: $A \cdot A^{-1} = A^{-1} \cdot A = E$.

Якщо $A = s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, то $A^{-1} = \left[s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right]^{-1} = s^{-1} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. У \mathbb{Z}_p для

кожного $s \in \mathbb{Z}_p$ існує обернений елемент s^{-1} : $s \cdot s^{-1} = s^{-1} \cdot s = e = 1$, причому єдиний. Надалі в доведенні, не обмежуючи загальності, множники s і t будуть знехтувані.

Нехай $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$. Тоді $A^{-1} = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}^{-1} = \frac{1}{a(a+k)-b} \begin{pmatrix} a+k & -1 \\ -b & a \end{pmatrix}$.

Нехай $t' = \frac{-1}{a(a+k)-b} \neq 0$ і $a' = -a-k$. Тоді

$$A^{-1} = t' \cdot \begin{pmatrix} a' & 1 \\ b & a'+k \end{pmatrix} \in CGL_{b,k}(2, \mathbb{Z}_p).$$

Звідси слідує, що $\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \begin{pmatrix} c & 1 \\ b & c+k \end{pmatrix}^{-1} = E$ тоді і тільки тоді, коли

$$a = c.$$

4. $CGL_{b,k}(2, \mathbb{Z}_p)$ є замкнутою відносно операції множення.

Нехай $A, B \in CGL_{b,k}(2, \mathbb{Z}_p)$. Якщо $A = E$ або $B = E$, ця властивість є очевидною.

Нехай $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ і $B = \begin{pmatrix} x & 1 \\ b & x+k \end{pmatrix}$ для довільних $a, x \in \mathbb{Z}_p$.

Значення

$$A \cdot B = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \begin{pmatrix} x & 1 \\ b & x+k \end{pmatrix} = \begin{pmatrix} ax+b & a+x+k \\ b(a+x+k) & b+(a+k)(x+k) \end{pmatrix}.$$

Якщо $a+x+k=0$, то $A \cdot B = \begin{pmatrix} ax+b & 0 \\ 0 & ax+b \end{pmatrix} = (ax+b) \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Оскільки $|A| \neq 0$ і $|B| \neq 0$, то $|A \cdot B| = |A| \cdot |B| \neq 0$ і, відповідно, $ax+b \neq 0$. Звідси слідує, що $A \cdot B \in CGL_{b,k}(2, \mathbb{Z}_p)$.

Якщо $a + x + k \neq 0$, то $A \cdot B = \frac{1}{a + x + k} \begin{pmatrix} \frac{ax + b}{a + x + k} & 1 \\ b & k + \frac{ax + b}{a + x + k} \end{pmatrix}$. Нехай

$t = \frac{1}{a + x + k} \neq 0$ і $y = \frac{ax + b}{a + x + k}$. Тоді $A \cdot B = t \begin{pmatrix} y & 1 \\ b & y + k \end{pmatrix} \in CGL_{b,k}(2, \mathbb{Z}_p)$.

5. Група $CGL_{b,k}(2, \mathbb{Z}_p)$ є абелевою.

Якщо $A = E$, то $A \cdot B = E \cdot B = B = B \cdot E = B \cdot A$.

Нехай $A = \begin{pmatrix} a & 1 \\ b & a + k \end{pmatrix}$ і $B = \begin{pmatrix} x & 1 \\ b & x + k \end{pmatrix}$. Тоді

$$A \cdot B = \begin{pmatrix} ax + b & a + x + k \\ b(a + x + k) & b + (a + k)(x + k) \end{pmatrix}, \quad \text{а}$$

$$B \cdot A = \begin{pmatrix} ax + b & a + x + k \\ b(a + x + k) & b + (x + k)(a + k) \end{pmatrix}, \text{ звідки } A \cdot B = B \cdot A.$$

Твердження доведено.

Для піднесення матриці $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ до степеня можна використовувати

вираз з [68]:

$$A^n = \begin{pmatrix} u_{n+1} - du_n & bu_n \\ cu_n & u_{n+1} - au_n \end{pmatrix}, \quad (1.1)$$

де $u_{n+1} = (a + d)u_n - |A|u_{n-1} = \text{tr}(A)u_n - |A|u_{n-1}$, $\text{tr}(A)$ – слід матриці A [69];

$$u_0 = 0, \quad u_1 = 1.$$

Для елемента групи $A = \begin{pmatrix} a & 1 \\ b & a + k \end{pmatrix} \in CGL_{b,k}(2, \mathbb{Z}_p)$ маємо: $\text{tr}(A) = 2a + k$

, $|A| = a(a + k) - b \neq 0$. Тоді $u_{n+1} = (2a + k)u_n - (a(a + k) - b)u_{n-1}$, а

$$A^n = \begin{pmatrix} u_{n+1} - (a + k)u_n & u_n \\ bu_n & u_{n+1} - au_n \end{pmatrix}.$$

Варто зазначити, що $|A^n| = |A|^n \neq 0$.

Оскільки $CGL_{b,k}(2, \mathbb{Z}_p)$ є комутативною групою за множенням, $A^n \in CGL_{b,k}(2, \mathbb{Z}_p)$. Відповідно до (1.1):

$$1) \text{ якщо } u_n = 0, \text{ то } A^n = \begin{pmatrix} u_{n+1} & 0 \\ 0 & u_{n+1} \end{pmatrix} = u_{n+1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in CGL_{b,k}(2, \mathbb{Z}_p);$$

$$2) \text{ якщо } u_n \neq 0, \text{ то } A^n = u_n \begin{pmatrix} \frac{u_{n+1}}{u_n} - a - k & 1 \\ b & \frac{u_{n+1}}{u_n} - a \end{pmatrix} \in CGL_{b,k}(2, \mathbb{Z}_p).$$

Твердження 3 (з [44]). Порядок групи $CGL_{b,k}(2, \mathbb{Z}_p)$ для $D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p$ дорівнює $p^2 - 1$.

Доведення (з [44]).

Нагадаємо,

що

$$CGL_{b,k}(2, \mathbb{Z}_p) = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, t, s, a, b, k \in \mathbb{Z}_p, t, s \neq 0, a(a+k) - b \neq 0 \right\}$$

.

Оскільки b і k є фіксованими, змінними є $t, a, s \in \mathbb{Z}_p, t, s \neq 0$. Тоді кількість різних значень матриць виду $t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ дорівнює кількості різних пар $\{t, a\}$ з заданими обмеженнями. Значення t може приймати $p-1$ різних значень з \mathbb{Z}_p ($t \neq 0$). Значення a обмежене умовою $a(a+k) - b \neq 0$. Для $D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p$ це рівняння не має цілих коренів відносно змінної a , тому вона може набувати p різних значень з \mathbb{Z}_p .

Кількість різних значень матриць виду $s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ дорівнює числу $p-1$ різних можливих значень $s \in \mathbb{Z}_p, s \neq 0$.

Таким чином, порядок групи $CGL_{b,k}(2, \mathbb{Z}_p)$ дорівнює $(p-1)p + p - 1 = p^2 - 1$.

Твердження доведено.

Звідси $CGL_{b,k}(2, \mathbb{Z}_p)$ для $D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p$ є мультиплікативною абелевою групою порядку $p^2 - 1$.

Зауваження 1.1 (з [70]). Кількість ненульових значень $D \in \mathbb{Z}_p : D = u^2 \in \mathbb{Z}_p$ і кількість значень $D \in \mathbb{Z}_p : D \neq u^2 \in \mathbb{Z}_p$ за простого $p \geq 3$ однакові й дорівнюють $\frac{p-1}{2}$.

Надалі

прийmemo

$$CGL_{b,k}(2, \mathbb{Z}_p) = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{matrix} t, s, a, b, k \in \mathbb{Z}_p, t, s \neq 0, \\ D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p \end{matrix} \right\}.$$

1.5. Діагоналізація матриць групи $CGL_{b,k}(2, \mathbb{Z}_p)$

Відповідно до [67] перестановочні матриці простої структури можна одночасно, тобто одним і тим же перетворенням подібності, привести до діагонального виду.

Під матрицями простої структури розуміють матриці, які мають n лінійно незалежних власних векторів [67]. Оскільки власні вектори, які відповідають попарно різним характеристичним числам, завжди лінійно незалежні, для того, щоб матриця мала просту структуру, достатньо, щоб усі корені характеристичного рівняння були різні [67], [71].

Характеристичний поліном матриці $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \in CGL_{b,k}(2, \mathbb{Z}_p)$

$$\text{дорівнює } |A - \lambda E| = \begin{vmatrix} a - \lambda & 1 \\ b & a + k - \lambda \end{vmatrix} = \lambda^2 - (2a + k)\lambda + a(a + k) - b, \text{ де } E -$$

одинична матриця розмірності $n = 2$.

Дискримінант характеристичного рівняння $D = (2a + k)^2 - 4(a^2 + ak - b) = k^2 + 4b$. У випадку, коли значення D не є квадратичним лишком у простому полі лишків \mathbb{Z}_p ($D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p$), характеристичний поліном не має коренів у \mathbb{Z}_p . Оскільки степінь рівняння $n = 2$, поліном незвідний над полем \mathbb{Z}_p .

Розглянемо незвідний поліном $f(x) = x^2 - D \in \mathbb{Z}_p[x]$. Просте алгебраїчне розширення степеня 2 поля \mathbb{Z}_p позначимо як $F_{p^2} = \mathbb{Z}_p[\sqrt{D}]$ [72], де $D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p$.

Поле Галуа F_{p^2} має характеристику p і степінь 2 [6].

Зауваження 1.2 (з [45]). Поле F_{p^2} є поле розкладання для характеристичних поліномів матриць із групи $CGL_{b,k}(2, \mathbb{Z}_p)$. Власні значення матриці $tA = t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ над полем $F_{p^2} = \mathbb{Z}_p[\sqrt{D}]$:

$$\lambda_{1,2}(a, t) = \frac{t}{2} (2a + k \pm \sqrt{D}), \quad t \neq 0. \quad (1.2)$$

Для матриці tA , $t \neq 0$, характеристичне рівняння $|tA - \lambda E| = t^2 \left| A - \frac{\lambda}{t} E \right| = 0$, звідки $\lambda_{1,2}(a, t) = t \cdot \lambda_{1,2}(a)$, де $\lambda_{1,2}(a)$ – власні значення матриці $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ над полем $F_{p^2} = \mathbb{Z}_p[\sqrt{D}]$.

Якщо $\lambda(a, t) = \frac{t}{2} (2a + k \pm \sqrt{D})$ є одним з коренів незвідного в \mathbb{Z}_p характеристичного рівняння, де $\lambda \in F_{p^2}$, то в силу теореми 2.14 з [6] інший корінь рівняння дорівнює $\lambda^p(a, t) = \frac{t}{2} (2a + k \mp \sqrt{D})$.

Для матриці sE власні значення $\lambda_{1,2}(s) = s \neq 0$.

Лема 1.3.19 з [71] засвідчує те, що сімейство діагоналізованих матриць є комутативним сімейством тоді і тільки тоді, коли воно одночасно діагоналізоване. На основі цієї леми сформульовано наступне зауваження.

Зауваження 1.3 (з [45]). Комутативне сімейство матриць $CGL_{b,k}(2, \mathbb{Z}_p)$ над полем $F_{p^2} = \mathbb{Z}_p[\sqrt{D}]$ одночасно діагоналізоване, тобто існує матриця

$C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$ з елементами з F_{p^2} , така, що для кожної матриці

$A \in CGL_{b,k}(2, \mathbb{Z}_p)$ добуток $C^{-1} \cdot A \cdot C$ є діагональною матрицею:

$$C^{-1} \cdot A \cdot C = \begin{pmatrix} \lambda_1(a, t) & 0 \\ 0 & \lambda_2(a, t) \end{pmatrix}.$$

Оскільки $C^{-1} \cdot A \cdot C = \begin{pmatrix} \lambda_1(a, t) & 0 \\ 0 & \lambda_2(a, t) \end{pmatrix}$, то

$$t \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \cdot \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \begin{pmatrix} \lambda_1(a, t) & 0 \\ 0 & \lambda_2(a, t) \end{pmatrix}. \text{ Виконавши множення}$$

матриць і їх порівняння, можна отримати:

$$\begin{cases} t(ac_{11} + c_{21}) = c_{11}\lambda_1(a, t), \\ t(bc_{11} + (a+k)c_{21}) = c_{21}\lambda_1(a, t), \\ t(ac_{12} + c_{22}) = c_{12}\lambda_2(a, t), \\ t(bc_{12} + (a+k)c_{22}) = c_{22}\lambda_2(a, t). \end{cases} \quad (1.3)$$

Враховуючи $\lambda_{1,2}(a, t) = t \cdot \lambda_{1,2}(a)$, остання система рівнянь може бути представлена як:

$$\begin{cases} ac_{11} + c_{21} = c_{11}\lambda_1(a), \\ bc_{11} + (a+k)c_{21} = c_{21}\lambda_1(a), \\ ac_{12} + c_{22} = c_{12}\lambda_2(a), \\ bc_{12} + (a+k)c_{22} = c_{22}\lambda_2(a); \end{cases} \Rightarrow \begin{cases} (a - \lambda_1(a))c_{11} + c_{21} = 0, \\ bc_{11} + (a+k - \lambda_1(a))c_{21} = 0, \\ (a - \lambda_2(a))c_{12} + c_{22} = 0, \\ bc_{12} + (a+k - \lambda_2(a))c_{22} = 0. \end{cases} \quad (1.4)$$

Нехай $\lambda_1(a) = \frac{2a+k+\sqrt{D}}{2}$. Тоді $\lambda_2(a) = \frac{2a+k-\sqrt{D}}{2}$.

З перших двох рівнянь системи:

$$\begin{cases} c_{21} = \frac{k + \sqrt{D}}{2} c_{11}, \\ bc_{11} + \left(\frac{k - \sqrt{D}}{2} \right) c_{21} = 0. \end{cases} \quad (1.5)$$

Нехай $c_{11} = 1$ у (1.5). Тоді $c_{21} = \frac{k + \sqrt{D}}{2}$ і перший власний вектор матриці

C дорівнює:

$$\bar{e}_1 = \begin{pmatrix} 1 \\ \frac{k + \sqrt{D}}{2} \end{pmatrix}. \quad (1.6)$$

Аналогічно, з інших двох рівнянь системи можна знайти другий власний вектор матриці C :

$$\bar{e}_2 = \begin{pmatrix} 1 \\ \frac{k - \sqrt{D}}{2} \end{pmatrix}. \quad (1.7)$$

Тоді $C = \begin{pmatrix} 1 & 1 \\ \frac{k + \sqrt{D}}{2} & \frac{k - \sqrt{D}}{2} \end{pmatrix}$. Відповідно матриця C не залежить від

значень a і t та є спільною для $CGL_{b,k}(2, \mathbb{Z}_p)$.

Перевірка:

$$\begin{aligned} C^{-1} \cdot A \cdot C &= \frac{1}{|C|} \begin{pmatrix} \frac{k - \sqrt{D}}{2} & -1 \\ -\frac{k + \sqrt{D}}{2} & 1 \end{pmatrix} t \begin{pmatrix} a & 1 \\ b & a + k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \frac{k + \sqrt{D}}{2} & \frac{k - \sqrt{D}}{2} \end{pmatrix} = \\ &= t \begin{pmatrix} \frac{2a + k + \sqrt{D}}{2} & 0 \\ 0 & \frac{2a + k + \sqrt{D}}{2} \end{pmatrix} = \begin{pmatrix} \lambda_1(a, t) & 0 \\ 0 & \lambda_2(a, t) \end{pmatrix}. \end{aligned}$$

Множина D_λ невідроджених діагональних матриць над полем $F_{p^2} = \mathbb{Z}_p[\sqrt{D}]$:

$$D_\lambda = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^p \end{pmatrix}, \lambda \in F_{p^2} \right\}. \quad (1.8)$$

Зауваження 1.4 (з [45]). Відображення $g(A) = C^{-1} \cdot A \cdot C$ задає взаємнооднозначну відповідність (бієкцію) між матрицями $A \in CGL_{b,k}(2, \mathbb{Z}_p)$ та діагональними матрицями з D_λ , тобто $g : CGL_{b,k}(2, \mathbb{Z}_p) \leftrightarrow D_\lambda$.

Доведення (з [45]).

Якщо задано матриці $A_1, A_2 \in CGL_{b,k}(2, \mathbb{Z}_p)$, $A_1 \neq A_2$, а λ_1, λ_1^p і λ_2, λ_2^p – власні значення матриць A_1 і A_2 відповідно, то $C^{-1} \cdot \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1^p \end{pmatrix} \cdot C \neq C^{-1} \cdot \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_2^p \end{pmatrix} \cdot C \Leftrightarrow \lambda_1 \neq \lambda_2$.

Кількість різних матриць множини D_λ дорівнює $p^2 - 1$, що відповідає порядку мультиплікативної абелевої групи $CGL_{b,k}(2, \mathbb{Z}_p)$. Це означає, що відображення $g = g(A)$ встановлює взаємнооднозначну відповідність між $CGL_{b,k}(2, \mathbb{Z}_p)$ і D_λ .

Нехай $F_{b,k} = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, t, s, a, b, k \in \mathbb{Z}_p, D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p \right\}$ – сімейство матриць, де p – просте, b, k – фіксовані в \mathbb{Z}_p .

Твердження 1.4 (з [45]). Сімейство матриць $F_{b,k}$ утворює поле Галуа порядку p^2 зі звичайними операціями множення та додавання матриць.

Доведення (з [45]).

Очевидно, що $F_{b,k} = CGL_{b,k}(2, \mathbb{Z}_p) \cup \Theta$, де $\Theta = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Нобхідно показати замкнутість операції додавання в множині $F_{b,k}$.

Відповідно до зауважень 1.3 і 1.4, для довільних матриць A_1 і A_2 з $F_{b,k}$ існує одна й та ж матриця C така, що:

$$\begin{cases} A_1 = C \cdot \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1^p \end{pmatrix} \cdot C^{-1}, \\ A_2 = C \cdot \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_2^p \end{pmatrix} \cdot C^{-1}; \end{cases} \Rightarrow A_1 + A_2 = C \cdot \begin{pmatrix} \lambda_1 + \lambda_2 & 0 \\ 0 & \lambda_1^p + \lambda_2^p \end{pmatrix} \cdot C^{-1}. \quad (1.9)$$

Поле Галуа $F_{p^2} = \mathbb{Z}_p[\sqrt{D}]$ має характеристику p . Тому в силу пропозиції 7.1.4 із [72] виконується рівність $\lambda_1^p + \lambda_2^p = (\lambda_1 + \lambda_2)^p$. Тоді для

$$\lambda_3 = \lambda_1 + \lambda_2: \quad A_1 + A_2 = C \cdot \begin{pmatrix} \lambda_3 & 0 \\ 0 & \lambda_3^p \end{pmatrix} \cdot C^{-1} \quad \text{або} \quad C^{-1} \cdot (A_1 + A_2) \cdot C = \begin{pmatrix} \lambda_3 & 0 \\ 0 & \lambda_3^p \end{pmatrix} \in D_\lambda.$$

Очевидно, що $C^{-1} \cdot \Theta \cdot C = \Theta$. Згідно з зауваженням 1.4, існує єдина матриця

$$A_3 \in CGL_{b,k}(2, \mathbb{Z}_p), \quad \text{що} \quad C^{-1} \cdot A_3 \cdot C = \begin{pmatrix} \lambda_3 & 0 \\ 0 & \lambda_3^p \end{pmatrix}, \quad \lambda_3 \in F_{p^2}. \quad \text{Відповідно,}$$

$$A_1 + A_2 = A_3 \in F_{b,k}.$$

Таким чином, сімейство матриць $F_{b,k}$ може бути представлене з допомогою матриці C у вигляді: $F_{b,k} = \left\{ C \cdot \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^p \end{pmatrix} \cdot C^{-1}, \lambda \in F_{p^2} = \mathbb{Z}_p[\sqrt{D}] \right\}$.

$F_{b,k}$ є алгебраїчним полем для звичайних операцій над матрицями, а його порядок дорівнює p^2 . ■

Наслідок 1 (з [45]). Мультиплікативна група $F_{b,k}^*$ скінченного поля $F_{b,k}$ циклічна, тобто група $CGL_{b,k}(2, \mathbb{Z}_p)$ – циклічна.

Наслідок 2 (з [45]). У полі $F_{b,k}$ кількість примітивних елементів дорівнює $\varphi(p^2 - 1)$, де $\varphi(m)$ – функція Ейлера від m .

1.6. Мета та завдання дисертаційного дослідження

Метою дисертаційного дослідження є підвищення криптографічної стійкості засобів захисту інформації в комп'ютерних системах і мережах за рахунок використання скінченних полів квадратних матриць другого порядку та їх примітивних елементів, що забезпечують розширення порядку мультиплікативної групи, придатної для реалізації криптографічних протоколів узгодження ключів і електронного цифрового підпису.

Для досягнення поставленої мети в роботі необхідно розв'язати такі завдання:

- провести аналіз сучасного стану використання скінченних полів і матричних структур у криптографічних застосуваннях та обґрунтувати доцільність застосування скінченних полів квадратних матриць другого порядку в комп'ютерних системах і мережах. Встановити умови існування, структуру та властивості скінченних полів квадратних матриць другого порядку над полем простих лишків, істотні для побудови криптографічних перетворень;
- розробити метод вибору примітивних елементів скінченних полів квадратних матриць другого порядку за заданих параметрів поля;
- розробити метод вибору параметрів скінченних полів квадратних матриць другого порядку та їх примітивних елементів, який забезпечує формування матричних полів, придатних для криптографічного застосування;
- удосконалити реалізацію криптографічних протоколів узгодження ключів Діффі-Хеллмана та електронного цифрового підпису Ель-Гамала шляхом перенесення операцій у скінченні поля квадратних матриць другого порядку. Провести практичне дослідження статистичних властивостей і обчислювальної складності запропонованих криптографічних рішень і оцінити їх ефективність порівняно з класичними реалізаціями над полем \mathbb{Z}_p .

1.7. Висновки до розділу 1

У першому розділі дисертації проведено аналіз сучасного стану використання скінченних полів і матричних структур у криптографічних застосуваннях та встановлено, що матриці над скінченними полями можуть бути ефективним математичним інструментом для побудови нових криптографічних перетворень. Показано, що сам по собі перехід від скалярних елементів до матричних структур не гарантує підвищення криптографічної стійкості, оскільки за відсутності строго визначеної алгебраїчної основи такі побудови можуть зводитися до лінійних задач і допускати ефективний криптоаналіз.

На основі аналізу відомих наукових джерел і наведених теоретичних положень встановлено, що перспективним напрямом є побудова скінченних полів матриць, а не довільних множин або груп матриць. Такий підхід дає можливість перенести на матричні елементи фундаментальні властивості скінченних полів, зокрема циклічність мультиплікативної групи, існування примітивних елементів і можливість конструктивного вибору генераторів великого порядку.

Розглянуто комутативні сімейства матриць другого порядку над полем простих лишків та виділено клас матриць, який разом з одиничною матрицею утворює абелеву групу за множенням. Показано, що за відповідного вибору параметрів таке сімейство матриць допускає одночасну діагоналізацію в квадратичному розширенні базового поля та перебуває у взаємнооднозначній відповідності з елементами поля Галуа порядку p^2 . Це, у свою чергу, дозволяє обґрунтувати існування скінченного поля квадратних матриць другого порядку зі звичайними операціями додавання і множення матриць.

Встановлено, що мультиплікативна група такого поля матриць є циклічною і має порядок $p^2 - 1$, а кількість її примітивних елементів визначається функцією Ейлера. У криптографічному аспекті це означає, що використання скінченного поля квадратних матриць другого порядку дає

змогу збільшити порядок мультиплікативної групи порівняно з базовим полем \mathbb{F}_q , а отже – розширити простір криптографічних параметрів і підвищити обчислювальну складність атак, що ґрунтуються на розв’язуванні задачі дискретного логарифмування.

Таким чином, результати першого розділу підтверджують доцільність використання скінченних полів квадратних матриць другого порядку як математичної основи для вдосконалення криптографічних протоколів узгодження ключів і електронного цифрового підпису. Отримані положення становлять теоретичне підґрунтя для подальшого розроблення методів вибору параметрів матричних полів, пошуку їх примітивних елементів і практичної реалізації криптографічних схем на цій основі.

РОЗДІЛ 2. МЕТОД ВИБОРУ ПРИМІТИВНИХ ЕЛЕМЕНТІВ СКІНЧЕННИХ ПОЛІВ КВАДРАТНИХ МАТРИЦЬ ДРУГОГО ПОРЯДКУ

2.1. Вступ

Як показано в першому розділі, скінченні поля та комутативні перетворення в них є базовими елементами криптографічних алгоритмів у комп'ютерних системах і мережах.

У першому розділі також продемонстровано результати досліджень [44], [45], які дозволили сформулювати сімейство квадратних матриць порядку 2 над полем простих чисел за модулем p , що утворює скінченне поле порядку p^2 зі звичайними операціями множення та додавання матриць.

Так, сімейство матриць

$$F_{b,k} = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p \right\}, \text{ де } p - \text{просте, } b, k -$$

фіксовані в \mathbb{Z}_p , утворює поле Галуа порядку p^2 зі звичайними операціями множення та додавання матриць.

Разом з тим, для використання скінченного поля $F_{b,k}$ в криптографічних застосуваннях, зокрема в протоколі узгодження ключа Діффі-Хеллмана [1], потрібно вміти визначати його примітивні елементи.

Цей розділ спрямовано на визначення умов, за яких матриця є примітивним елементом скінченного поля, а також на методику знаходження всіх примітивних елементів поля матриць.

2.2. Умови для генератора мультиплікативної групи скінченного поля матриць

Сформулюємо наступні означення.

Означення 2.1. Послідовність $A, A^2, \dots, A^l = \delta \cdot E$ степенів матриці $A \in F_{b,k}$ називається ланцюгом степенів довжини l , якщо для $n < l$: $A^n \neq s \cdot E$, де $\delta, s \in \mathbb{Z}_p$.

Рівність $l = 1$ означає, що $A = \delta \cdot E$, $\delta \in \mathbb{Z}_p$.

Означення 2.2. Довжину l ланцюга степенів матриці A будемо називати періодом матриці A і позначатимемо $period(A) = l$.

Зауважимо, що $period(A) \leq ord(A)$, де $ord(A)$ – порядок матриці A як елемента мультиплікативної групи $F_{b,k}^*$.

Розглянемо матрицю $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \in CGL_{b,k}(2, \mathbb{Z}_p)$ для $t=1$, де

$$CGL_{b,k}(2, \mathbb{Z}_p) = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, t, s, a, b, k \in \mathbb{Z}_p, t, s \neq 0, a(a+k) - b \neq 0 \right\}$$

є мультиплікативною групою $F_{b,k}^*$ скінченного поля $F_{b,k}$ [44]. Тоді визначник $\det(A) = \Delta_a = a(a+k) - b \neq 0$.

Характеристичне рівняння матриці A має вигляд $\lambda^2 - (2a+k)\lambda + [a(a+k) - b] = 0$ або $\lambda^2 - (2a+k)\lambda + \Delta_a = 0$.

Корені характеристичного рівняння $\lambda_{1,2}(a)$ є власними значеннями матриці A . Далі значення $\lambda_{1,2}(a)$ будемо скорочено позначати через $\lambda_{1,2}$.

Нагадаємо, що перестановочні матриці простої структури можна одночасно привести до діагонального виду [67]. Для того, щоб матриця мала просту структуру (мала n лінійно незалежних власних векторів), достатньо, щоб усі корені характеристичного рівняння були різні [67], [73]. Необхідною та достатньою умовою для цього є нерівність нулю дискримінанта характеристичного рівняння $D = (2a+k)^2 - 4(a^2 + ak - b) = k^2 + 4b$.

Розглянемо два випадки для $D \neq 0$.

Випадок 1. Дискримінант характеристичного рівняння D є квадратичним лишком у простому полі лишків \mathbb{Z}_p ($D = k^2 + 4b = u^2 \in \mathbb{Z}_p, u \neq 0$).

Тоді $\exists \lambda_{1,2} \in \mathbb{Z}_p$, $\lambda_1 \neq \lambda_2$, а матриця A діагоналізована:
 $\exists C, C^{-1} : C^{-1}AC = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, а $A = C \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} C^{-1}$. Таким чином,
 $A^n = C \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} C^{-1}$.

Зазначимо, що згідно з малою теоремою Ферма [74] для простого p :

$\lambda_{1,2}^{p-1} = 1$. Тому $A^{p-1} = C \begin{pmatrix} \lambda_1^{p-1} & 0 \\ 0 & \lambda_2^{p-1} \end{pmatrix} C^{-1} = CEC^{-1} = E$, де E – одинична матриця.

Таким чином, порядок матриці A як породжувального елемента циклічної підгрупи дорівнює найменшому спільному кратному порядків елементів $\lambda_{1,2}$ у \mathbb{Z}_p і не перевищує значення $p-1$. Якщо порядки елементів $\lambda_{1,2}$ взаємно прості або хоча б один з елементів $\lambda_{1,2}$ є примітивним у \mathbb{Z}_p , порядок елемента A циклічної підгрупи є максимальним і дорівнює $p-1$.

Випадок 2. Дискримінант характеристичного рівняння D не є квадратичним лишком у простому полі лишків \mathbb{Z}_p ($D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p$).

Тоді характеристичний поліном не має коренів у \mathbb{Z}_p , а власні значення $\lambda_{1,2}$ матриці A містяться в полі $F_{p^2} = \mathbb{Z}_p[\sqrt{D}]$ розкладання для характеристичних поліномів другого степеня над \mathbb{Z}_p . Причому в силу теореми 2.14 з [6] $\lambda_1 = \lambda_2^p$ і $\lambda_2 = \lambda_1^p$ для простого p .

Оскільки характеристичне рівняння матриці A має вигляд $\lambda^2 - (2a + k)\lambda + \Delta_a = 0$, то за формулою Вієта [75] $\lambda_1\lambda_2 = \Delta_a = \lambda_1\lambda_1^p = \lambda_1^{p+1} = \lambda_2^{p+1}$. Тому

$$A^{p+1} = C \begin{pmatrix} \lambda_1^{p+1} & 0 \\ 0 & \lambda_2^{p+1} \end{pmatrix} C^{-1} = C \begin{pmatrix} \Delta_a & 0 \\ 0 & \Delta_a \end{pmatrix} C^{-1} = \Delta_a E, \quad (2.1)$$

де $\Delta_a \in \mathbb{Z}_p$.

Із формули (2.1) слідує, що

$$\text{period}(A) \leq p+1, \quad (2.2)$$

Зауваження 2.1. Нехай $A \in F_{b,k}$. Тоді $l = \text{period}(A)$ є дільником $p+1$, тобто $p+1 = l \cdot q$. Водночас $\det(A) = \Delta_a = \delta^q$ і $\Delta_a^l = \delta^2$, де $A^l = \delta \cdot E$.

Доведення.

Представимо число $p+1$ у вигляді $p+1 = l \cdot q + r$, де $0 \leq r \leq l-1$. Згідно з (2.1) запишемо: $\Delta_a E = A^{p+1} = A^{lq} \cdot A^r = (\delta E)^q \cdot A^r = \delta^q \cdot A^r$. У силу означення 2.2 для $l = \text{period}(A)$, маємо рівності $r=0$ і $\Delta_a = \delta^q$. Оскільки $A^l = \delta \cdot E$, то $\det(A^l) = \det(\delta \cdot E)$ або $\Delta_a^l = \delta^2$. ■

Твердження 2.1. Якщо $A \in F_{b,k}$, то наступні чотири речення є рівносильними:

- 1) $\text{period}(A) = p+1$;
- 2) $A^n \neq s \cdot E$ для $1 \leq n \leq \frac{p+1}{2}$;
- 3) $A \neq s \cdot E$ і елементи послідовності $u_{n+1} = \text{tr}(A)u_n - \det(A)u_{n-1}$, $\text{tr}(A)$ – слід матриці A [69], $u_0 = 0$, $u_1 = 1$, за $1 \leq n \leq \frac{p+1}{2}$ не дорівнюють нулю: $u_n \neq 0$;
- 4) $A^{\frac{p+1}{n}} \neq s \cdot E$ для всіх простих n -дільників $p+1$.

Доведення.

Покажемо, що вираз 1) еквівалентний виразу 2). Із умови $\text{period}(A) = p+1$ слідує, що $A^n \neq s \cdot E$, $1 \leq n \leq \frac{p+1}{2}$, звідки

$period(A) = l > \frac{p+1}{2}$. Тоді, в силу зауваження 2.1, $\begin{cases} (p+1):l; \\ l > \frac{p+1}{2}; \end{cases}$ звідки

$p+1 = l = period(A)$, отже вираз 1) еквівалентний виразу 2).

У [68] показано, що для квадратної матриці $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ її степінь

$$A^n = \begin{pmatrix} u_{n+1} - du_n & bu_n \\ cu_n & u_{n+1} - au_n \end{pmatrix}, \text{ де } u_{n+1} = tr(A)u_n - \det(A)u_{n-1}, u_0 = 0, u_1 = 1. \text{ Якщо}$$

серед елементів b і c є ненульовий, то $A^n = s \cdot E$ тоді і тільки тоді, коли $u_n = 0$

:

$$A^n \neq s \cdot E \Leftrightarrow u_n \neq 0. \quad (2.3)$$

Останнє твердження свідчить, що вираз 2) еквівалентний виразу 3) для $A \neq s \cdot E$.

Очевидно, що для простого n виконується нерівність $\frac{p+1}{n} \leq \frac{p+1}{2}$. Тому

з виразу 2) слідує вираз 4). Нехай $(p+1):n$ і n – просте, таке, що

$$A^{\frac{p+1}{n}} \neq s \cdot E. \quad (2.4)$$

Якщо $period(A) = l < p+1$ і $A^l = \delta \cdot E$, згідно з зауваженням 2.1 число $p+1 = l \cdot q$. Представимо натуральне число $q \geq 2$ добутком $q = n \cdot f$, де n – деяке просте число. Тоді $p+1 = l \cdot n \cdot f$ і $A^{\frac{p+1}{n}} = (A^l)^f = \delta^f \cdot E$, що протирічить умові (2.4). ■

Твердження 2.2. Нехай $A \in F_{b,k}$ і $\det(A) = \Delta_a \neq u^2 \in \mathbb{Z}_p$. Тоді:

(а) якщо просте p є числом Мерсенна ($p = 2^m - 1$), то

$$period(A) = p+1;$$

(б) якщо $p \neq 2^m - 1$, то наступні чотири речення є рівносильними:

$$1) \ period(A) = p+1;$$

$$2) \quad A^n \neq s \cdot E \quad \text{для} \quad 1 \leq n \leq \frac{p+1}{g}, \quad \text{де}$$

$$g = \min \{ f = 2c + 1 : c \geq 1, (p+1) \vdots f \};$$

$$3) \quad \text{елементи послідовності} \quad u_{n+1} = \text{tr}(A)u_n - \det(A)u_{n-1}, \quad u_0 = 0,$$

$$u_1 = 1, \text{ за } 1 \leq n \leq \frac{p+1}{g} \text{ не дорівнюють нулю: } u_n \neq 0;$$

$$4) \quad A^{\frac{p+1}{n}} \neq s \cdot E \quad \text{для всіх простих } n\text{-дільників } p+1 \text{ таких, що} \\ n \geq g \geq 3.$$

Доведення.

Нехай $l = \text{period}(A)$ і $\delta \cdot E = A^l$. У відповідності до зауваження 2.1 $\Delta_a = \delta^q$ і $p+1 = l \cdot q$. За $q = 2h$ значення $\Delta_a = (\delta^h)^2 = u^2$, що протирічить умові $\Delta_a \neq u^2$ твердження. Таким чином, число $p+1$ кратне періоду l за непарного $q = 2h+1$.

У пункті (а) величина $p+1 = 2^m$, а це означає, що $q = 1$ і $l = p+1$.

У пункті (б) величина $p+1 \neq 2^m$, тоді $p+1$ має непарні дільники $f \geq 3$ і значення $g = \min \{ f = 2c + 1 : c \geq 1, (p+1) \vdots f \} \geq 3$.

Покажемо, що речення 1) еквівалентне реченню 2). Із умови $\text{period}(A) = p+1$ слідує, що $A^n \neq s \cdot E$, $1 \leq n \leq \frac{p+1}{g} < p+1$.

Нехай тепер кратність $q = 2h+1 \geq 3$. Крім того, виконано наступні умови:

$$A^n \neq s \cdot E, \quad 1 \leq n \leq \frac{p+1}{g}. \quad (2.5)$$

Очевидно, що тоді $q = 2h+1 \geq g = \min \{ f = 2c + 1 : c \geq 1, (p+1) \vdots f \} = g \geq 3$,

а тому $\text{period}(A) = l = \frac{p+1}{q} \leq \frac{p+1}{g}$. У силу означення для $\text{period}(A) = l$,

$A^l = \delta \cdot E$, що протирічить умові (2.5). Отже, за умови виконання (2.4), кратність $q = 2h + 1 = 1$, а тому $l = p + 1$. Таким чином, з 2) слідує 1), а речення 1) еквівалентне реченню 2).

Рівносильність 2) і 3) легко слідує з співвідношення (2.3), оскільки $\det(s \cdot E) = s^2 \neq \det(A)$, звідки $A \neq s \cdot E$.

Речення 4), очевидно, слідує з 2), оскільки $\frac{p+1}{n} \leq \frac{p+1}{g}$. Нагадаємо, що частка $q = \frac{p+1}{l} = 2h + 1$ є непарним числом. Якщо $\text{period}(A) = l < p + 1$, то натуральне число $2h + 1 > 1$ записується добутком $2h + 1 = n \cdot f$, де n – деяке просте число. Тоді $p + 1 = l \cdot n \cdot f$, $n \geq 3$, та степінь $A^{\frac{p+1}{n}} = (A^l)^f = \delta^f \cdot E$, що протирічить умові (2.5). Отже, з речення 4) слідує речення 1). ■

Наслідок 2.1. Нехай $A = \begin{pmatrix} a & 1 \\ b & a + k \end{pmatrix} \in F_{b,k}$ і $\det(A) = \Delta_a \neq u^2 \in \mathbb{Z}_p$. Якщо

$p = 2q - 1$ з простим числом $q \geq 3$, то тільки для $a \neq -\frac{k}{2}$ виконується $\text{period}(A) = p + 1$.

Доведення.

Згідно з реченням 3) пункту (б) твердження 2.2, для $p = 2q - 1$ значення $p + 1 = 2q$, а $g = q$. Умова $u_n \neq 0$, $1 \leq n \leq \frac{2q}{g} = 2$, з $u_0 = 0$, $u_1 = 1$ означає, що $u_2 = (2a + k) \cdot 1 - \Delta_a \cdot 0 = 2a + k \neq 0$ або $a \neq -\frac{k}{2}$. ■

Твердження 2.3. Нехай матриця $A \in F_{b,k}^*$ має $\text{period}(A) = l$ і $A^l = \delta \cdot E$. Тоді

$$\text{ord}(A) = \text{ord}(\delta) \cdot \text{period}(A). \quad (2.6)$$

Доведення.

Позначимо через h порядок δ в \mathbb{Z}_p^* , тобто $\text{ord}(\delta) = h$. Оскільки $A^h = (\delta \cdot E)^h = \delta^h \cdot E = E$, то $\text{ord}(A) \leq l \cdot h$.

Запишемо степені матриці $A, A^2, \dots, A^{l \cdot h - 1}, A^{l \cdot h} = E$ у вигляді блокової матриці розміру $h \cdot l$, враховуючи співвідношення (2.1) і (2.2):

$$\begin{pmatrix} A & A^2 & \dots & A^{l-1} & A^l = \delta \cdot E \\ \delta \cdot A & \delta \cdot A^2 & \dots & \delta \cdot A^{l-1} & \delta \cdot A^l = \delta^2 \cdot E \\ \delta^2 \cdot A & \delta^2 \cdot A^2 & \dots & \delta^2 \cdot A^{l-1} & \delta^2 \cdot A^l = \delta^3 \cdot E \\ \dots & \dots & \dots & \dots & \dots \\ \delta^{h-1} \cdot A & \delta^{h-1} \cdot A^2 & \dots & \delta^{h-1} \cdot A^{l-1} & \delta^{h-1} \cdot A^l = \delta^h \cdot E = E \end{pmatrix}. \quad (2.7)$$

Очевидно, що $\text{ord}(A) = l \cdot h$ тоді і тільки тоді, коли всі елементи в цій матриці різні. Розглянемо питання про можливість рівності двох довільних елементів у матриці (2.7): $\delta^u \cdot A^n = \delta^v \cdot A^m$, де $0 \leq u, v \leq h-1$, $1 \leq n, m \leq l$.

Не обмежуючи загальності, вважаємо, що $n \leq m$. Тоді $A^{m-n} = \delta^{u-v} \cdot E$, де $0 \leq m-n \leq l-1$.

У силу означення $\text{period}(A) = l$ маємо рівність $m-n=0$ або $m=n$. Звідси $\delta^{u-v} = 1 = \delta^{v-u}$, тобто $\delta^{|u-v|} = 1$, $0 \leq |u-v| \leq h-1$. Оскільки $\text{ord}(\delta) = h$ у \mathbb{Z}_p^* , то $|u-v| = 0$ або $u=v$. Отже, елементи $\delta^u \cdot A^n$ і $\delta^v \cdot A^m$ співпадають тільки за умов, коли $m=n$ і $u=v$. Звідси слідує, що в блоковій матриці (2.7) усі елементи різні. ■

Зауваження 2.2. Якщо $\text{period}(A) = l$ і $A^l = \delta \cdot E$, то для $\delta \cdot t \neq 0$:

- 1) $\text{period}(A) = \text{period}(t \cdot A)$;
- 2) $\text{ord}(t \cdot A) = \text{ord}(t^l \cdot \delta) \cdot \text{period}(A)$.

Доведення.

Нехай $\text{period}(A) = l$, $\text{period}(t \cdot A) = m$. Тоді $\begin{cases} A^l = \delta \cdot E, \\ (t \cdot A)^m = s \cdot E \end{cases}$ тоді і тільки

тоді, коли $\begin{cases} (t \cdot A)^l = t^l \cdot \delta \cdot E, \\ A^m = t^{-m} \cdot s \cdot E \end{cases}$, звідки слідує, що $\begin{cases} \text{period}(t \cdot A) = m \leq l, \\ \text{period}(A) = l \leq m \end{cases}$ або $m = l$

. Пункт 1) зауваження 2.2 доведено.

У силу формули (2.6) і пункту 1) зауваження 2.2:
 $\text{ord}(t \cdot A) = \text{ord}(x) \cdot \text{period}(t \cdot A) = \text{ord}(x) \cdot \text{period}(A)$, де
 $(t \cdot A)^l = x \cdot E = t^l \cdot \delta \cdot E$ або $x = t^l \cdot \delta$. Звідси слідує пункт 2) зауваження 2.2. ■

Твердження 2.4. Матриця $t \cdot A = t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \in F_{b,k}$ має

$\text{ord}(t \cdot A) = p^2 - 1$, тобто є примітивним елементом скінченного поля $F_{b,k}$
(генератором мультиплікативної групи $F_{b,k}^*$ поля $F_{b,k}$) тоді і тільки тоді, коли:

- 1) $\text{period}(A) = p + 1$;
- 2) $\det(A) = \Delta_a$ такий, що $t^2 \cdot \Delta_a$ є примітивним елементом поля \mathbb{Z}_p
(первісним коренем).

Доведення.

Нехай $l = \text{period}(A)$ і $\delta \cdot E = A^l$. Оскільки порядок мультиплікативної групи $|F_{b,k}^*| = p^2 - 1 \geq \text{ord}(t \cdot A)$, $\text{ord}(t^l \cdot \delta) \leq p - 1$ для $t^l \cdot \delta \in \mathbb{Z}_p$ і, згідно з (2.2), значення $\text{period}(A) \leq p + 1$, то із зауваження 2.2 слідує, що $\text{ord}(t \cdot A) \leq \text{ord}(t^l \cdot \delta) \cdot \text{period}(A) \leq (p - 1) \cdot (p + 1) = p^2 - 1$.

Тому $\text{ord}(t \cdot A) = p^2 - 1$ тоді і тільки тоді, коли $\begin{cases} \text{period}(A) = l = p + 1, \\ \text{ord}(t^l \cdot \delta) = p - 1 \end{cases}$ або

$$\begin{cases} \text{period}(A) = p + 1, \\ \text{ord}(t^{p-1} \cdot t^2 \cdot \delta) = p - 1. \end{cases}$$

За теоремою Ферма для \mathbb{Z}_p справедливо $t^{p-1} = 1$. Згідно з (2.1) маємо:
 $\delta \cdot E = A' = A^{p+1} = \Delta_a \cdot E$, тобто $\delta = \Delta_a$. Тоді $\text{ord}(1 \cdot t^2 \cdot \Delta_a) = p-1$, що означає
 примітивність $t^2 \cdot \Delta_a$ у полі \mathbb{Z}_p . ■

Зауваження 2.3. Якщо $\det(A) = \Delta_a = u^2 \in \mathbb{Z}_p$, то $t^2 \cdot \Delta_a = (tu)^2$ не є
 примітивним елементом поля \mathbb{Z}_p . Згідно з твердженням 2.4, матриця
 $t \cdot A \in F_{b,k}$ не є примітивним елементом поля $F_{b,k}$.

З пункту (а) твердження 2.2, наслідку 2.1 та твердження 2.4 очевидним
 чином слідує наступне зауваження.

Зауваження 2.4. Нехай $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \in F_{b,k}$, $\det(A) = \Delta_a \neq u^2 \in \mathbb{Z}_p$.

Якщо $p = 2^m - 1$ (число Мерсенна) або $p = 2q - 1$ з простим $q \geq 3$ і $a \neq -\frac{k}{2}$, то

матриця $t \cdot A = t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \in F_{b,k}$ є примітивним елементом поля $F_{b,k}$

(генератором мультиплікативної групи $F_{b,k}^*$) тоді і тільки тоді, коли елемент
 $\det(t \cdot A) = t^2 \cdot \Delta_a$ є примітивним у полі \mathbb{Z}_p (генератором \mathbb{Z}_p^*).

Нехай σ – найменший первісний корінь у \mathbb{Z}_p . Тоді множину Σ всіх
 первісних коренів знаходять так [76]:

$$\Sigma = \{ \sigma^i : \langle i, p-1 \rangle = 1 \}. \quad (2.8)$$

Через $\text{ind} \Delta_a = \gamma$ позначимо індекс числа Δ_a за модулем p та основою
 σ , тобто $\Delta_a = \sigma^\gamma \pmod{p}$.

Зазвичай вважають, що $\gamma = 0, 1, 2, \dots, p-2$ – найменший невід'ємний
 лишок за модулем $p-1$. Оскільки значення $\sigma^i \in \Sigma$ є квадратичним нелишком
 у \mathbb{Z}_p , а для $\Delta_a \neq u^2$ число $\gamma = \text{ind} \Delta_a$ є непарним, то різниця $i - \gamma$ є парним
 числом. Отже, існують такі $t_i \in \mathbb{Z}_p$, що

$$\frac{\sigma^i}{\Delta_a} = \sigma^{i-\gamma} = \left(\sigma^{\frac{i-\gamma}{2}} \right)^2 = t_i^2, \langle i, p-1 \rangle = 1.$$

Множина

$$T = \left\{ t_i = \pm \sigma^{\frac{i-\gamma}{2}} : \langle i, p-1 \rangle = 1, \gamma = \text{ind} \Delta_a \right\} \quad (2.9)$$

визначає весь можливий набір коефіцієнтів t_i , коли добуток $t_i^2 \cdot \Delta_a$ є примітивним елементом поля \mathbb{Z}_p . У відповідності до цього та твердження 2.4 сформулюємо наступний наслідок.

Наслідок 2.2. Нехай $t \cdot A = t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \in F_{b,k}$, $\text{period}(A) = p+1$,

$\det(A) = \Delta_a \neq u^2 \in \mathbb{Z}_p$, а σ – найменший первісний корінь у \mathbb{Z}_p . Тоді матриця $t \cdot A$ є примітивним елементом поля $F_{b,k}$ тоді і тільки тоді, коли коефіцієнт t – один із $2 \cdot \varphi(p-1)$ елементів множини T :

$$t \in T, \quad (2.10)$$

де множину T задано формулою (2.9).

Приклад 1.

Матриця $A = \begin{pmatrix} a & 1 \\ 9 & a+3 \end{pmatrix} \in F_{9,3}$ над \mathbb{Z}_{13} . Значення

$D = k^2 + 4b = 6 \neq u^2 \in \mathbb{Z}_{13}$. Для $a=1$ визначник $\Delta_a = \begin{vmatrix} 1 & 1 \\ 9 & 4 \end{vmatrix} = 8 \neq u^2 \in \mathbb{Z}_{13}$. Крім

того, $p+1 = 14 \neq 2^m$.

Для визначення $\text{period}(A)$ застосуємо пункт (б) твердження 2.2:

$g = \min \{ f = 2l+1 : l \geq 1, 14 : f \} = 7$, $\text{tr}(A) = 5$, $|A| = \Delta_a = 8$. Тоді послідовність

$u_{n+1} = 5u_n - 8u_{n-1}$, $u_0 = 0$, $u_1 = 1$ для $1 \leq n \leq \frac{p+1}{g} = \frac{14}{7} = 2$ набуває значень $u_1 = 1$,

$u_2 = 5$. Оскільки $u_n \neq 0$, $\text{period}(A) = p+1 = 14$.

Значення $\sigma = 2$ є найменшим первісним коренем у \mathbb{Z}_{13} , тому множина Σ усіх примітивних елементів поля \mathbb{Z}_{13} визначається так (див. (2.8)):

$$\Sigma = \{2^i : \langle i, 12 \rangle = 1\} = \{2^1, 2^5, 2^7, 2^{11}\}.$$

Знайдемо індекс γ для визначника $|A| = \Delta_a = 8$ за основи $\sigma = 2$: $\gamma = \text{ind} 8 = 3$. Для $i = 1, 5, 7, 11$ значення $\frac{i - \gamma}{2} = \frac{i - 3}{2} = -1, 1, 2, 4$.

Запишемо множину T у відповідності до (2.9), враховуючи, що $1 = 2^{p-1} = 2^{12}$: $T = \{\pm 2^{-1} = \pm 2^{11} = \pm 7, \pm 2^1, \pm 2^2 = \pm 4, \pm 2^4 = \pm 3\}$.

Відповідно до (2.10), значення $t \in \{\pm 2, \pm 3, \pm 4, \pm 7\}$, а кожна з наведених нижче матриць $t \cdot A$ є примітивним елементом поля $F_{9,3}$ над \mathbb{Z}_{13} : $\pm 2 \cdot \begin{pmatrix} 1 & 1 \\ 9 & 4 \end{pmatrix}$, $\pm 3 \cdot \begin{pmatrix} 1 & 1 \\ 9 & 4 \end{pmatrix}$, $\pm 4 \cdot \begin{pmatrix} 1 & 1 \\ 9 & 4 \end{pmatrix}$, $\pm 7 \cdot \begin{pmatrix} 1 & 1 \\ 9 & 4 \end{pmatrix}$. Водночас, $\Delta_a = 8 \notin \Sigma$, отже сама матриця $A = \begin{pmatrix} 1 & 1 \\ 9 & 4 \end{pmatrix}$ не є примітивним елементом поля $F_{9,3}$ над \mathbb{Z}_{13} .

Приклад 2.

Матриця $A = \begin{pmatrix} a & 1 \\ 11 & a+3 \end{pmatrix} \in F_{11,3}$ над \mathbb{Z}_{19} . Значення

$D = k^2 + 4b = 53 = 15 \neq u^2 \in \mathbb{Z}_{19}$. Для $a = 0$ визначник

$\Delta_a = \begin{vmatrix} 0 & 1 \\ 11 & 3 \end{vmatrix} = -11 = 8 \neq u^2 \in \mathbb{Z}_{19}$. Крім того, $p+1 = 20 \neq 2^m$.

Визначимо $\text{period}(A)$ для $a = 0$, застосовуючи пункт (б) твердження 2.2: $g = \min\{f = 2l+1 : l \geq 1, 20 \nmid f\} = 5$, $\text{tr}(A) = 3$, $|A| = \Delta_a = 8$. Тоді послідовність $u_{n+1} = 3u_n - 8u_{n-1}$, $u_0 = 0$, $u_1 = 1$ для $1 \leq n \leq \frac{p+1}{g} = \frac{20}{5} = 4$ набуває значень $u_1 = 1$, $u_2 = 3$, $u_3 = 1$, $u_4 = 17$. Оскільки $u_n \neq 0$, $\text{period}(A) = p+1 = 20$.

Найменшим первісним коренем у \mathbb{Z}_{19} є значення $\sigma = 2$, тому відповідно до (2.8) множина всіх примітивних елементів поля \mathbb{Z}_{19} : $\Sigma = \{2^i : \langle i, 18 \rangle = 1\} = \{2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}\}$.

Оскільки $\gamma = \text{ind} \Delta_a = \text{ind} 8 = 3$, а значення $\frac{i-\gamma}{2} = \frac{i-3}{2} = -1, 1, 2, 4, 5, 7$, множина T у відповідності до (2.9) має вигляд: $T = \{\pm 2^{-1} = \pm 10 = \mp 9, \pm 2^1, \pm 2^2 = \pm 4, \pm 2^4 = \pm 16 = \mp 3, \pm 2^5 = \pm 13 = \mp 6, \pm 2^7 = \pm 14 = \mp 5\}$.

Матриця $A = \begin{pmatrix} 0 & 1 \\ 11 & 3 \end{pmatrix}$ не є примітивним елементом поля $F_{11,3}$ над \mathbb{Z}_{19} ,

оскільки $\Delta_a = 8 \notin \Sigma$. Кожна ж з матриць $t \cdot A$ є примітивним елементом поля $F_{11,3}$ над \mathbb{Z}_{19} для $t \in \{\pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 9\}$.

Приклад 3.

Нехай $p = 31 = 2^5 - 1$ (число Мерсенна).

Значення $\sigma = 3$ є найменшим первісним коренем у \mathbb{Z}_{31} , тому відповідно до (2.8) множина всіх примітивних елементів \mathbb{Z}_{31} : $\Sigma = \{3^i : \langle i, 30 \rangle = 1\} = \{3^1, 3^7, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{29}\} = \{3, 17, 13, 24, 22, 12, 11, 21\}$ – усього $\varphi(p-1) = \varphi(30) = 8$ елементів.

Матриця $A = \begin{pmatrix} a & 1 \\ -1 & a+4 \end{pmatrix} \in F_{-1,4}$ над \mathbb{Z}_{31} . Значення

$D = k^2 + 4b = 12 \neq u^2 \in \mathbb{Z}_{31}$. Для $a = 16$ визначник

$\Delta_a = \begin{vmatrix} 16 & 1 \\ -1 & 20 \end{vmatrix} = 321 = 11 \neq u^2 \in \mathbb{Z}_{31}$. Оскільки $\Delta_a = 11 \in \Sigma$, то в силу зауваження

2.4 матриця $A = \begin{pmatrix} 16 & 1 \\ -1 & 20 \end{pmatrix}$ є примітивним елементом поля $F_{-1,4}$ над \mathbb{Z}_{31} :

$\text{ord}(A) = |F_{-1,4}| = p^2 - 1 = 960$.

Значення $\gamma = \text{ind} \Delta_a = \text{ind} 11 = 23$, тому для $\langle i, 30 \rangle = 1$:

$$\frac{i - \gamma}{2} = \frac{i - 23}{2} = -11, -8, -6, -5, -3, -2, 0, 3.$$

Враховуючи, що $1 = 3^{p-1} = 3^{30}$, множина T у відповідності до (2.9) записується так:

$$T = \left\{ \begin{array}{l} \pm 3^{19} = \pm 12, \pm 3^{22} = \pm 14, \pm 3^{24} = \pm 2, \pm 3^{25} = \pm 6, \pm 3^{27} = \pm 23 = \mp 8, \\ \pm 3^{28} = \pm 7, \pm 1, \pm 3^3 = \pm 27 = \mp 4 \end{array} \right\}.$$

Кожна матриця $t \cdot \begin{pmatrix} 16 & 1 \\ -1 & 20 \end{pmatrix}$, $t \in \{\pm 1, \pm 2, \pm 4, \pm 6, \pm 7, \pm 8, \pm 12, \pm 14\}$, є

примітивним елементом поля $F_{-1,4}$ над \mathbb{Z}_{31} .

Твердження 2.5. Існує рівно $\varphi(p+1)$ різних матриць

$$A_j = \begin{pmatrix} a_j & 1 \\ b & a_j + k \end{pmatrix} \in F_{b,k} \text{ над } \mathbb{Z}_p, \quad p \geq 3, \text{ з } \text{period}(A_j) = p+1 \text{ і } \det(A_j) \neq u^2 \in \mathbb{Z}_p,$$

що визначають усі $\varphi(p^2 - 1)$ примітивні елементи поля $F_{b,k}$ над \mathbb{Z}_p , а саме:

$$t_{ji} \cdot A_j, \text{ де } t_{ji} \in T_j = \left\{ \pm \sigma^{\frac{i-\gamma_j}{2}} : \langle i, p-1 \rangle = 1, \gamma_j = \text{ind}(\det(A_j)) \right\}, \quad 1 \leq j \leq \varphi(p+1), \quad \sigma -$$

найменший первісний корінь у \mathbb{Z}_p .

Доведення.

Оскільки для натурального f виконується рівність $\langle f, f+1 \rangle = 1$, то для послідовних парних чисел $p-1 = 2f$ і $p+1 = 2(f+1)$ їх найбільший спільний дільник $d = \langle p-1, p+1 \rangle = 2$. Тому значення функції Ейлера

$$\begin{aligned} \varphi(p^2 - 1) &= \varphi((p-1)(p+1)) = \frac{d}{\varphi(d)} \cdot \varphi(p-1) \cdot \varphi(p+1) = \\ &= 2 \cdot \varphi(p-1) \cdot \varphi(p+1) \end{aligned} \quad (2.11)$$

Якщо матриця $t \cdot A = t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ є примітивним елементом поля $F_{b,k}$

над \mathbb{Z}_p , то в силу твердження 2.4 і зауваження 2.3 маємо $\text{period}(A) = p+1$ і

$\det(A) = \Delta_a \neq u^2 \in \mathbb{Z}_p$. Згідно з наслідком 2.2 для $2 \cdot \varphi(p-1)$ коефіцієнтів t , визначених формулами (2.9) і (2.10), матриці $t \cdot A$ будуть примітивними елементами поля $F_{b,k}$. Тоді зі співвідношення (2.11) слідує, що різних матриць виду $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$, які відповідають примітивним елементам $t \cdot A$ поля $F_{b,k}$ над \mathbb{Z}_p , є рівно

$$\frac{\varphi(p^2-1)}{2 \cdot \varphi(p-1)} = \varphi(p+1). \quad (2.12)$$

Таким чином, існує набір матриць $A_j = \begin{pmatrix} a_j & 1 \\ b & a_j+k \end{pmatrix}$, $1 \leq j \leq \varphi(p+1)$, з $\text{period}(A_j) = p+1$ і $\det(A_j) \neq u^2 \in \mathbb{Z}_p$. Кожній матриці A_j відповідають коефіцієнти t_{ji} у кількості $2 \cdot \varphi(p-1)$ (див. (2.9)): $t_{ji} \in T_j = \left\{ \pm \sigma^{\frac{i-\gamma_j}{2}} : \langle i, p-1 \rangle = 1, \gamma_j = \text{ind}(\det(A_j)) \right\}$, де σ – найменший первісний корінь у \mathbb{Z}_p .

Отже, $\varphi(p^2-1)$ примітивних елементів поля $F_{b,k}$ над \mathbb{Z}_p представлено в вигляді $t_{ji} \cdot A_j$. Згідно з (2.12) та наслідком 2.2 кількість матриць $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \in F_{b,k}$ над \mathbb{Z}_p , що мають $\text{period}(A) = p+1$ і $\det(A) = \Delta_a \neq u^2 \in \mathbb{Z}_p$ співпадає з $\varphi(p+1)$. ■

Твердження 2.6. Нехай $A(a) = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \in F_{b,k}$ над \mathbb{Z}_p , де

$D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p$. Тоді матриці $A(a)$ і $A(-a-k)$ такі, що:

- 1) $\det(A(a)) = \det(A(-a-k)) = \Delta_a$;
- 2) $\text{period}(A(a)) = \text{period}(A(-a-k)) = l$;

3) $\text{ord}(t \cdot A(a)) = p^2 - 1$ тоді і тільки тоді, коли $\text{ord}(t \cdot A(-a - k)) = p^2 - 1$ для $t \in \mathbb{Z}_p$.

Доведення.

Легко бачити, що речення 1) твердження виконується:

$$\det(A(-a - k)) = \begin{vmatrix} -a - k & 1 \\ b & -a \end{vmatrix} = a(a + k) - b = \begin{vmatrix} a & 1 \\ b & a + k \end{vmatrix} = \Delta_a.$$

Корені характеристичного рівняння матриці $A(a)$: $\det(A(a) - \lambda E) = \lambda^2 - (2a + k)\lambda + \Delta_a = 0$ у квадратичному розширенні поля $\mathbb{Z}_p[\sqrt{D}]$ дорівнюють $\lambda_{1,2} = \frac{1}{2}[(2a + k) \pm \sqrt{D}]$. Для матриці $A(-a - k)$ характеристичне рівняння $\det(A(-a - k) - \mu E) = \mu^2 + (2a + k)\mu + \Delta_a = 0$ має корені $\mu_{1,2} = \frac{1}{2}[-(2a + k) \pm \sqrt{D}]$. Абелева група матриць $F_{b,k}^*$ над \mathbb{Z}_p одночасно діагоналізується в полі розкладу $\mathbb{Z}_p[\sqrt{D}]$ їх характеристичних

многочленів за допомогою матриці $C = \begin{pmatrix} 1 & 1 \\ \frac{k + \sqrt{D}}{2} & \frac{k - \sqrt{D}}{2} \end{pmatrix},$

$$C^{-1} = \frac{-1}{\sqrt{D}} \begin{pmatrix} \frac{k - \sqrt{D}}{2} & -1 \\ -\frac{k + \sqrt{D}}{2} & 1 \end{pmatrix} [45].$$

Так, для $A(a)$:

$$\begin{aligned} C^{-1} \cdot A(a) \cdot C &= \frac{-1}{\sqrt{D}} \begin{pmatrix} \frac{k - \sqrt{D}}{2} & -1 \\ -\frac{k + \sqrt{D}}{2} & 1 \end{pmatrix} \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_1 \frac{k + \sqrt{D}}{2} & \lambda_2 \frac{k - \sqrt{D}}{2} \end{pmatrix} = \\ &= \frac{-1}{\sqrt{D}} \begin{pmatrix} -\sqrt{D}\lambda_1 & 0 \\ 0 & -\sqrt{D}\lambda_2 \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}. \end{aligned}$$

Для матриці $A(-a-k)$:

$$\begin{aligned} C^{-1} \cdot A(-a-k) \cdot C &= \frac{-1}{\sqrt{D}} \begin{pmatrix} \frac{k-\sqrt{D}}{2} & -1 \\ -\frac{k+\sqrt{D}}{2} & 1 \end{pmatrix} \begin{pmatrix} -\lambda_2 & -\lambda_1 \\ -\lambda_2 \frac{k+\sqrt{D}}{2} & -\lambda_1 \frac{k-\sqrt{D}}{2} \end{pmatrix} = \\ &= \frac{-1}{\sqrt{D}} \begin{pmatrix} \sqrt{D}\lambda_2 & 0 \\ 0 & \sqrt{D}\lambda_1 \end{pmatrix} = \begin{pmatrix} -\lambda_2 & 0 \\ 0 & -\lambda_1 \end{pmatrix}. \end{aligned}$$

Зауважимо, що $\mu_1 = -\lambda_2 = -\frac{1}{2}[(2a+k) - \sqrt{D}]$ і

$\mu_2 = -\lambda_1 = -\frac{1}{2}[(2a+k) + \sqrt{D}]$. Тоді

$$\begin{cases} A^n(a) = \left\{ C \cdot \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \cdot C^{-1} \right\}^n = C \cdot \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \cdot C^{-1}, \\ A^n(-a-k) = \left\{ C \cdot \begin{pmatrix} -\lambda_2 & 0 \\ 0 & -\lambda_1 \end{pmatrix} \cdot C^{-1} \right\}^n = C \cdot \begin{pmatrix} (-\lambda_2)^n & 0 \\ 0 & (-\lambda_1)^n \end{pmatrix} \cdot C^{-1} = \\ = (-1)^n \cdot C \cdot \begin{pmatrix} \lambda_2^n & 0 \\ 0 & \lambda_1^n \end{pmatrix} \cdot C^{-1}. \end{cases}$$

Якщо $A^n(a) = \delta \cdot E$, $\delta \in \mathbb{Z}_p$, то $\begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} = \delta \cdot C^{-1} \cdot E \cdot C = \begin{pmatrix} \delta & 0 \\ 0 & \delta \end{pmatrix}$.

Оскільки $period(A(a)) = l$, то l є найменшим натуральним числом, за якого степені власних чисел $\lambda_1^n = \lambda_2^n = \delta \in \mathbb{Z}_p$. Тому $A^l(a) = \delta \cdot E$ тоді і тільки тоді, коли $A^l(-a-k) = (-1)^l \cdot \delta \cdot E$, що означає рівність $period(A(a)) = period(A(-a-k)) = l$. Речення 2) твердження доведено.

Розглянемо речення 3). У силу твердження 2.4, зауваження 2.3 і наслідку 2.2 умова $ord(t \cdot A(a)) = p^2 - 1$ означає, що $period(A(a)) = p + 1$,

$$\det(A(a)) = \Delta_a \neq u^2 \in \mathbb{Z}_p \quad i$$

$$t \in T = \left\{ \pm \sigma^{\frac{i-\gamma}{2}} : \langle i, p-1 \rangle = 1, \gamma = \text{ind} \Delta_a \right\} = \left\{ \pm \sqrt{\frac{\sigma^i}{\Delta_a}} : \langle i, p-1 \rangle = 1 \right\}.$$

Згідно з доведеними вище реченнями 1) і 2) твердження маємо $\text{period}(A(-a-k)) = p+1$, $\det(A(-a-k)) = \Delta_a \neq u^2 \in \mathbb{Z}_p$. Із наслідку 2.2 слідує, що за умови виконання (2.10) матриця $t \cdot A(-a-k)$ є примітивним елементом поля $F_{b,k}$ над \mathbb{Z}_p . Отже, із $\text{ord}(t \cdot A(a)) = p^2 - 1$ слідує $\text{ord}(t \cdot A(-a-k)) = p^2 - 1$. Позначивши $x = -a - k$, маємо, що з $\text{ord}(t \cdot A(-a-k)) = p^2 - 1 = \text{ord}(t \cdot A(x))$ слідує $\text{ord}(t \cdot A(-x-k)) = \text{ord}(t \cdot A(a)) = p^2 - 1$. Таким чином, речення 3) доведено. ■

2.3. Опис методу вибору примітивних елементів скінченних полів матриць другого порядку

Одержані в підрозділі 2.2 теоретичні результати дозволяють сформулювати метод вибору примітивних елементів скінченного поля матриць другого порядку. Розроблений метод орієнтовано не на безпосередній перебір усіх елементів поля, а на послідовне виділення таких матриць, для яких одночасно забезпечуються максимальний період у полі розширення та максимальний порядок визначника в базовому полі. Такий підхід дає змогу перейти від загальних умов примітивності до конструктивного формування множини всіх примітивних елементів поля $F_{b,k}$.

Розроблений метод вибору примітивних елементів поля $F_{b,k}$ полягає в наступному:

- 1) для матриці-кандидата $t \cdot A$ визначають її основні характеристики, а саме слід $\text{tr}(A)$, визначник $\det(A)$ та дискримінант характеристичного рівняння. Це дає змогу встановити характер власних значень матриці та

- віднести її до одного з двох випадків: коли характеристичний многочлен розкладається над \mathbb{Z}_p , або коли його корені належать лише квадратичному розширенню поля;
- 2) матриці A , для яких дискримінант є квадратичним лишком у полі \mathbb{Z}_p , відкидають як такі, що не можуть породжувати мультиплікативну групу поля $F_{b,k}$, оскільки в цьому випадку їх порядок обмежується порядком елементів базового поля. Подальший розгляд здійснюють лише для матриць, у яких дискримінант не є квадратичним лишком;
 - 3) для відібраних матриць перевіряють умову досягнення максимального можливого періоду в нерозкладному випадку, тобто умову $period(A) = p + 1$. Для цього використовують еквівалентні критерії, встановлені в підрозділі 2.2: через степені матриці, через відповідні значення сліду степенів матриці, а також через перевірку показників, пов'язаних із простими дільниками числа $p + 1$;
 - 4) після виділення матриць A із періодом $p + 1$ визначають порядок їх визначника в мультиплікативній групі поля \mathbb{Z}_p . Відповідно до встановлених тверджень, порядок матриці $t \cdot A$ в полі $F_{b,k}$ визначають періодом матриці A та порядком її визначника в \mathbb{Z}_p ;
 - 5) матрицю $t \cdot A$ визнають примітивним елементом поля $F_{b,k}$ тоді і тільки тоді, коли одночасно виконуються дві умови: її період дорівнює $p + 1$, а $t^2 \cdot \det(A)$ є примітивним елементом поля \mathbb{Z}_p . У такому разі порядок матриці $t \cdot A$ досягає значення $p^2 - 1$, тобто вона є генератором мультиплікативної групи поля $F_{b,k}$;
 - 6) завершальним етапом методу є об'єднання всіх отриманих матриць у повну множину примітивних елементів поля та контроль її повноти на основі встановлених співвідношень для кількості таких елементів.

Отже, розроблений метод задає загальну схему вибору примітивних елементів скінченного поля матриць другого порядку і зводить цю задачу до послідовної перевірки структури характеристичного рівняння, періоду матриці та примітивності її визначника в базовому полі.

2.4. Особливості застосування розробленого методу

Розглянемо поле $F_{9,3}$ над \mathbb{Z}_{13} . Визначимо всі примітивні елементи цього поля.

Оскільки порядок мультиплікативної групи $|F_{9,3}^*| = p^2 - 1 = 168$, то кількість примітивних елементів дорівнює $\varphi(p^2 - 1) = \varphi(12 \cdot 14) = \varphi(2^3 \cdot 3 \cdot 7) = 2^2 \cdot 2 \cdot 6 = 48$. Найменшим первісним коренем у \mathbb{Z}_{13} є $\sigma = 2$, а множина всіх примітивних елементів поля \mathbb{Z}_{13} становить $\Sigma = \{2^1, 2^5, 2^7, 2^{11}\}$ (див. приклад 1).

Згідно з твердженням 2.5 існує рівно $\varphi(p + 1) = \varphi(14) = 6$ різних матриць $A_j = \begin{pmatrix} a_j & 1 \\ 9 & a_j + 3 \end{pmatrix}$ з $\text{period}(A_j) = p + 1 = 14$, $\det(A_j) \neq u^2 \in \mathbb{Z}_{13}$, що визначають усі $\varphi(p^2 - 1) = 48$ примітивних елементів поля $F_{9,3}$ над \mathbb{Z}_{13} : $t_{ji} \cdot A_j$, де $t_{ji} \in \left\{ \pm 2^{\frac{1-\gamma_i}{2}}, \pm 2^{\frac{5-\gamma_i}{2}}, \pm 2^{\frac{7-\gamma_i}{2}}, \pm 2^{\frac{11-\gamma_i}{2}} \right\}$, $\gamma_j = \text{ind}(\det(A_j))$, $1 \leq j \leq 6$.

У силу твердження 2.6, матриці $A_j = \begin{pmatrix} a_j & 1 \\ 9 & a_j + 3 \end{pmatrix}$ і $\begin{pmatrix} -(a_j + 3) & 1 \\ 9 & -a_j \end{pmatrix}$ одночасно або є примітивними елементами, або ні. Число $p = 13$ можна представити в вигляді $p = 2 \cdot q - 1 = 2 \cdot 7 - 1$, де $q = 7 > 3$ – просте число. У силу наслідку 2.1 і зауваження 2.4, для $a_j \neq -\frac{k}{2} = 5$ усі матриці A_j з $\det(A_j) \neq u^2 \in \mathbb{Z}_{13}$ визначають примітивні елементи поля $F_{9,3}$ над \mathbb{Z}_{13} .

Наведемо відповідні пари матриць і з'ясуємо, чи є $\det(A_j)$ квадратичним лишком.

Нагадаємо, що для $x \in \mathbb{Z}_{13}$:

x	± 1	± 2	± 3	± 4	± 5	± 6
x^2	1	4	9	3	12	10

$$\text{Для } a_j = 0: \quad A_j = \begin{pmatrix} 0 & 1 \\ 9 & 3 \end{pmatrix}, \quad \begin{pmatrix} -(a_j + 3) & 1 \\ 9 & -a_j \end{pmatrix} = \begin{pmatrix} -3 & 1 \\ 9 & 0 \end{pmatrix} = \begin{pmatrix} 10 & 1 \\ 9 & 0 \end{pmatrix}, \quad \text{а}$$

$\det(A_j) = -9 = 4 = 2^2$. Такі матриці не задають примітивні елементи поля $F_{9,3}$ над \mathbb{Z}_{13} .

$$\text{Для } a_j = 1: \quad A_j = \begin{pmatrix} 1 & 1 \\ 9 & 4 \end{pmatrix}, \quad \begin{pmatrix} -(a_j + 3) & 1 \\ 9 & -a_j \end{pmatrix} = \begin{pmatrix} -4 & 1 \\ 9 & -1 \end{pmatrix} = \begin{pmatrix} 9 & 1 \\ 9 & 12 \end{pmatrix}, \quad \text{а}$$

$$\det(A_j) = -5 = 8 \neq u^2 \in \mathbb{Z}_{13}.$$

$$\text{Для } a_j = 2: \quad A_j = \begin{pmatrix} 2 & 1 \\ 9 & 5 \end{pmatrix}, \quad \begin{pmatrix} -(a_j + 3) & 1 \\ 9 & -a_j \end{pmatrix} = \begin{pmatrix} -5 & 1 \\ 9 & -2 \end{pmatrix} = \begin{pmatrix} 8 & 1 \\ 9 & 11 \end{pmatrix}, \quad \text{а}$$

$$\det(A_j) = 1 = 1^2. \text{ Такі матриці не задають примітивні елементи поля } F_{9,3} \text{ над } \mathbb{Z}_{13}$$

.

$$\text{Для } a_j = 3: \quad A_j = \begin{pmatrix} 3 & 1 \\ 9 & 6 \end{pmatrix}, \quad \begin{pmatrix} -(a_j + 3) & 1 \\ 9 & -a_j \end{pmatrix} = \begin{pmatrix} -6 & 1 \\ 9 & -3 \end{pmatrix} = \begin{pmatrix} 7 & 1 \\ 9 & 10 \end{pmatrix}, \quad \text{а}$$

$$\det(A_j) = 9 = 3^2. \text{ Такі матриці не задають примітивні елементи поля } F_{9,3} \text{ над } \mathbb{Z}_{13}.$$

$$\text{Для } a_j = 4: \quad A_j = \begin{pmatrix} 4 & 1 \\ 9 & 7 \end{pmatrix}, \quad \begin{pmatrix} -(a_j + 3) & 1 \\ 9 & -a_j \end{pmatrix} = \begin{pmatrix} -7 & 1 \\ 9 & -4 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 9 & 9 \end{pmatrix}, \quad \text{а}$$

$$\det(A_j) = 5 \neq u^2 \in \mathbb{Z}_{13}.$$

Для $a_j = 5$: $A_j = \begin{pmatrix} 5 & 1 \\ 9 & 8 \end{pmatrix}$, $\begin{pmatrix} -(a_j + 3) & 1 \\ 9 & -a_j \end{pmatrix} = \begin{pmatrix} -8 & 1 \\ 9 & -5 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 9 & 8 \end{pmatrix}$, а

$\det(A_j) = 5 \neq u^2 \in \mathbb{Z}_{13}$. Такі матриці не задають примітивні елементи поля $F_{9,3}$

над \mathbb{Z}_{13} , оскільки $a_j \neq -\frac{k}{2} = 5$.

Для $a_j = 11$: $A_j = \begin{pmatrix} 11 & 1 \\ 9 & 1 \end{pmatrix}$, $\begin{pmatrix} -(a_j + 3) & 1 \\ 9 & -a_j \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 9 & -11 \end{pmatrix} = \begin{pmatrix} 12 & 1 \\ 9 & 2 \end{pmatrix}$, а

$\det(A_j) = 2 \neq u^2 \in \mathbb{Z}_{13}$.

Для кожної пари матриць з періодом $p+1=14$, які знайдено для $a_j \in \{1, 4, 11\}$, визначимо відповідні їм примітивні елементи $\pm t_{ji} \cdot A_j$:

1) $A(1) = \begin{pmatrix} 1 & 1 \\ 9 & 4 \end{pmatrix}$, $A(9) = \begin{pmatrix} 9 & 1 \\ 9 & 12 \end{pmatrix}$. Визначник $\det(A(1)) = \det(A(9)) = 8$,

$\gamma = \text{ind} 8 = 3$. Для $i = 1, 5, 7, 11$ значення $\frac{i-3}{2} = -1, 1, 2, 4$, а множина

$T = \{\pm 2^{-1} = \pm 7 = \mp 6, \pm 2, \pm 4, \pm 3\}$. Отже, матриці $t \cdot \begin{pmatrix} 1 & 1 \\ 9 & 4 \end{pmatrix}$, $t \cdot \begin{pmatrix} 9 & 1 \\ 9 & 12 \end{pmatrix}$,

$t \in \{\pm 2, \pm 3, \pm 4, \pm 6\}$ є примітивними елементами поля $F_{9,3}$ над \mathbb{Z}_{13} ;

2) $A(4) = \begin{pmatrix} 4 & 1 \\ 9 & 7 \end{pmatrix}$, $A(6) = \begin{pmatrix} 6 & 1 \\ 9 & 9 \end{pmatrix}$. Визначник $\det(A(4)) = \det(A(6)) = 5$,

$\gamma = \text{ind} 5 = \text{ind}(2^9) = 9$. Для $i = 1, 5, 7, 11$ значення $\frac{i-9}{2} = -4, -2, -1, 1$.

Оскільки $-4 \equiv 8 \pmod{12}$, $-2 \equiv 10 \pmod{12}$, $-1 \equiv 11 \pmod{12}$, множина

$T = \{\pm 2^8 = \pm 9 = \mp 4, \pm 2^{10} = \pm 10 = \mp 3, \pm 2^{11} = \pm 7 = \mp 6, \pm 2\}$. Отже, матриці

$t \cdot \begin{pmatrix} 4 & 1 \\ 9 & 7 \end{pmatrix}$, $t \cdot \begin{pmatrix} 6 & 1 \\ 9 & 9 \end{pmatrix}$, $t \in \{\pm 2, \pm 3, \pm 4, \pm 6\}$ є примітивними елементами

поля $F_{9,3}$ над \mathbb{Z}_{13} ;

$$3) \quad A(11) = \begin{pmatrix} 11 & 1 \\ 9 & 1 \end{pmatrix}, \quad A(12) = \begin{pmatrix} 12 & 1 \\ 9 & 2 \end{pmatrix}. \quad \text{Визначник}$$

$\det(A(11)) = \det(A(12)) = 2$, $\gamma = \text{ind} 2 = 1$. Для $i = 1, 5, 7, 11$ значення

$$\frac{i-1}{2} = 0, 2, 3, 5. \quad \text{Тоді} \quad \text{множина}$$

$$T = \{\pm 2^0 = \pm 1, \pm 2^2 = \pm 4, \pm 2^3 = \pm 8 = \mp 5, \pm 2^5 = \pm 6\}. \quad \text{Отже, матриці}$$

$$t \cdot \begin{pmatrix} 11 & 1 \\ 9 & 1 \end{pmatrix}, \quad t \cdot \begin{pmatrix} 12 & 1 \\ 9 & 2 \end{pmatrix}, \quad t \in \{\pm 1, \pm 4, \pm 5, \pm 6\} \text{ є примітивними елементами}$$

поля $F_{9,3}$ над \mathbb{Z}_{13} .

Таким чином, знайдено всі 48 примітивних елементів поля $F_{9,3}$ над \mathbb{Z}_{13} .

2.5.Методика вибору примітивних елементів скінченних полів матриць другого порядку

Продемонстровані в підрозділі 2.4 особливості застосування розробленого методу вибору примітивних елементів поля $F_{b,k}$ над \mathbb{Z}_p дозволяють сформулювати методику, орієнтовану на практичне застосування в комп'ютерних системах. На відміну від методу, який визначає загальні умови та логіку відбору примітивних елементів, методика встановлює впорядковану послідовність обчислювальних дій, за допомогою яких у програмній реалізації формується повний перелік примітивних елементів поля матриць.

Методика вибору примітивних елементів скінченних полів матриць другого порядку включає такі етапи:

- 1) задають вхідні параметри поля: просте число p та фіксовані параметри, що визначають сімейство матриць другого порядку над \mathbb{Z}_p , яке утворює поле $F_{b,k}$. Одночасно обчислюють значення $p^2 - 1$, $p - 1$ і $p + 1$, а також виконують їх розклад на прості множники;

- 2) у базовому полі \mathbb{Z}_p визначають найменший первісний корінь і формують множину примітивних елементів цього поля. Цю інформацію використовують надалі для перевірки примітивності визначників і для побудови скалярних коефіцієнтів, що переводять матрицю з періодом $p + 1$ у примітивний елемент поля $F_{b,k}$;
- 3) для кожної матриці обчислюють слід, визначник і дискримінант характеристичного рівняння. Перевірку того, чи є дискримінант квадратичним лишком у \mathbb{Z}_p , виконують або за критерієм Ейлера, або за попередньо сформованою таблицею квадратичних лишків;
- 4) матриці з дискримінантом, що є квадратичним лишком, виключають з подальшого розгляду. Для решти матриць перевіряють умову $period(A) = p + 1$. У комп'ютерній реалізації доцільно перевіряти її не повним перебором степенів, а лише для показників, що відповідають простим дільникам числа $p + 1$, оскільки саме така перевірка забезпечує істотне скорочення обсягу обчислень;
- 5) для кожної матриці, що пройшла перевірку на період $p + 1$, визначають порядок її визначника в \mathbb{Z}_p . Якщо визначник є примітивним елементом базового поля, то таку матрицю безпосередньо заносять до множини примітивних елементів поля $F_{b,k}$;
- 6) якщо визначник матриці не є примітивним, але матриця має період $p + 1$, тоді за індексом визначника відносно найменшого первісного кореня обчислюють множину допустимих скалярних коефіцієнтів t . Для кожного такого коефіцієнта формують матрицю $t \cdot A$, яка вже є примітивним елементом поля $F_{b,k}$;
- 7) з урахуванням встановлених властивостей пар матриць $A(a)$ і $A(-a - k)$ програмній реалізації доцільно опрацьовувати їх узгоджено, що дозволяє уникнути повторних перевірок та дублювання результатів.

Повноту отриманої множини контролюють за кількістю знайдених примітивних елементів, яка має дорівнювати $\varphi(p^2 - 1)$;

- 8) на завершальному етапі формують упорядкований перелік усіх примітивних елементів поля матриць другого порядку, який може бути безпосередньо використаний у криптографічних застосуваннях, зокрема в протоколах узгодження ключів та інших перетвореннях, що базуються на скінченних полях.

Таким чином, визначена методика переводить теоретичні положення розробленого методу в послідовність практичних обчислювальних процедур, придатних для програмної реалізації в комп'ютерних системах. Її використання дає змогу формувати всі примітивні елементи поля квадратних матриць порядку 2, а отже, застосовувати таке поле в криптографічних алгоритмах із більшим порядком мультиплікативної групи, ніж у базовому полі \mathbb{Z}_p .

Визначена методика формування всіх примітивних елементів поля квадратних матриць порядку 2 дає змогу використовувати його в криптографічних застосуваннях, таких як протокол Діффі-Хеллмана або інші протоколи, що базуються на скінченних полях.

Крім того, використання поля квадратних матриць $F_{b,k} = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, t, s, a, b, k \in \mathbb{Z}_p, D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p \right\}$ над \mathbb{Z}_p дозволяє збільшити в порівнянні з полем \mathbb{Z}_p порядок мультиплікативної групи поля до значення $|F_{b,k}^*| = p^2 - 1$. Відповідно, криптографічну стійкість алгоритмів, що використовують це поле, буде підвищено.

2.6. Висновки до розділу 2

У другому розділі розроблено метод вибору примітивних елементів скінченних полів матриць другого порядку, який за рахунок послідовної

перевірки дискримінанта характеристичного рівняння, максимального періоду матриці в квадратичному розширенні та примітивності її визначника в базовому полі дає змогу конструктивно формувати множину примітивних елементів поля без повного перебору всіх його елементів.

У розділі встановлено умови, за яких матриця другого порядку є генератором мультиплікативної групи скінченного поля матриць. Показано, що матриці, для яких дискримінант характеристичного рівняння є квадратичним лишком у полі \mathbb{Z}_p , не можуть забезпечувати максимальний порядок у полі матриць, тоді як у випадку нерозкладного характеристичного многочлена примітивність матриці зводиться до одночасного виконання двох умов: досягнення максимального періоду $p + 1$ та примітивності її визначника в базовому полі \mathbb{Z}_p . Одержано еквівалентні критерії перевірки цих умов через степені матриці, значення сліду степенів матриці та перевірку показників, пов'язаних із простими дільниками числа $p + 1$.

На основі одержаних теоретичних результатів розроблено методику вибору примітивних елементів скінчених полів матриць другого порядку, орієнтовану на практичну й програмну реалізацію. Методика охоплює формування множини матриць-кандидатів, обчислення їх сліду, визначника та дискримінанта, перевірку умови максимального періоду, визначення порядку визначника та побудову примітивних елементів за допомогою скалярних коефіцієнтів із базового поля. Встановлено співвідношення, які дозволяють контролювати повноту сформованої множини примітивних елементів і уникати дублювання результатів під час обчислень.

Особливості застосування розробленого методу продемонстровано на конкретному прикладі поля матриць другого порядку над \mathbb{Z}_{13} , для якого сформовано повну множину з 48 примітивних елементів, що узгоджується з теоретичною кількістю $\varphi(p^2 - 1)$ та підтверджує коректність і повноту запропонованого підходу.

Практичне значення одержаних результатів полягає в тому, що розроблений метод і методика дають змогу формувати всі примітивні елементи скінченного поля матриць другого порядку для їх подальшого використання в криптографічних алгоритмах комп'ютерних систем і мереж. Використання поля матриць порядку 2 над \mathbb{Z}_p забезпечує збільшення порядку мультиплікативної групи з $p-1$ до p^2-1 порівняно з базовим полем, що створює передумови для розширення можливостей криптографічних перетворень і потенційного підвищення їх криптографічної стійкості.

Основні результати досліджень цього розділу опубліковано в [46], [47].

РОЗДІЛ 3. МЕТОД ВИБОРУ ПАРАМЕТРІВ ПОЛЯ КВАДРАТНИХ МАТРИЦЬ ДРУГОГО ПОРЯДКУ ТА ПРИМІТИВНОГО ЕЛЕМЕНТУ В НЬОМУ

3.1. Вступ

Попередній розділ спрямовано на дослідження можливості використання скінченного поля $F_{b,k}$ в криптографічних застосуваннях, зокрема в протоколі узгодження ключа Діффі-Хеллмана [1]. Для цього представлено підхід до визначення матриць $t \cdot A = t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$, що є примітивними елементами скінченного поля $F_{b,k}$, а також показано структуру множини таких примітивних елементів у полі $F_{b,k}$.

Зокрема, твердження 2.5 доводить, що існує рівно $\varphi(p+1)$ різних матриць $A_j = \begin{pmatrix} a_j & 1 \\ b & a_j+k \end{pmatrix} \in F_{b,k}$ над \mathbb{Z}_p з $\text{period}(A_j) = p+1$ і $\det(A_j) \neq u^2 \in \mathbb{Z}_p$, що визначають усі $\varphi(p^2-1)$ примітивні елементи поля $F_{b,k}$ над \mathbb{Z}_p , а саме:

$$t_{ji} \cdot A_j, \quad (3.1)$$

$$\text{де } t_{ji} \in T_j = \left\{ \pm \sigma^{\frac{i-\gamma_j}{2}} : \langle i, p-1 \rangle = 1, \gamma_j = \text{ind}(\det(A_j)) \right\}, 1 \leq j \leq \varphi(p+1);$$

σ – найменший первісний корінь у \mathbb{Z}_p ;

$\text{ind}(\det(A_j)) = \gamma$ – індекс числа $\det(A_j)$ за основою σ :

$$\det(A_j) \equiv \sigma^\gamma \pmod{p}, \quad 0 \leq \gamma \leq p-2.$$

Наведена в розділі 2 методика знаходження всіх матриць $A_j = \begin{pmatrix} a_j & 1 \\ b & a_j+k \end{pmatrix} \in F_{b,k}$, що визначають усі $\varphi(p^2-1)$ примітивні елементи

поля $F_{b,k}$ над \mathbb{Z}_p , передбачає перебір значень a_j з наступною перевіркою, чи $\det(A_j) \in \mathbb{Z}_p$ є квадратичним лишком у \mathbb{Z}_p .

У випадку, коли параметри b і k поля $F_{b,k}$ попередньо не задано, його використання, зокрема, в криптографічних застосуваннях, відповідно до запропонованих у попередньому розділі методу й методики, вимагає окремого вирішення двох завдань: вибору параметрів b і k , що задовольняють умові $k^2 + 4b \neq u^2 \in \mathbb{Z}_p$, а також знаходження примітивних елементів поля $F_{b,k}$ для визначених параметрів. Такий підхід є трудомістким і стимулює пошук і дослідження шляхів, що дозволяють однією процедурою визначати як необхідні параметри поля $F_{b,k}$, так і його примітивні елементи.

Крім того, елементами поля $F_{b,k}$ є матриці $t \cdot A = t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$, а підхід другого розділу дозволяє отримати всі примітивні елементи виду $t_{ji} \cdot A_j$ із (3.1) з окремою процедурою визначення коефіцієнта t_{ji} . Така ситуація, з метою спрощення обчислювальних процедур, обумовлює доцільність дослідження спеціального випадку примітивного елемента виду $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ для $t=1$.

Таким чином, метою цього розділу є розробка та дослідження методу вибору параметрів скінченних полів матриць 2×2 з одночасним формуванням примітивних елементів у них.

3.2. Задача вибору параметрів поля матриць

Розглянемо матрицю $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$. Тоді $|A| = \Delta_a = a(a+k) - b \neq 0$.

Характеристичне рівняння матриці A має вигляд $\lambda^2 - (2a+k)\lambda + [a(a+k) - b] = 0$ або $\lambda^2 - (2a+k)\lambda + \Delta_a = 0$.

Корені характеристичного рівняння $\lambda_{1,2}(a)$ є власними значеннями матриці A . Далі значення $\lambda_{1,2}(a)$ будемо скорочено позначати через $\lambda_{1,2}$.

Для того, щоб матриця мала максимальну кількість лінійно незалежних власних векторів, достатньо, щоб усі корені її характеристичного рівняння були різні [67], [73]. Для матриці A необхідною та достатньою умовою для цього є $D = k^2 + 4b \neq 0$.

У попередньому розділі показано, що:

- 1) для $D = u^2 \in \mathbb{Z}_p$, $u \neq 0$, значення $\text{ord}(A) = \text{LCM}(\text{ord}(\lambda_1), \text{ord}(\lambda_2))$ у \mathbb{Z}_p і $\text{ord}(A) \leq p-1$. Максимальна межа досягається тоді і тільки тоді, коли найменше спільне кратне порядків власних чисел $\lambda_{1,2}$ дорівнює $p-1$, наприклад, коли хоча б один з елементів $\lambda_{1,2}$ є примітивним у \mathbb{Z}_p ;
- 2) для $D \neq u^2 \in \mathbb{Z}_p$, $u \neq 0$, справедливим є вираз

$$A^{p+1} = C \begin{pmatrix} \lambda_1^{p+1} & 0 \\ 0 & \lambda_2^{p+1} \end{pmatrix} C^{-1} = C \begin{pmatrix} \Delta_a & 0 \\ 0 & \Delta_a \end{pmatrix} C^{-1} = \Delta_a E, \quad (3.2)$$

де $\Delta_a \in \mathbb{Z}_p$. Для елемента A матричного поля $F_{b,k}$ порядку $|F_{b,k}| = p^2$ значення $\text{ord}(A) \leq p^2 - 1$. Згідно з твердженням 2.4, максимальна межа $\text{ord}(A) = p^2 - 1$ досягається, якщо $\text{period}(A) = p+1$ і $\lambda_1^{p+1} = \lambda_2^{p+1} = \Delta_a$ є примітивним елементом поля \mathbb{Z}_p з порядком $p-1$.

Зауваження 3.1. Для власних чисел $\lambda_{1,2}$ матриці A , $D \neq u^2 \in \mathbb{Z}_p$, виконується рівність $\lambda_1^i = \lambda_2^i = \delta$ тоді і тільки тоді, коли $\lambda_1^i = \delta \in \mathbb{Z}_p$.

Доведення.

Представимо матрицю A в вигляді $A = C \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} C^{-1}$, де $C = \|c_{ij}\|$,

$c_{ij} \in \mathbb{Z}_p(\sqrt{D})$, є діагоналізуюча матриця для $A = \|a_{ij}\|$, $a_{ij} \in \mathbb{Z}_p$.

Якщо $\lambda_1^i = \lambda_2^i$, то

$$A^i = C \cdot \begin{pmatrix} \lambda_1^i & 0 \\ 0 & \lambda_2^i \end{pmatrix} \cdot C^{-1} = C \cdot \lambda_1^i \cdot E \cdot C^{-1} = \lambda_1^i \cdot E = \delta \cdot E = \begin{pmatrix} \delta & 0 \\ 0 & \delta \end{pmatrix}, \text{ де } \lambda_1^i = \delta \in \mathbb{Z}_p.$$

Нехай тепер $\lambda_1^i = \delta \in \mathbb{Z}_p$. Оскільки характеристичний поліном матриці A незвідний у \mathbb{Z}_p , то власне число $\lambda_2 = \lambda_1^p$. У силу теореми Ферма [74] для елементів \mathbb{Z}_p слідує: $\lambda_2^i = (\lambda_1^p)^i = (\lambda_1^i)^p = \delta^p = \delta$, тобто $\lambda_1^i = \lambda_2^i = \delta$. ■

Наслідок 3.1. Степінь $A^i = \delta \cdot E$ тоді і тільки тоді, коли значення $\lambda_1^i = \delta \in \mathbb{Z}_p$.

Зауважимо, що умова примітивності Δ_a в \mathbb{Z}_p для забезпечення максимального порядку циклічної підгрупи, породженої матрицею A , є необхідною, проте не достатньою. Останнє спричинено тим, що рівність $\lambda_1^{p+1} = \lambda_2^{p+1}$ не виключає випадків, коли $\lambda_1^i = \lambda_2^i$ для $i < p+1$ (див. приклад 1).

Нагадаємо, що для піднесення квадратної матриці $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ до степеня використовується вираз з [68]

$$A^i = \begin{pmatrix} \mathcal{G}_{i+1} - d\mathcal{G}_i & b\mathcal{G}_i \\ c\mathcal{G}_i & \mathcal{G}_{i+1} - a\mathcal{G}_i \end{pmatrix}, \quad (3.3)$$

де

$$\mathcal{G}_{i+1} = \text{tr}(A)\mathcal{G}_i - \det(A)\mathcal{G}_{i-1}, \quad (3.4)$$

$\text{tr}(A)$ – слід матриці A [69]; $\mathcal{G}_0 = 0$, $\mathcal{G}_1 = 1$.

Нагадаємо також, що твердження 2.1 свідчить про те, що якщо $A \in F_{b,k}$, то $\text{period}(A) = p+1$ тоді і тільки тоді, коли $A \neq s \cdot E$ і

$$\mathcal{G}_i \neq 0 \text{ для } 1 \leq i \leq \frac{p+1}{2}. \quad (3.5)$$

Твердження ж 2.2 говорить про те, що для $A \in F_{b,k}$ і $\det(A) = \Delta_a \neq u^2 \in \mathbb{Z}_p$ справедливе наступне:

(в) якщо просте p є числом Мерсенна ($p = 2^m - 1$), то $\text{period}(A) = p + 1$;

(г) якщо $p \neq 2^m - 1$, то $\text{period}(A) = p + 1$ тоді і тільки тоді, коли

$$\mathcal{G}_i \neq 0 \text{ для } 1 \leq i \leq \frac{p+1}{\gamma}, \quad (3.6)$$

де $\gamma = \min \{f = 2c + 1 : c \geq 1, (p+1) \vdots f\}$.

Приклад 1.

а) Нехай $p = 11$, $b = 10$, $k = 5$, а матриця $A = \begin{pmatrix} a & 1 \\ 10 & a+5 \end{pmatrix} \in F_{10,5}$ над \mathbb{Z}_{11} .

Значення $D = k^2 + 4b = 10 \neq u^2 \in \mathbb{Z}_{11}$. Для $a = 8$ визначник

$\Delta_a = 6D \neq u^2 \in \mathbb{Z}_{11}$. Число $\frac{p+1}{2} = 6$ не є простим.

Для визначення $\text{period}(A)$ застосуємо твердження 2.1. Обрахувавши $\text{tr}(A) = 10 = -1$, $\det(A) = \Delta_a = -5$, знайдемо значення елементів \mathcal{G}_i послідовності (3.4) для $1 \leq i \leq 6$ за формулою (3.5): 0, 1, -1, 6, 0, 8,

Отримуємо $\mathcal{G}_4 = 0$, $\mathcal{G}_5 = 8$, звідки $\text{period}(A) \neq p + 1$. Характеристичний

поліном матриці $A = \begin{pmatrix} 8 & 1 \\ 10 & 2 \end{pmatrix}$ дорівнює $\lambda^2 + \lambda + 6$, має дискримінант

$D = 10 \neq u^2 \in \mathbb{Z}_{11}$ і є незвідним над полем \mathbb{Z}_{11} . Полем розкладу $\lambda^2 + \lambda + 6$ є квадратичне розширення поля $\mathbb{Z}_{11}[\sqrt{10}]$, у якому власні значення матриці A

дорівнюють $\lambda_{1,2} = \frac{1}{2}(-1 \pm \sqrt{10})$. Згідно з формулою (3.3) для степеня A^i маємо:

$$A^4 = \begin{pmatrix} 8 & 0 \\ 0 & 8 \end{pmatrix} = 8E, \text{ тобто } period(A) = 4 = \frac{p+1}{3} \text{ та } \lambda_1^4 = \lambda_2^4 = 8 \in \mathbb{Z}_{11};$$

б) нехай $p=13$, $b=7$, $k=4$, а матриця $A = \begin{pmatrix} a & 1 \\ 7 & a+4 \end{pmatrix} \in F_{7,4}$ над \mathbb{Z}_{13} .

Дискримінант $D = k^2 + 4b = 5 \neq u^2 \in \mathbb{Z}_{13}$. Для $a=5$ матриця $A = \begin{pmatrix} 5 & 1 \\ 7 & 9 \end{pmatrix}$

має $tr(A) = 1$ і $\det(A) = \Delta_a = -1$. Полем розкладу характеристичного поліному

$\lambda^2 - \lambda + 1$ матриці A є просте квадратичне розширення поля $\mathbb{Z}_{13}[\sqrt{5}]$, у якому

власні значення дорівнюють $\lambda_{1,2} = \frac{1}{2}(-1 \pm \sqrt{5})$. Число $\frac{p+1}{2} = 7$ є простим, але

визначник $\Delta_a = -1 = 5^2 \in \mathbb{Z}_{13}$. Таким чином, для визначення періоду матриці A

не можна застосовувати твердження 2.2 і користуватися умовою (3.6). Тому

використаємо твердження 2.1, обрахувавши послідовність (3.4) для $1 \leq i \leq 7$ за формулою (3.5): 0, 1, 1, 2, 3, 5, 8, 0, 8, ..., де $\mathcal{Q}_7 = 0$, $\mathcal{Q}_8 = 8$.

Згідно з формулою (3.3): $A^7 = 8E$, звідки $period(A) = 7 = \frac{p+1}{2}$ та

$$\lambda_1^7 = \lambda_2^7 = 8 \in \mathbb{Z}_{13};$$

в) нехай $p=19$, $b=11$, $k=3$, а матриця $A = \begin{pmatrix} a & 1 \\ 11 & a+3 \end{pmatrix} \in F_{11,3}$ над \mathbb{Z}_{19} .

Дискримінант $D = k^2 + 4b = 15 \neq u^2 \in \mathbb{Z}_{19}$. Для $a=9$ матриця

$A = \begin{pmatrix} 9 & 1 \\ 11 & 12 \end{pmatrix}$ має $tr(A) = 2$, $\det(A) = \Delta_a = 2$ і характеристичний поліном

$\lambda^2 - 2\lambda + 2$. Оскільки $\frac{1}{4}D = 18 \neq u^2 \in \mathbb{Z}_{19}$, то полем розкладу полінома

$\lambda^2 - 2\lambda + 2$ буде квадратичне розширення поля $\mathbb{Z}_{19}[\sqrt{18}]$. Власними

значеннями матриці $A \in \lambda_{1,2} = 1 \pm \sqrt{18} \in \mathbb{Z}_{19}[\sqrt{18}]$. Для визначення $period(A)$ обчислимо значення \mathcal{G}_i за формулою (3.4) для $1 \leq i \leq 4$ згідно з (3.6): 0, 1, 2, 2, 0, -4, ..., де $\mathcal{G}_4 = 0$, $\mathcal{G}_5 = -4$. Це означає, що $A^4 = -4E$, звідки $period(A) = 4 = \frac{p+1}{5}$ та $\lambda_1^4 = \lambda_2^4 = -4 \in \mathbb{Z}_{19}$.

Нехай $r \equiv m \equiv n \pmod{p+1}$, $0 \leq r \leq p$.

$$\text{Тоді} \quad \begin{cases} n = \nu(p+1) + r, \\ m = \mu(p+1) + r. \end{cases} \quad \text{з урахуванням} \quad (2.1),$$

$$A^n = A^{\nu(p+1)+r} = (A^{p+1})^\nu \cdot A^r = \Delta_a^\nu \cdot A^r, \quad A^m = A^{\mu(p+1)+r} = (A^{p+1})^\mu \cdot A^r = \Delta_a^\mu \cdot A^r. \quad \text{Тоді}$$

$$A^m = \frac{\Delta_a^\mu}{\Delta_a^\nu} \cdot A^n = \Delta_a^{\mu-\nu} \cdot A^n \quad \text{або}$$

$$A^m = \Delta_a^{\frac{m-n}{p+1}} \cdot A^n. \quad (3.7)$$

Зазначимо, що рівність (3.7) вказує на «періодичність» повторення значень степенів матриці A поля $F_{b,k}$ з точністю до визначеного коефіцієнта із \mathbb{Z}_p .

Розглянемо більш детально питання вибору параметрів матриці

$$A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix} \quad \text{з} \quad D \neq u^2 \in \mathbb{Z}_p, \quad \text{щоб порядок породженої нею циклічної}$$

підгрупи був максимальним.

Зазначимо, що для забезпечення максимального значення $ord(A)$ для $D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p$ згідно з твердженням 2.4 необхідно, щоб Δ_a був примітивним у \mathbb{Z}_p з порядком $p-1$. Для найменшого первісного кореня σ_0 в \mathbb{Z}_p це означає, що $\Delta_a = \sigma_0^i$, де $GCF(i, p-1) = 1$. Якщо значення $t \neq 0$, то його можна подати степенем σ_0 : $t = \sigma_0^\nu$, $0 < \nu < p$. Тоді для примітивного Δ_a із рівності $\Delta_a = t^j$, $0 < j < p$, маємо $\sigma_0^{\nu j} = \sigma_0^i$. Ця рівність рівносильна

порівнянню $v \cdot j \equiv i \pmod{p-1}$, де $GCF(i, p-1) = 1$. Для $GCF(v \cdot j, p-1) \neq 1$ вказане порівняння не має розв'язків, зокрема для $GCF(j, p-1) \neq 1$. Тому необхідною умовою примітивності Δ_a є вимога

$$\Delta_a = a(a+k) - b \neq t^j \in \mathbb{Z}_p, \quad (3.8)$$

де $1 < j < p$, $GCF(j, p-1) \neq 1$.

Обмежимося розглядом для простих $p > 2$ базового випадку, коли

$$\begin{cases} D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p, \\ \Delta_a = a(a+k) - b \neq t^2 \in \mathbb{Z}_p. \end{cases} \quad (3.9)$$

Очевидно, що $\Delta_a = a(a+k) - b \neq t^2 \in \mathbb{Z}_p$ є необхідною умовою. Але вона не є достатньою.

З виразу $D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p$ слідує, що $b \neq 0$. Тоді для довільного квадратичного залишка q у \mathbb{Z}_p виконується рівність $k^2 + 4b = q$ або $b = \frac{q - k^2}{4}$.

Підставивши останній вираз у $\Delta_a = a(a+k) - b \neq t^2 \in \mathbb{Z}_p$, отримаємо:

$$\left(a + \frac{k}{2}\right)^2 - \left(\frac{1}{2}\right)^2 q \neq t^2 \in \mathbb{Z}_p \quad \text{або} \quad (2a+k)^2 - q \neq (2t)^2 \in \mathbb{Z}_p. \quad \text{Таким чином,}$$

останній вираз дозволяє звести задачу вибору параметрів поля матриць до пошуку квадратичного залишка r у \mathbb{Z}_p , яке задає за фіксованого квадратичного залишка q у \mathbb{Z}_p різницю $(2a+k)^2 - q = r$ або

$$(2a+k)^2 = q + r. \quad (3.10)$$

Зауваження 3.2. Для найпростішого випадку, коли $2a+k=0$ або $a = -\frac{k}{2}$, для значень символу Лежандра виконуються такі рівності (див. [72]):

$$\left(\frac{p-q}{p}\right) = \left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{q}{p}\right). \quad (3.11)$$

Тоді пара $\{q; r = p - q\}$ є квадратичними нелишками в \mathbb{Z}_p тільки для p виду $p = 4w + 1$, оскільки для p виду $p = 4w + 3$ значення $r = p - q$ є завжди квадратичним лишком для квадратичного нелишка q [72]. Матриця

$A = \begin{pmatrix} a & 1 \\ b & a + k \end{pmatrix}$ для $a = -\frac{k}{2}$ має вид $A = \begin{pmatrix} -k/2 & 1 \\ b & k/2 \end{pmatrix}$ без змінних параметрів.

У такому випадку $A^2 = \left(\frac{k^2}{4} + b\right) \cdot E = \frac{D}{4} \cdot E$, а $period(A) = 2$.

Мультиплікативна група має просту структуру

$$CGL_p(b, k) = \left\{ t \cdot \begin{pmatrix} -k/2 & 1 \\ b & k/2 \end{pmatrix}, sE, \quad t, s, k \in \mathbb{Z}_p, t, s \neq 0 \right\}, \text{ а її порядок дорівнює}$$

$$2(p-1).$$

Далі будемо розглядати випадок, коли $2a + k \neq 0$.

Розв'язок рівняння (3.10) зводиться до пошуку, за фіксованого квадратичного нелишка q у \mathbb{Z}_p , квадратичних нелишків r у \mathbb{Z}_p таких, що $q + r = t^2 \in \mathbb{Z}_p$. Визначимо, яка кількість таких пар q і r існує.

Для вирішення задачі пошуку квадратичних нелишків $q, r \in \mathbb{Z}_p$ таких, що $q + r = t^2 \in \mathbb{Z}_p$, розглянемо задачу пошуку квадратичних лишків $q, r \in \mathbb{Z}_p$ таких, що $q + r = t^2 \in \mathbb{Z}_p$.

3.3. Пошук квадратичних лишків $q, r \in \mathbb{Z}_p$ таких, що $q + r = t^2 \in \mathbb{Z}_p$

Вираз $q + r = t^2 \in \mathbb{Z}_p$ перепишемо у полі \mathbb{Z}_p в вигляді

$$q^2 + r^2 = t^2. \quad (3.12)$$

Розглянемо наступні випадки:

1) $qr = 0$;

2) $\begin{cases} qr \neq 0; \\ t = 0; \end{cases}$

3) $qrt \neq 0$.

Випадок 1. Якщо $qr = 0$, то
$$\begin{cases} q = 0; \\ r^2 - t^2 = 0; \\ r = 0; \\ q^2 - t^2 = 0; \end{cases} \quad \text{або} \quad \begin{cases} q = 0; \\ r = \pm t; \\ r = 0; \\ q = \pm t. \end{cases}$$

Кількість пар $(q; r)$: $qr = 0$, які є розв'язком рівняння (3.12) для довільного $t \in \mathbb{Z}_p$, дорівнює $2p$. Кількість різних таких пар $(q; r)$ з точністю до їх перестановки дорівнює p .

Кількість різних пар $(q^2; r^2)$: $qr = 0$ з точністю до їх перестановки для $t \in \mathbb{Z}_p$ дорівнює кількості квадратичних лишків у \mathbb{Z}_p , включаючи нульовий:

$$\frac{p-1}{2} + 1 = \frac{p+1}{2}.$$

Випадок 2. Якщо $\begin{cases} qr \neq 0, \\ t = 0; \end{cases}$ то $q^2 + r^2 = 0$, де $q^2, r^2 \in \{1, 2, 3, \dots, p-1\}$.

Оскільки $q \neq 0$, $1 + (r/q)^2 = 0$.

Нехай $w = r/q$. Тоді $1 + w^2 = 0$ або

$$w^2 = -1. \quad (3.13)$$

Відповідно до наслідку 3 розділу 5 §1 [72] рівняння (3.13) має розв'язок для простих p тоді і тільки тоді, коли $p = 4l + 1$.

Приймемо, що w_0 є розв'язком рівняння (3.13), тобто $1 + w_0^2 = 0$, $p = 4l + 1$. Тоді для кожного $q \in \mathbb{Z}_p$: $q^2(1 + w_0^2) = q^2 + (qw_0)^2 = 0$. Це означає, що множина пар $\{q; qw_0\} = \{q; r\}$ задає всі можливі розв'язки в полі \mathbb{Z}_p рівняння $q^2 + r^2 = 0$, $p = 4l + 1$. Крім того, оскільки $w_0 \in \mathbb{Z}_p$, то $w_0^2 = p-1$ або $w_0 = \pm(p-1)^{\frac{1}{2}}$.

Для $\begin{cases} qr \neq 0; \\ p = 4l + 3 \end{cases}$ завжди справедливим є $q^2 + r^2 \neq 0$.

Таким чином, кількість пар $(q; r)$: $qr \neq 0$, які є розв'язком рівняння (3.12) для $t = 0$, дорівнює $2(p-1)$ для $p = 4l + 1$ і нулю для $p = 4l + 3$. Кількість же різних пар $(q; r)$ з точністю до їх перестановки для $p = 4l + 1$ дорівнює $p-1$.

Наслідок 3.2. Кількість різних пар $(q^2; r^2)$: $qr \neq 0$ з точністю до їх перестановки, які є розв'язком рівняння (3.12) для $t = 0$, дорівнює $(p-1)/4$ для $p = 4l + 1$ і нулю для $p = 4l + 3$.

Зазначимо також, що система ненульових квадратичних лишків у \mathbb{Z}_p , $p = 4l + 1$, володіє властивістю симетрії розташування в упорядкованій за зростанням множині лишків за модулем p : $1; \dots; q^2; \dots; p - q^2; \dots; p - 1 = w_0^2$, $q^2 \leq \frac{p-1}{2}$ (див. формулу (3.11)).

Наслідок 3.3. Кількість ненульових квадратичних лишків r^2 у \mathbb{Z}_p за фіксованого ненульового квадратичного лишка q^2 , які задовольняють умові $q^2 + r^2 = 0$, дорівнює одиниці для $p = 4l + 1$ і нулю для $p = 4l + 3$.

У зауваженні 3.2 відзначено, що аналогічною властивістю симетрії володіють і квадратичні нелишки в \mathbb{Z}_p , $p = 4l + 1$: для кожного квадратичного нелишка η існує квадратичний нелишок f , що $\eta + f = 0$, тобто $f = p - \eta$.

Наслідок 3.4. Кількість квадратичних нелишків η у \mathbb{Z}_p за фіксованого квадратичного нелишка f , які задовольняють умові $\eta + f = 0$ дорівнює одиниці для $p = 4l + 1$ і нулю для $p = 4l + 3$.

Приклад 2.

Нехай $p = 4l + 1 = 13$, $w_0^2 = 12$. Тоді $w_0 = \pm 5 = \{5; 8\}$. Відповідно, маємо наступні пари значень $(q; r)$ такі, що $q^2 + r^2 = 0$: $(1; \pm 5)$, $(2; \pm 10)$, $(3; \pm 2)$, $(4; \pm 7)$, $(5; \pm 12)$, $(6; \pm 4)$, $(7; \pm 9)$, $(8; \pm 1)$, $(9; \pm 6)$, $(10; \pm 11)$, $(11; \pm 3)$, $(12; \pm 8)$.

Кількість пар $(q; r)$ дорівнює $2(p-1) = 24$. Кількість же різних пар $(q; r)$ з точністю до їх перестановки дорівнює $p-1 = 12$: $(1; 5)$, $(1; 8)$, $(2; 3)$, $(2; 10)$, $(3; 11)$, $(4; 6)$, $(4; 7)$, $(5; 12)$, $(6; 9)$, $(7; 9)$, $(8; 12)$, $(10; 11)$.

Кількість різних пар $(q^2; r^2)$ з точністю до їх перестановки дорівнює $(p-1)/4 = 3$: $(1; 12)$, $(3; 10)$, $(4; 9)$.

Випадок 3. Якщо $qrt \neq 0$, то вираз $q^2 + r^2 = t^2$ еквівалентний виразу $\left(\frac{q}{t}\right)^2 + \left(\frac{r}{t}\right)^2 = 1$. Виконаємо заміну $x = \frac{q}{t}$, $y = \frac{r}{t}$. Отримаємо систему:

$$\begin{cases} xy \neq 0; \\ x^2 + y^2 = 1. \end{cases} \quad (3.14)$$

Застосуємо відомий підхід знаходження піфагорових трійок чисел у \mathbb{Z}_p для розв'язання системи (3.14), який використовує стереографічну проекцію Riemann [77], [78], [79].

Розглянемо «пряму» $1 - y = nx$ і співставимо параметр n з кожною парою $(x; y)$ розв'язків $x^2 + y^2 = 1$ над \mathbb{Z}_p .

Якщо пара $(x_0; y_0)$ є розв'язком системи (3.14), то $x_0 \neq \pm 1 \neq y_0$. Існує єдине значення параметра $n \in \mathbb{Z}_p$, за якого точка $(x_0; y_0)$ лежить на «прямій» $1 - y_0 = nx_0$ та яке дорівнює

$$n = (1 - y_0)/x_0.$$

У той же час, для довільного $n \in \mathbb{Z}_p$ справедливе наступне:

$$\begin{cases} 1-y=nx; \\ x^2+y^2=1; \\ xy \neq 0; \end{cases} \Leftrightarrow \begin{cases} 1-y=nx; \\ x^2=(1-y)(1+y); \\ xy \neq 0; \end{cases} \Leftrightarrow \begin{cases} 1-y=nx; \\ x^2=nx(1+y); \\ xy \neq 0; \end{cases} \Leftrightarrow \begin{cases} 1-y=nx; \\ 1+y=\frac{1}{n}x; \\ n \neq 0; \\ xy \neq 0. \end{cases}$$

Оскільки $2 = x \frac{n^2+1}{n} \neq 0$, то $x = \frac{2n}{n^2+1}$, а $y = \frac{1-n^2}{n^2+1}$, де $n^2+1 \neq 0$, $n \neq 0$,

$n \neq \pm 1$.

Зауваження 3.3. Множини $\mathbb{Z}_3 \setminus \{0; \pm 1\} = \emptyset$ і $\mathbb{Z}_5 \setminus \{0; \pm 1; n^2+1=0\} = \emptyset$.

Таким чином, якщо пара чисел $(x; y)$ є розв'язком системи (3.14), то

$$\text{завжди } p \geq 7 \text{ і існує } n \in \mathbb{Z}_p \setminus \{0; \pm 1\}, \quad n^2+1 \neq 0, \text{ таке, що } \begin{cases} x = \frac{2n}{n^2+1}; \\ y = \frac{1-n^2}{n^2+1}. \end{cases}$$

Підставляючи ці значення $(x; y)$ у рівняння $x^2 + y^2 = 1$, отримаємо

$$\left(\frac{2n}{n^2+1}\right)^2 + \left(\frac{1-n^2}{n^2+1}\right)^2 = 1. \text{ Множачи це рівняння на } \left(\frac{n^2+1}{n}\right)^2, \text{ записуємо вирази}$$

(3.13) і (3.14) у \mathbb{Z}_p для $p \geq 7$ одним співвідношенням:

$$2^2 + \left(n - \frac{1}{n}\right)^2 = \left(n + \frac{1}{n}\right)^2. \quad (3.15)$$

Зауваження 3.4. Нехай f, g – квадратичні лишки в \mathbb{Z}_p . Тоді рівність (3.12) $q^2 + r^2 = t^2$ для $q = 2$ можна записати таким чином: $2^2 + f = g$.

Наслідок 3.5. Оскільки вирази (3.12) і (3.15) є еквівалентними для $qr \neq 0$ і $n - \frac{1}{n} \neq 0$, то рівність $2^2 + f = g$, де $f \neq 0$, g – квадратичні лишки в \mathbb{Z}_p ,

$p \geq 7$, можлива лише в випадку, коли $f = \left(n - \frac{1}{n}\right)^2$ і $g = \left(n + \frac{1}{n}\right)^2$, де

$n \in \mathbb{Z}_p \setminus \{0; \pm 1\}$.

Розглянемо функцію $f(n) = \left(n - \frac{1}{n}\right)^2$ для $n \in \mathbb{Z}_p \setminus \{0; \pm 1\}$, $p \geq 7$.

Очевидно, що в \mathbb{Z}_p коренями цієї функції є розв'язки рівняння $n^2 - 1 = 0$, тобто $n = \pm 1$, а в $\mathbb{Z}_p \setminus \{0; \pm 1\}$ коренів не існує.

Зауваження 3.5. Функція $f(n) = \left(n - \frac{1}{n}\right)^2$ для $n \in \mathbb{Z}_p \setminus \{0; \pm 1\}$, $p \geq 7$,

набуває кожне своє значення $f(n) \neq -4$ у \mathbb{Z}_p рівно 4 рази. Значення $f(n) = -4$ у \mathbb{Z}_p функція набуває для $p = 4l + 1$ двічі, для $p = 4l + 3$ – жодного разу.

Доведення.

Нехай $f(n_0) = \left(n_0 - \frac{1}{n_0}\right)^2$. Знайдемо всі n , для яких

$f(n) = \left(n - \frac{1}{n}\right)^2 = f(n_0) = \left(n_0 - \frac{1}{n_0}\right)^2$. З останнього виразу слідує, що

$$\begin{aligned} \left(n - \frac{1}{n}\right)^2 - \left(n_0 - \frac{1}{n_0}\right)^2 &= \left(n - \frac{1}{n} - n_0 + \frac{1}{n_0}\right) \left(n - \frac{1}{n} + n_0 - \frac{1}{n_0}\right) = \\ &= \left(n - n_0 + \frac{n - n_0}{nn_0}\right) \left(n + n_0 - \frac{n + n_0}{nn_0}\right) = 0. \end{aligned}$$

Розв'язком останнього рівняння є сукупність $\left[\begin{array}{l} (n - n_0) \left(1 + \frac{1}{nn_0}\right) = 0; \\ (n + n_0) \left(1 - \frac{1}{nn_0}\right) = 0 \end{array} \right.$ або

$\left[\begin{array}{l} n = \pm n_0; \\ n = \pm \frac{1}{n_0}. \end{array} \right.$ Таким чином, для аргументів $n \in \left\{ n_0; -n_0; \frac{1}{n_0}; -\frac{1}{n_0} \right\}$ функція

$f(n) = \left(n - \frac{1}{n}\right)^2$ повторює свої значення: $f(n_0) = f(-n_0) = f\left(\frac{1}{n_0}\right) = f\left(-\frac{1}{n_0}\right)$.

Для інших значень аргументу $n \notin \left\{ n_0; -n_0; \frac{1}{n_0}; -\frac{1}{n_0} \right\}$: $f(n) \neq f(n_0)$.

Розглянемо тепер питання кількості різних елементів множини

$$\left\{n; -n; \frac{1}{n}; -\frac{1}{n}\right\} \text{ у } \mathbb{Z}_p \setminus \{0; \pm 1\}.$$

Оскільки для $n \neq 0$:
$$\begin{cases} n = -n; \\ n = \frac{1}{n} \end{cases} \Leftrightarrow \begin{cases} \frac{1}{n} = -\frac{1}{n}; \\ -n = -\frac{1}{n} \end{cases} \Leftrightarrow n = \pm 1, \text{ достатньо розв'язати}$$

систему
$$\begin{cases} n = -\frac{1}{n}; \\ -n = \frac{1}{n} \end{cases} \text{ або } n^2 = -1.$$

Останнє рівняння в \mathbb{Z}_p має розв'язки тільки для $p = 4l + 1$ [72] (див.

випадок 2 для $\begin{cases} qr \neq 0; \\ t = 0 \end{cases}$). Позначимо ці розв'язки через $\pm n_0$. Очевидно, що

$$f(\pm n_0) = \left(n_0 - \frac{1}{n_0}\right)^2 = \frac{(n_0^2 - 1)^2}{n_0^2} = \frac{(-1 - 1)^2}{-1} = -4. \blacksquare$$

Приклад 3.

Розглянемо розподіл значень функції $f(n) = \left(n - \frac{1}{n}\right)^2$, $n \in \mathbb{Z}_p \setminus \{0; \pm 1\}$,

для $p = 4l + 1 = 13$ і $p = 4l + 3 = 11$. Для цього виконаємо пряме обчислення $f(n)$ і занесемо результат у таблиці 3.1 і 3.2.

Таблиця 3.1. Значення $f(n) = \left(n - \frac{1}{n}\right)^2$ у \mathbb{Z}_{13}

n	2	3	4	5	6	7	8	9	10	11
$f(n)$	12	10	10	9	12	12	9	10	10	12

Таблиця 3.2. Значення $f(n) = \left(n - \frac{1}{n}\right)^2$ у \mathbb{Z}_{11}

n	2	3	4	5	6	7	8	9
$f(n)$	5	1	1	5	5	1	1	5

Отримані результати ілюструють зауваження 3.5:

- функція $f(n) = \left(n - \frac{1}{n}\right)^2$ для $n \in \mathbb{Z}_p \setminus \{0; \pm 1\}$ набуває кожне своє значення $f(n) \neq -4$ у \mathbb{Z}_p рівно 4 рази;
- значення $f(n) = -4$ у \mathbb{Z}_p функція набуває для $p = 4l + 1 = 13$ двічі, для $p = 4l + 3 = 11$ – жодного разу.

Зауваження 3.6. Кількість різних значень функції $f(n) = \left(n - \frac{1}{n}\right)^2$ для $n \in \mathbb{Z}_p \setminus \{0; \pm 1\}$, $p \geq 7$, дорівнює числу $l = \left\lfloor \frac{p-1}{4} \right\rfloor$, де $[x]$ – функція цілої частини числа x .

Доведення.

Нехай k – кількість різних значень функції $f(n) \neq -4$ для $n \in \mathbb{Z}_p \setminus \{0; \pm 1\}$. Тоді, в силу зауваження 3.5, кількість різних значень аргумента функції $f(n) = \left(n - \frac{1}{n}\right)^2$, $n \in \mathbb{Z}_p \setminus \{0; \pm 1\}$, оцінюється зверху:

$$\begin{cases} 2 + 4k \leq p - 3, \text{ if } p = 4l + 1; \\ 4k \leq p - 3, \text{ if } p = 4l + 3 \end{cases} \quad \text{або} \quad \begin{cases} k \leq l - 1, \text{ if } p = 4l + 1; \\ k \leq l, \text{ if } p = 4l + 3. \end{cases}$$

Позначимо через $\{n_{j1}, n_{j2}, n_{j3}, n_{j4}\}$, $1 \leq j \leq k$, елементи з $\mathbb{Z}_p \setminus \{0; \pm 1\}$, для яких значення $f(n_{j1}) = f(n_{j2}) = f(n_{j3}) = f(n_{j4}) = f_j \neq -4$.

Оскільки k – число різних значень функції $f(n) \neq -4$ для $n \in \mathbb{Z}_p \setminus \{0; \pm 1\}$

$$\text{, то } \begin{cases} \bigcup_{j=1}^k \{n_{j1}, n_{j2}, n_{j3}, n_{j4}\} \cup \{\pm n_0 : f(\pm n_0) = -4\} = \mathbb{Z}_p \setminus \{0; \pm 1\} \text{ if } p = 4l + 1; \\ \bigcup_{j=1}^k \{n_{j1}, n_{j2}, n_{j3}, n_{j4}\} = \mathbb{Z}_p \setminus \{0; \pm 1\} \text{ if } p = 4l + 3. \end{cases}$$

Звідси слідує, що $\begin{cases} k = l - 1, \text{ if } p = 4l + 1; \\ k = l, \text{ if } p = 4l + 3, \end{cases}$ а число різних значень функції

$$f(n) = \left(n - \frac{1}{n}\right)^2, \quad n \in \mathbb{Z}_p \setminus \{0; \pm 1\}, \text{ дорівнює } \begin{cases} k + 1 = l, \text{ if } p = 4l + 1; \\ k = l, \text{ if } p = 4l + 3, \end{cases} \text{ а } l = \left\lfloor \frac{p-1}{4} \right\rfloor.$$

■

Наслідок 3.6. З $\frac{p-1}{2}$ ненульових квадратичних лишків у \mathbb{Z}_p , $p \geq 7$,

рівно $l = \left\lfloor \frac{p-1}{4} \right\rfloor$ лишків можна представити як $\left(n - \frac{1}{n}\right)^2$, $n \in \mathbb{Z}_p \setminus \{0; \pm 1\}$.

Звернемо увагу, що $\frac{p-1}{2} = \begin{cases} 2l, \text{ if } p = 4l + 1; \\ 2l + 1, \text{ if } p = 4l + 3. \end{cases}$

Наслідок 3.7. Нехай f почергово набуває значень усіх ненульових квадратичних лишків у \mathbb{Z}_p , $p \geq 7$. Тоді сума $2^2 + f = g$ є ненульовим квадратичним лишком рівно $l - 1 = \left\lfloor \frac{p-1}{4} \right\rfloor - 1$ разів для $p = 4l + 1$ і $l = \left\lfloor \frac{p-1}{4} \right\rfloor$ разів для $p = 4l + 3$. Сума $2^2 + f = g$ є квадратичним нелишком рівно l разів для $p = 4l + 1$ і $l + 1$ разів для $p = 4l + 3$.

Для доведення наслідку 3.7 достатньо скористатися виразом (3.15) і наслідками 3.5 і 3.6, врахувавши, що сума g набуває нульового значення за

умови, коли $g = \left(n + \frac{1}{n}\right)^2$ або $n^2 = -1$. Під час доведення зауваження 3.5

показано, що $n^2 = -1$ має розв'язки $\pm n_0$ тільки для $p = 4l + 1$, а

$$f(\pm n_0) = \left(\pm n_0 - \frac{1}{\pm n_0}\right)^2 = -4. \text{ Тому значення } f = -4 \text{ зменшує на 1 кількість}$$

ненульових квадратичних лишків f , які в сумі $2^2 + f = g$ формують ненульовий квадратичний лишок.

На основі розглянутих випадків для виразу (3.12) сформулюємо наступне твердження.

Твердження 3.1. Справедливе наступне:

1. Нехай h є ненульовим квадратичним лишком у \mathbb{Z}_p , а f набуває всіх ненульових квадратичних лишків у \mathbb{Z}_p . Тоді сума $h + f = g$ є квадратичним лишком рівно l разів, а квадратичним нелишком – l разів для простого $p = 4l + 1$ і $l + 1$ разів для простого $p = 4l + 3$.
2. Нехай h є квадратичним нелишком у \mathbb{Z}_p , а f набуває всіх квадратичних нелишків у \mathbb{Z}_p . Тоді сума $h + f = g$ є квадратичним лишком рівно $l + 1$ разів, а квадратичним нелишком – $l - 1$ разів для простого $p = 4l + 1$ і l разів для простого $p = 4l + 3$.

Доведення.

Спочатку в пункті 1 розглянемо окремо випадки $p = 3$ і $p = 5$.

Для $p = 3 = 4 \cdot 0 + 3$ величина $l = 0$.

Для $u \in \mathbb{Z}_3 = \{0; 1; 2\}$ значення $u^2 \in \{0; 1\}$. Тоді $h = f = 1$ і $g = 1 + 1 = 2 \neq u^2 \in \mathbb{Z}_3$.

Отже, значення $g = h + f$ стає:

- нуль разів квадратичним лишком, $0 = l$;
- один раз квадратичним нелишком, $1 = l + 1$.

Для $p = 5 = 4 \cdot 1 + 1$ величина $l = 1$. Для При $u \in \mathbb{Z}_5 = \{0; 1; 2; 3; 4\}$ значення $u^2 \in \{0; 1; 4\}$.

Значення суми $g = h + f$ за фіксованого h є по одному разу квадратичним лишком і нелишком, $1 = l$.

Тепер розглянемо в пункті 1 випадок простих $p \geq 7$.

Нехай $\{QR\}$, $\{QNR\}$ – множини квадратичних лишків і нелишків у \mathbb{Z}_p відповідно. Використаємо позначення наслідку 3.7: $f \neq 0$, $f, g \in \{QR\}$, $2^2 + f = g$. Для довільного $u \in \mathbb{Z}_p$, $u \neq 0$, множини $u^2 \cdot \{QR\} \equiv \{QR\}$, $u^2 \cdot \{QNR\} \equiv \{QNR\}$, а $2^2 \cdot \{1, 2, \dots, p-1\} \equiv \{1, 2, \dots, p-1\}$. Отже, $\{2^2 \cdot u^2\} \equiv \{QR\} \setminus 0$. Нехай у рівності $2^2 \cdot u^2 + f \cdot u^2 = g \cdot u^2$, за визначеного квадратичного лишка $h = 2^2 \cdot u^2$, лишки $f \cdot u^2$ набувають значень усіх ненульових квадратичних лишків у \mathbb{Z}_p . Тоді з наслідку 3.7 і наслідку 3.3 слідує перший пункт твердження 3.1.

Спочатку в пункті 2 розглянемо окремо випадки $p = 3$ і $p = 5$.

Для $v \neq u^2 \in \mathbb{Z}_3$ значення $v = 2$, величина $l = [3/4] = 0$. Тоді $h = f = 2$ і $g = 2 + 2 = 1^2$.

Значення суми g стає:

- один раз квадратичним лишком, $1 = l + 1$;
- нуль разів квадратичним нелишком, $0 = l$.

Для $v \neq u^2 \in \mathbb{Z}_5$ значення $v \in \{2; 3\}$. Величина $l = [5/4] = 1$ і значення g за фіксованого h стає:

- два рази квадратичним лишком, $2 = l + 1$;
- нуль разів квадратичним нелишком, $0 = l - 1$.

Тепер розглянемо в пункті 2 випадок простих $p \geq 7$.

Нехай тепер f набуває тих ненульових значень квадратичних лишків у \mathbb{Z}_p , для яких відповідно до наслідку 3.7 сума $2^2 + f = g$ є квадратичним нелишком.

Для довільного квадратичного нелишка $u \in \{QNR\} \subset \mathbb{Z}_p$ зберігається рівність $2^2 \cdot u + f \cdot u = g \cdot u \neq 0$.

Виходячи з властивості мультиплікативності символу Лежандра, множини $u \cdot \{QR\} = \{QNR\}$, $u \cdot \{QNR\} = \{QR\}$ (див. наслідок 2 розділу 5 §1 [72]).

Нехай за сталого квадратичного нелишка $h = 2^2 \cdot u$ квадратичний нелишок $f \cdot u$ набуває всіх значень з множини $\{QNR\}$.

Згідно з наслідком 3.7 для простого $p = 4l + 1$ сума $2^2 + f$ дає квадратичний нелишок g рівно l разів, а для $p = 4l + 3$ – $l + 1$ разів. Тому сума $(2^2 + f) \cdot u = h + f \cdot u = g \cdot u$ для простого $p = 4l + 1$ дає квадратичний лишок $g \cdot u \neq 0$ рівно l разів, а для $p = 4l + 3$ – $l + 1$ разів. Враховуючи наслідок 3.4 про властивість симетрії розташування квадратичних лишків і квадратичних нелишків у впорядкованій за зростанням множині лишків за простим модулем $p = 4l + 1$, маємо: значення $f \cdot u = p - h$ є також квадратичним нелишком для квадратичного нелишка h . Таким чином, справедливе наступне: сума $g \cdot u = h + f \cdot u$ квадратичного нелишка h з усіма можливими квадратичними нелишками $f \cdot u$ у \mathbb{Z}_p є лишком рівно $l + 1$ разів.

Для завершення доведення другого пункту твердження нагадаємо, що в \mathbb{Z}_p для $p = 4l + 1$ існує $2l$ квадратичних нелишків f , а для $p = 4l + 3$ – таких значень f рівно $2l + 1$. Вище доведено, що для фіксованого значення нелишка h сума $h + f = g$ є рівно $l + 1$ разів лишком у \mathbb{Z}_p . Тому сума $h + f = g$ є квадратичним нелишком $2l - (l + 1) = l - 1$ разів для $p = 4l + 1$ і $2l + 1 - (l + 1) = l$ разів – для $p = 4l + 3$.

Твердження 3.1 доведено. ■

Твердження 3.2. Нехай h – ненульовий квадратичний лишок (нелишок), а f набуває всі можливі квадратичні нелишки (ненульові лишки) у \mathbb{Z}_p . Тоді сума $h + f = g$ є:

- 1) по l разів квадратичним лишком і нелишком для простого $p = 4l + 1$;
- 2) $l + 1$ разів квадратичним лишком і l разів квадратичним нелишком для простого $p = 4l + 3$.

Доведення.

Спочатку розглянемо окремо випадки $p = 3$ і $p = 5$.

Для \mathbb{Z}_3 величина $l = [3/4] = 0$, квадратичний лишок $h = 1$, квадратичний нелишок $f = 2$. Тоді $g = h + f$ стає квадратичним лишком один раз, $1 = l + 1$, і квадратичним нелишком – нуль разів, $0 = l$.

Для \mathbb{Z}_5 величина $l = [5/4] = 1$, квадратичні лишки $h \in \{1; 4\}$, квадратичні нелишки $f \in \{2; 3\}$. Значення g за фіксованого h стає квадратичним лишком і квадратичним нелишком по одному разу, $1 = l$.

Тепер розглянемо випадок простих $p \geq 7$.

Нехай $h \neq 0$, а $f \in \{1; 2; \dots; p-1\}$. Можливі значення суми $h + f = g$ утворюють множину $F_h = \{0; 1; 2; \dots; p-1\} \setminus h$.

Нехай просте $p = 4l + 1$.

Якщо $h \neq 0$ є квадратичним лишком, то в F_h по $2l$ квадратичних лишків і нелишків.

Згідно з пунктом 1 твердження 3.1 для квадратичних лишків $f \neq 0$ значення $g = h + f$ рівно l разів стає квадратичним лишком і l разів – квадратичним нелишком. Відповідно до наслідка 3.4 для квадратичних нелишків f , сума $g = h + f \neq 0$. Тому, за принципом Діріхле, значення g у множині F_h для $2 \cdot l$ квадратичних нелишків f стає рівно $2 \cdot l - l = l$ разів квадратичним лишком і $2 \cdot l - l = l$ разів – квадратичним нелишком.

Якщо h є квадратичним нелишком, то в F_h є $2l+1$ квадратичних лишків і $2l-1$ квадратичних нелишків.

Відповідно до пункту 2 твердження 3.1 для квадратичних нелишків f значення $g = h + f$ рівно $l+1$ раз стає квадратичним лишком і $l-1$ раз – квадратичним нелишком. Тому в результаті сумування квадратичного нелишка h по чергово з $2 \cdot l$ квадратичними лишками $f \neq 0$ сума $g = h + f$ буде $(2 \cdot l + 1) - (l + 1) = l$ разів квадратичним лишком і, відповідно, $(2 \cdot l - 1) - (l - 1) = l$ разів – квадратичним нелишком.

Нехай тепер просте $p = 4l + 3$.

Якщо $h \neq 0$ є квадратичним лишком, то в F_h по $2l+1$ квадратичних лишків і нелишків.

Відповідно до пункту 1 твердження 3.1 сума $g = h + f$ для квадратичних лишків $f \neq 0$ стає l разів квадратичним лишком і $l+1$ разів – квадратичним нелишком. Тому для $2 \cdot l$ квадратичних нелишків f сума $g = h + f$ є $(2 \cdot l + 1) - l = l + 1$ раз квадратичним лишком і $(2 \cdot l + 1) - (l + 1) = l$ разів – квадратичним нелишком.

Якщо ж h є квадратичним нелишком, то в F_h рівно $2l+2$ квадратичних лишків і $2l$ нелишків. Відповідно до пункту 2 твердження 3.1 сума $g = h + f$ для квадратичних нелишків f є $l+1$ раз квадратичним лишком і l разів – квадратичним нелишком. Тому для $2 \cdot l + 1$ квадратичних лишків $f \neq 0$ сума $g = h + f$ стає $(2 \cdot l + 2) - (l + 1) = l + 1$ раз квадратичним лишком і $2 \cdot l - l = l$ разів – квадратичним нелишком.

Твердження 3.2 доведено. ■

Підсумовуючи твердження 3.1 і 3.2, продемонструємо в таблицях 3.3 і 3.4 наглядно розподіл кількості квадратичних лишків і нелишків для сум

$\{qr\} \setminus 0 + \{QR\} \setminus 0$, $\{qnr\} + \{QNR\}$, $\{qr\} \setminus 0 + \{QNR\}$, коли перший доданок фіксований (його позначено малими літерами), а другий набуває всіх можливих значень з множини визначення, за простого $p = 4l + 1$ і $p = 4l + 3$.

Таблиця 3.3. Кількість квадратичних лишків і нелишків для $p = 4l + 1$

$\{QR\} \setminus \{QNR\}$	$\{QR\} \setminus 0$	$\{QNR\}$
$\{qr\} \setminus 0$	l	l
$\{qnr\}$	l	$l+1$

Таблиця 3.4. Кількість квадратичних лишків і нелишків для $p = 4l + 3$

$\{QR\} \setminus \{QNR\}$	$\{QR\} \setminus 0$	$\{QNR\}$
$\{qr\} \setminus 0$	l	$l+1$
$\{qnr\}$	$l+1$	$l+1$

Розглянемо приклади для $p = 4l + 1$ і $p = 4l + 3$.

Приклад 4.

Побудуємо можливі комбінації $\{QR\} \setminus 0 + \{QR\} \setminus 0$, $\{QNR\} + \{QNR\}$, $\{QR\} \setminus 0 + \{QNR\}$ та визначимо, з якою частотою в цих сумах зустрічаються значення, що належать множинам $\{QR\}$ і $\{QNR\}$.

I. $p = 4l + 1$

1. Нехай $p = 4l + 1 = 4 \cdot 3 + 1 = 13$.

Спершу нагадаємо, що для $p = 13$ ненульовими квадратичними лишками є: $\{1; 3; 4; 9; 10; 12\}$. Відповідно, квадратичними нелишками є: $\{2; 5; 6; 7; 8; 11\}$.

Можливі суми $\{QR\} \setminus 0 + \{QR\} \setminus 0$, $\{QNR\} + \{QNR\}$, $\{QR\} \setminus 0 + \{QNR\}$ зведемо в таблиці 3.5-3.7.

Таблиця 3.5. Значення $\{QR\} \setminus 0 + \{QR\} \setminus 0$ у \mathbb{Z}_{13}

$\{QR\} \setminus 0 \backslash \{QR\} \setminus 0$	1	3	4	9	10	12
1	2	4	5	10	11	0
3	4	6	7	12	0	2
4	5	7	8	0	1	3
9	10	12	0	5	6	8
10	11	0	1	6	7	9
12	0	2	3	8	9	11

Таблиця 3.6. Значення $\{QNR\} + \{QNR\}$ у \mathbb{Z}_{13}

$\{QNR\} \backslash \{QNR\}$	2	5	6	7	8	11
2	4	7	8	9	10	0
5	7	10	11	12	0	3
6	8	11	12	0	1	4
7	9	12	0	1	2	5
8	10	0	1	2	3	6
11	0	3	4	5	6	9

Таблиця 3.7. Значення $\{QR\} \setminus 0 + \{QNR\}$ у \mathbb{Z}_{13}

$\{QR\} \setminus 0 \backslash \{QNR\}$	2	5	6	7	8	11
1	3	6	7	8	9	12
3	5	8	9	10	11	1
4	6	9	10	11	12	2
9	11	1	2	3	4	7
10	12	2	3	4	5	8
12	1	4	5	6	7	10

У таблицях 3.5-3.7 сірим кольором виділено випадки, коли сума є квадратичним лишком у \mathbb{Z}_{13} .

Результат ілюструє твердження 3.1 і 3.2:

- кожен рядок (стовпець) таблиці 3.4 містить рівно $l = 3$ квадратичні лишки і $l = 3$ квадратичні нелишки;
- кожен рядок (стовпець) таблиці 3.5 містить рівно $l + 1 = 4$ квадратичні лишки і $l - 1 = 2$ квадратичні нелишки;
- кожен рядок (стовпець) таблиці 3.6 містить рівно $l = 3$ квадратичні лишки і $l = 3$ квадратичні нелишки.

2. Нехай $p = 4l + 1 = 4 \cdot 4 + 1 = 17$.

Для $p = 17$ ненульовими квадратичними лишками є: $\{1; 2; 4; 8; 9; 13; 15; 16\}$

. Відповідно, квадратичними нелишками є: $\{3; 5; 6; 7; 10; 11; 12; 14\}$.

Можливі суми $\{QR\} \setminus 0 + \{QR\} \setminus 0$, $\{QNR\} + \{QNR\}$, $\{QR\} \setminus 0 + \{QNR\}$ зведемо в таблиці 3.8-3.10.

Таблиця 3.8. Значення $\{QR\} \setminus 0 + \{QR\} \setminus 0$ у \mathbb{Z}_{17}

$\{QR\} \setminus 0$ \ $\{QR\} \setminus 0$	1	2	4	8	9	13	15	16
1	2	3	5	9	10	14	16	0
2	3	4	6	10	11	15	0	1
4	5	6	8	12	13	0	2	3
8	9	10	12	16	0	4	6	7
9	10	11	13	0	1	5	7	8
13	14	15	0	4	5	9	11	12
15	16	0	2	6	7	11	13	14
16	0	1	3	7	8	12	14	15

Таблиця 3.9. Значення $\{QNR\} + \{QNR\}$ у \mathbb{Z}_{17}

$\{QNR\}$ \ $\{QNR\}$	3	5	6	7	10	11	12	14
3	6	8	9	10	13	14	15	0
5	8	10	11	12	15	16	0	2
6	9	11	12	13	16	0	1	3
7	10	12	13	14	0	1	2	4
10	13	15	16	0	3	4	5	7
11	14	16	0	1	4	5	6	8
12	15	0	1	2	5	6	7	9
14	0	2	3	4	7	8	9	11

Таблиця 3.10. Значення $\{QR\} \setminus 0 + \{QNR\}$ у \mathbb{Z}_{17}

$\{QR\} \setminus 0 \backslash \{QNR\}$	3	5	6	7	10	11	12	14
1	4	6	7	8	11	12	13	15
2	5	7	8	9	12	13	14	16
4	7	9	10	11	14	15	16	1
8	11	13	14	15	1	2	3	5
9	12	14	15	16	2	3	4	6
13	16	1	2	3	6	7	8	10
15	1	3	4	5	8	9	10	12
16	2	4	5	6	9	10	11	13

У таблицях 3.8-3.10 сірим кольором виділено випадки, коли сума є квадратичним лишком у \mathbb{Z}_{17} .

Отриманий результат також ілюструє твердження 3.1 і 3.2:

- кожен рядок (стовпець) таблиці 3.8 містить рівно $l = 4$ квадратичні лишки і $l = 4$ квадратичні нелишки;
- кожен рядок (стовпець) таблиці 3.9 містить рівно $l + 1 = 5$ квадратичні лишки і $l - 1 = 3$ квадратичні нелишки;
- кожен рядок (стовпець) таблиці 3.10 містить рівно $l = 4$ квадратичні лишки і $l = 4$ квадратичні нелишки.

II. $p = 4l + 3$

1. Нехай $p = 4l + 3 = 4 \cdot 2 + 3 = 11$.

Для $p = 11$ ненульовими квадратичними лишками є: $\{1; 3; 4; 5; 9\}$.

Відповідно, квадратичними нелишками є: $\{2; 6; 7; 8; 10\}$.

Можливі суми $\{QR\} \setminus 0 + \{QR\} \setminus 0$, $\{QNR\} + \{QNR\}$, $\{QR\} \setminus 0 + \{QNR\}$ зведемо в таблиці 3.11-3.13.

Таблиця 3.11. Значення $\{QR\} \setminus 0 + \{QR\} \setminus 0$ у \mathbb{Z}_{11}

$\{QR\} \setminus 0 \backslash \{QR\} \setminus 0$	1	3	4	5	9
1	2	4	5	6	10
3	4	6	7	8	1
4	5	7	8	9	2
5	6	8	9	10	3
9	10	1	2	3	7

Таблиця 3.12. Значення $\{QNR\} + \{QNR\}$ у \mathbb{Z}_{11}

$\{QNR\} \backslash \{QNR\}$	2	6	7	8	10
2	4	8	9	10	1
6	8	1	2	3	5
7	9	2	3	4	6
8	10	3	4	5	7
10	1	5	6	7	9

Таблиця 3.13. Значення $\{QR\} \setminus 0 + \{QNR\}$ у \mathbb{Z}_{11}

$\{QR\} \setminus 0 \backslash \{QNR\}$	2	6	7	8	10
1	3	7	8	9	0
3	5	9	10	0	2
4	6	10	0	1	3
5	7	0	1	2	4
9	0	4	5	6	8

У таблицях 3.11-3.13 сірим кольором виділено випадки, коли сума є квадратичним лишком у \mathbb{Z}_{11} .

Результат підтверджує твердження 3.1 і 3.2:

- кожен рядок (стовпець) таблиці 3.11 містить рівно $l = 2$ квадратичні лишки і $l + 1 = 3$ квадратичні нелишки;
- кожен рядок (стовпець) таблиці 3.12 містить рівно $l + 1 = 3$ квадратичні лишки і $l = 2$ квадратичні нелишки;

– кожен рядок (стовпець) таблиці 3.13 містить рівно $l+1=3$ квадратичні лишки і $l=2$ квадратичні нелишки.

2. Нехай $p = 4l + 3 = 4 \cdot 4 + 3 = 19$.

Для $p = 19$ ненульовими квадратичними лишками є: $\{1; 4; 5; 6; 7; 9; 11; 16; 17\}$. Відповідно, квадратичними нелишками є: $\{2; 3; 8; 10; 12; 13; 14; 15; 18\}$.

Можливі суми $\{QR\} \setminus 0 + \{QR\} \setminus 0$, $\{QNR\} + \{QNR\}$, $\{QR\} \setminus 0 + \{QNR\}$ зведемо в таблиці 3.14-3.16.

Таблиця 3.14. Значення $\{QR\} \setminus 0 + \{QR\} \setminus 0$ у \mathbb{Z}_{19}

$\{QR\} \setminus 0$ $\{QR\} \setminus 0$	1	4	5	6	7	9	11	16	17
1	2	5	6	7	8	10	12	17	18
4	5	8	9	10	11	13	15	1	2
5	6	9	10	11	12	14	16	2	3
6	7	10	11	12	13	15	17	3	4
7	8	11	12	13	14	16	18	4	5
9	10	13	14	15	16	18	1	6	7
11	12	15	16	17	18	1	3	8	9
16	17	1	2	3	4	6	8	13	14
17	18	2	3	4	5	7	9	14	15

Таблиця 3.15. Значення $\{QNR\} + \{QNR\}$ у \mathbb{Z}_{19}

$\{QNR\} \backslash \{QNR\}$	2	3	8	10	12	13	14	15	18
2	4	5	10	12	14	15	16	17	1
3	5	6	11	13	15	16	17	18	2
8	10	11	16	18	1	2	3	4	7
10	12	13	18	1	3	4	5	6	9
12	14	15	1	3	5	6	7	8	11
13	15	16	2	4	6	7	8	9	12
14	16	17	3	5	7	8	9	10	13
15	17	18	4	6	8	9	10	11	14
18	1	2	7	9	11	12	13	14	17

Таблиця 3.16. Значення $\{QR\} \setminus 0 + \{QNR\}$ у \mathbb{Z}_{19}

$\{QR\} \setminus 0 \backslash \{QNR\}$	2	3	8	10	12	13	14	15	18
1	3	4	9	11	13	14	15	16	0
4	6	7	12	14	16	17	18	0	3
5	7	8	13	15	17	18	0	1	4
6	8	9	14	16	18	0	1	2	5
7	9	10	15	17	0	1	2	3	6
9	11	12	17	0	2	3	4	5	8
11	13	14	0	2	4	5	6	7	10
16	18	0	5	7	9	10	11	12	15
17	0	1	6	8	10	11	12	13	16

У таблицях 3.14-3.16 сірим кольором виділено випадки, коли сума є квадратичним лишком у \mathbb{Z}_{19} .

Отриманий результат також ілюструє твердження 3.1 і 3.2:

- кожен рядок (стовпець) таблиці 3.14 містить рівно $l = 4$ квадратичні лишки і $l + 1 = 5$ квадратичних нелишків;
- кожен рядок (стовпець) таблиці 3.15 містить рівно $l + 1 = 5$ квадратичних лишків і $l = 4$ квадратичні нелишки;
- кожен рядок (стовпець) таблиці 3.16 містить рівно $l + 1 = 5$ квадратичних лишків і $l = 4$ квадратичні нелишки.

Зауваження 3.7. Матриця A має максимальний порядок $\text{ord}(A)$ тільки тоді, коли $\frac{r}{4}$ є примітивним елементом у \mathbb{Z}_p .

Доведення.

Виходячи з виразу (2.1), $\text{ord}(A)$ набуває максимального значення тільки тоді, коли Δ_a є примітивним у \mathbb{Z}_p з порядком $p - 1$.

Зауважимо, що $\Delta_a = \lambda_1 \lambda_2 = a(a+k) - b$. Оскільки, $b = \frac{q-k^2}{4}$, маємо

$$\Delta_a = a(a+k) - b = \frac{(2a+k)^2 - q}{4}. \text{ Беручи до уваги вираз (3.10) } (2a+k)^2 = q+r,$$

значення $\Delta_a = \frac{r}{4}$. ■

Попередній приклад ілюструє справедливість зауваження 3.7.

Зауваження 3.8. Оскільки відображення $\frac{\{QNR\}}{4}$ є перетворенням множини $\{QNR\}$: $\frac{\{QNR\}}{4} = \{QNR\}$, значення r для максимального порядку $ord(A)$ обчислюється шляхом множення примітивних елементів \mathbb{Z}_p на 4.

Зауваження 3.9. Порядок $ord(A)$ визначає пара значень $\{q; r\}$ для довільного $k \in \mathbb{Z}_p$, $b = \frac{q-k^2}{4}$ і $a \in \mathbb{Z}_p$: $(2a+k)^2 = q+r$.

Доведення.

Характеристичне рівняння матриці $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ має вигляд

$$\lambda^2 - (2a+k)\lambda + \Delta_a = 0. \text{ Оскільки } (2a+k)^2 = q+r \text{ згідно з (3.10), а } \Delta_a = \frac{r}{4},$$

характеристичне рівняння можна записати так: $\lambda^2 - (q+r)^{\frac{1}{2}}\lambda + 4^{-1}r = 0$.

Таким чином, власні значення $\lambda_{1,2}$ матриці A залежать тільки від значень q і r .

Зважаючи на те, що $ord(A)$ визначають власні значення $\lambda_{1,2}$ матриці A , а також значення $\Delta_a = \frac{r}{4}$, вибір значення k не впливає на $ord(A)$. ■

3.4. Опис методу вибору параметрів b і k матричного поля $F_{b,k}$ і примітивного елементу в ньому

Спершу розглянемо випадок, коли просте p є числом Мерсенна

$(p = 2^m - 1)$ або $3 \leq \frac{p+1}{2} = \rho$ є простим числом.

3.4.1. Спеціальний важливий випадок методу вибору параметрів b і k матричного поля $F_{b,k}$ і примітивного елементу в ньому, коли

p є числом Мерсенна або $3 \leq \frac{p+1}{2} = \rho$ є простим числом

Згідно з зауваженням 2.4 матриця $A = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ з $a \neq -\frac{k}{2}$ буде

примітивним елементом поля $F_{b,k}$ тоді і тільки тоді, коли визначник $\det(A) = \Delta_a$ є примітивним у полі \mathbb{Z}_p .

Тоді метод вибору параметрів b і k поля $F_{b,k}$ і примітивного елементу в ньому полягає в виконанні наступних п'яти кроків:

- 1) знайти первісний корінь σ_0 у \mathbb{Z}_p і обрати примітивний елемент σ в \mathbb{Z}_p : $\sigma = \sigma_0^i$, $GCF(i, p-1) = 1$; покласти значення $r = 4\sigma$, тобто обрати $\Delta_a = \sigma$;
- 2) для значення $2a + k = y \in \mathbb{Z}_p^*$, тобто $y = 1, 2, \dots, p-1$, обчислити $q = y^2 - 4\sigma$;
- 3) застосовуючи квадратичний закон взаємності [72], перевірити, чи є значення q квадратичним нелишком у \mathbb{Z}_p : за означенням символу Лежандра, перевірити рівність

$$\left(\frac{q}{p}\right) = -1 \text{ або } \left(\frac{y^2 - 4\sigma}{p}\right) = -1; \quad (3.16)$$

- 4) для розв'язку y_0 рівняння (3.16) і довільного значення параметра $k \in \mathbb{Z}_p$ обчислити параметри

$$q_0 = y_0^2 - 4\sigma, \quad b_0 = \frac{q_0 - k^2}{4}, \quad a_0 = \frac{y_0 - k}{2}; \quad (3.17)$$

- 5) матриця

$$A(k) = \begin{pmatrix} a_0 & 1 \\ b_0 & a_0 + k \end{pmatrix} = \begin{pmatrix} \frac{y_0 - k}{2} & 1 \\ \frac{y_0^2 - k^2 - 4\sigma}{4} & \frac{y_0 + k}{2} \end{pmatrix}$$

є примітивним елементом у матричному полі $F_{b,k}$ для кожного

$$k \in \mathbb{Z}_p.$$

Нагадаємо, що на мові символів Лежандра закон квадратичної взаємності має таке формулювання: для двох різних непарних простих чисел

$$p \quad \text{і} \quad q \quad \text{значення} \quad \left(\frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q} \right). \quad \text{Крім того,} \quad \left(\frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}},$$

$$\left(\frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}}.$$

Зауваження 3.10. Кількість $N_q(\sigma)$ розв'язків по y рівняння (3.16) для заданого примітивного елемента $\sigma \in \mathbb{Z}_p$ оцінюється так:

$$\left\lfloor \frac{p}{4} \right\rfloor \leq N_q(\sigma) \leq \left\lfloor \frac{p}{4} \right\rfloor + 1. \quad (3.18)$$

Доведення.

Очевидно, що примітивний елемент $\sigma \in \mathbb{Z}_p$ є квадратичним нелишком, інакше б усі елементи \mathbb{Z}_p були лишками (див. також (3.8)). Тому значення

$$\text{символу Лежандра:} \quad \left(\frac{-4\sigma}{p} \right) = \left(\frac{-1}{p} \right) \cdot \left(\frac{2^2}{p} \right) \cdot \left(\frac{\sigma}{p} \right) = (-1)^{\frac{p-1}{2}} \cdot 1 \cdot (-1) = (-1)^{\frac{p+1}{2}}.$$

Отже, елемент -4σ є нелишком для $p = 4l + 1$ і лишком для $p = 4l + 3$.

Звідси, в силу твердження 3.2 і пункту 1 з твердження 3.1, слідує, що:

- сума $(-4\sigma + y^2)$ елемента -4σ як квадратичного нелишка для $p = 4l + 1$ з усіма ненульовими квадратичними лишками y^2 із \mathbb{Z}_p^* буде нелишком рівно $l = \left\lfloor \frac{p}{4} \right\rfloor$ разів;
- сума $(-4\sigma + y^2)$ елемента -4σ як квадратичного лишка для $p = 4l + 3$ з усіма ненульовими квадратичними лишками y^2 буде нелишком у \mathbb{Z}_p рівно $(l + 1)$ разів. ■

Алгоритм вибору параметрів b і k поля $F_{b,k}$ і примітивного елемента в ньому наведено на рисунку 3.1.

1. Set prime $p : p = 2^m - 1$ or $3 \leq \frac{p+1}{2} = \rho$ is a prime
2. Factorize $p-1$, find the primitive root σ_0 in \mathbb{Z}_p
3. $\sigma \leftarrow \sigma_0^i$, $GCF(i, p-1) = 1$
4. $r \leftarrow 4\sigma$
5. **for** $y = 1$ to $p-1$
6. $q \leftarrow y^2 - 4\sigma$
7. **if** $\left(\frac{q}{p}\right) = -1$ **then**
8. $y_0 \leftarrow y$
9. **break**
10. **end if**
11. **end for**
12. $q_0 \leftarrow y_0^2 - 4\sigma$
13. $b_0 \leftarrow \frac{q_0 - k^2}{4}$
14. $a_0 \leftarrow \frac{y_0 - k}{2}$
15. $A(k) \leftarrow \begin{pmatrix} \frac{y_0 - k}{2} & 1 \\ \frac{y_0^2 - k^2 - 4\sigma}{4} & \frac{y_0 + k}{2} \end{pmatrix}, k \in \mathbb{Z}_p$

Рисунок 3.1. Алгоритм вибору параметрів b і k поля $F_{b,k}$ і

примітивного елементу в ньому для простого $p = 2^m - 1$ або простого $\frac{p+1}{2} \geq 3$

Виконаємо оцінку часової складності цього алгоритму.

Для цього будемо використовувати загальновідомі оцінки складності операцій у скінченному полі [80], [81], [82], [83].

Крім того, для оцінювання прогнозованого порядку часу побудови матричного поля $F_{b,k}$ і примітивного елементу цього поля суттєву роль відіграють результати, подані в таблицях 3.3 і 3.4. Там показано, що обираючи на проміжку $(0; p)$ довільним чином квадратичний лишок або нелишок та додаючи його до наперед заданого лишка або нелишка, із ймовірністю, близькою до $1/2$ (за великих p), отримуємо нелишок (лишок).

Таким чином:

- складність імовірнісного алгоритму обчислення первісного кореня за модулем p за відомого розкладу числа $p - 1$ на прості співмножники дорівнює $O(\log^2 p)$;
- складність операції розкладання числа $p - 1$ на прості співмножники із застосування швидкого методу решета числового поля [84] дорівнює $L_p \left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}} \right] = O \left(\exp \left(\left(\sqrt[3]{\frac{64}{9}} + o(1) \right) (\log p)^{\frac{1}{3}} (\log \log p)^{\frac{2}{3}} \right) \right)$;
- складність операції знаходження оберненого елементу в \mathbb{Z}_p дорівнює $O(\log p)$;
- складність знаходження символу Лежандра дорівнює $O(\log p)$.

Прогнозований порядок часу виконання алгоритму (кількість арифметичних операцій) на рисунку 3.1 дорівнює

$$L_p \left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}} \right] + O(\log^2 p) + O(\log p) + O(\log p) = L_p \left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}} \right].$$

Приклад 5.

Нехай $p = 2^5 - 1 = 31$. Тоді:

1) нехай $\sigma = 3$ – найменший первісний корінь;

2) нехай $y = 1$, тоді $q = 1 - 4 \cdot 3 = -11 = 20$;

$$3) \left(\frac{q}{p} \right) = \left(\frac{20}{31} \right) = \left(\frac{2^2 \cdot 5}{31} \right) = \left(\frac{2}{31} \right)^2 \cdot \left(\frac{5}{31} \right) = 1 \cdot (-1)^{\frac{30 \cdot 4}{2}} \cdot \left(\frac{31}{5} \right) = \left(\frac{1}{5} \right) = 1.$$

Повертаємося до кроку 2 методу:

2) нехай $y = 2$, тоді $q = 2^2 - 4 \cdot 3 = -8$;

$$3) \left(\frac{q}{p} \right) = \left(\frac{-2^3}{31} \right) = \left(\frac{-1}{31} \right) \cdot \left(\frac{2}{31} \right)^3 = (-1)^{\frac{30}{2}} \cdot (-1)^{\frac{30 \cdot 32}{8}} = -1. \quad \text{Отже, оберемо}$$

$y = 2$ як одне з розв'язків рівняння (3.16);

4) за (3.17) обчислимо параметри $q_0 = -8 = 23$, $b_0 = \frac{23 - k^2}{4}$, $a_0 = \frac{2 - k}{2}$;

$$5) \text{ матриця } A(k) = \begin{pmatrix} \frac{2-k}{2} & 1 \\ \frac{23-k^2}{4} & \frac{2+k}{2} \end{pmatrix} \in \text{ примітивним елементом}$$

матричного поля $F_{b_0, k}$ для кожного $k \in \mathbb{Z}_{31}$. Наприклад, для $k = 12$

значення $A(12) = \begin{pmatrix} 26 & 1 \\ 24 & 7 \end{pmatrix} \in \text{ примітивним елементом матричного}$

поля $F_{24, 12}$ порядку $|F_{24, 12}| = p^2 = 31^2$.

Приклад 6.

Нехай $p = 61$, $3 \leq \frac{p+1}{2} = 31$ – просте. Тоді:

1) нехай $\sigma = 2$ – найменший первісний корінь;

2) нехай $y = 1$, тоді $q = 1 - 4 \cdot 2 = -7 = 54$;

3) обчислюємо

$$\left(\frac{q}{p}\right) = \left(\frac{54}{61}\right) = \left(\frac{2}{61}\right) \cdot \left(\frac{3}{61}\right)^3 = (-1)^{\frac{60-62}{8}} \cdot (-1)^{\frac{30 \cdot 2}{2 \cdot 2}} \cdot \left(\frac{61}{3}\right) = -1 \cdot (-1) \cdot \left(\frac{1}{3}\right) = 1.$$

Повертаємося до кроку 2 методу:

2) нехай $y = 2$, тоді $q = 2^2 - 4 \cdot 2 = -4$;

3) $\left(\frac{q}{p}\right) = \left(\frac{-2^2}{61}\right) = 1$. Повертаємося до кроку 2 методу:

2) нехай $y = 3$, тоді $q = 3^2 - 4 \cdot 2 = 1$;

3) $\left(\frac{q}{p}\right) = \left(\frac{1}{61}\right) = 1$. Повертаємося до кроку 2 методу:

2) нехай $y = 4$, тоді $q = 4^2 - 4 \cdot 2 = 8$;

3) $\left(\frac{q}{p}\right) = \left(\frac{2^3}{61}\right) = -1$. Отже, оберемо $y = 4$ як одне з розв'язків рівняння (3.16);

4) за (3.17) обчислимо параметри $q_0 = 8$, $b_0 = \frac{8 - k^2}{4}$, $a_0 = \frac{4 - k}{2}$;

5) матриця $A(k) = \begin{pmatrix} \frac{4-k}{2} & 1 \\ \frac{8-k^2}{4} & \frac{4+k}{2} \end{pmatrix}$ примітивним елементом матричного

поля $F_{b_0, k}$ для кожного $k \in \mathbb{Z}_{61}$.

Зокрема, значення $A(5) = \begin{pmatrix} 30 & 1 \\ 11 & 35 \end{pmatrix}$ є примітивним елементом

матричного поля $F_{11,5}$ порядку $|F_{11,5}| = p^2 = 61^2$.

Означення 3.3. Лічильною функцією нелишків N_q називається кількість різних значень нелишків $q \in \mathbb{Z}_p$, яких набуває функція $q = y^2 - 4\sigma$

для різних $y \in \left\{ \pm 1; \pm 2; \dots; \pm \frac{p-1}{2} \right\}$ і примітивних елементів $\sigma \in \mathbb{Z}_p$ (див. (3.17)).

Означення 3.4. Частотою n_q нелишка $q \in \mathbb{Z}_p$ як значення функції $q = y^2 - 4\sigma$ називається кількість різних значень примітивних елементів $\sigma \in \mathbb{Z}_p$, для яких цей нелишок з'являється.

Означення 3.5. Кратністю κ_q нелишка $q \in \mathbb{Z}_p$ як значення функції $q = y^2 - 4\sigma$ називається кількість різних значень $y \in \left\{ \pm 1; \pm 2; \dots; \pm \frac{p-1}{2} \right\}$, для яких цей нелишок з'являється.

Через $N_{b,k}$ позначимо кількість різних пар параметрів $(b; k)$, які обираються за вказаним методом та задають усі матричні поля $F_{b,k}$ над \mathbb{Z}_p . За формулою (3.17) параметр $b = \frac{q - k^2}{4}$. За фіксованого параметра k функція $f = q - k^2$ є бієкцією відносно аргументу q . Тому у відповідності до означення 3.3, число $N_{b,k}$ задовольняє рівності $N_{b,k} = N_q \cdot p$, де $N_q \leq \frac{p-1}{2}$.

У силу зауваження 3.10, серед значень функції $q = y^2 - 4\sigma$ для кожного примітивного елемента $\sigma \in \mathbb{Z}_p$ існує не менше $l = \left\lceil \frac{p}{4} \right\rceil$ квадратичних нелишків. Тому із оцінки (3.18) слідує, що $N_q \geq N_q(\sigma) \geq \left\lceil \frac{p}{4} \right\rceil$.

Зауваження 3.11. Якщо просте p є числом Мерсенна або $3 \leq \frac{p+1}{2} = \rho$ є простим числом, то потужність сімейства $\{F_{b,k}\}$ скінченних матричних полів над \mathbb{Z}_p , побудованих за запропонованим методом, задовольняє співвідношенню:

$$\left\lfloor \frac{p}{4} \right\rfloor \cdot p \leq |\{F_{b,k}\}| = N_q \cdot p \leq \frac{p-1}{2} \cdot p. \quad (3.19)$$

У відповідності до (3.17) параметр $a = \frac{y-k}{2}$. Тому для нелишка q як значення функції $q = y^2 - 4\sigma$ кратність κ_q вказує на кількість примітивних елементів матричного поля $F_{b,k}$ виду $A(k) = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$.

У силу твердження 2.5 (див. співвідношення (3.1)), існує рівно $\varphi(p+1)$ матриць $A(k)$, $k \in \mathbb{Z}_p$, що породжують примітивні елементи в полі $F_{b,k}$. Тому для кратності κ_q виконується нерівність:

$$\kappa_q \leq \varphi(p+1). \quad (3.20)$$

Якщо за фіксованого значення квадратичного лишка $y^2 \in \mathbb{Z}_p$ для примітивних елементів σ_1, σ_2 із \mathbb{Z}_p значення функції $q = y^2 - 4\sigma$ співпадають, то $\sigma_1 = \sigma_2$. Тому частота n_q нелишка $q \in \mathbb{Z}_p$ дорівнює кількості різних квадратичних лишків y^2 , що задають це q як значення функції. Рівність $y^2 = z^2$ у \mathbb{Z}_p виконується тільки за умови $z = \pm y$. Отже, кожен нелишок $q \in \mathbb{Z}_p$ для $y \neq 0$ може бути значенням функції $q = y^2 - 4\sigma$ за фіксованого примітивного $\sigma \in \mathbb{Z}_p$ тільки для двох значень $\pm y \in \left\{ \pm 1; \pm 2; \dots; \pm \frac{p-1}{2} \right\}$. Таким чином отримано наступні твердження.

Зауваження 3.12. Кратність κ_q нелишка $q \in \mathbb{Z}_p$ як значення функції $q = y^2 - 4\sigma$ дорівнює подвоєній частоті n_q , тобто

$$\kappa_q = 2n_q. \quad (3.21)$$

Наслідок 3.8. Кратність κ_q квадратичного нелишка $q \in \mathbb{Z}_p$ дорівнює кількості різних пар $(y; \sigma)$, для яких $q = y^2 - 4\sigma$.

Наслідок 3.9. Для обчислення лічильної функції N_q нелишків $q \in \mathbb{Z}_p$ і значень частот n_q (а також кратностей κ_q згідно з (3.21)) достатньо дослідити множину значень функції $q = y^2 - 4\sigma$ для $y \in \left\{1; 2; \dots; \frac{p-1}{2}\right\}$, $\sigma \in \mathbb{Z}_p$.

Приклад 7.

Нехай просте число $p = 37$ і $\frac{p+1}{2} = 19$, що є також простим числом.

Для опису сімейства скінченних полів $F_{b,k}$ над \mathbb{Z}_{37} визначимо всі можливі пари параметрів $(b; k)$. Зазначимо також усі примітивні елементи

$A(k)$ матричних полів $F_{b,k}$ виду $\begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$.

Найменшим первісним коренем у \mathbb{Z}_{37} є $\sigma_0 = 2$, а кількість усіх примітивних елементів поля \mathbb{Z}_{37} дорівнює $\varphi(p-1) = 12$. Множина всіх примітивних елементів \mathbb{Z}_{37} становить

$\Sigma = \{2^j : \langle j, 36 \rangle = 1\} = \{2; 32; 17; 13; 15; 18; 35; 5; 20; 24; 22; 19\}$. Пронумеруємо

елементи множини Σ у порядку слідування:

$\Sigma = \{\sigma_i : 1 \leq i \leq 12\} = \{2; 32; 17; 13; 15; 18; 35; 5; 20; 24; 22; 19\}$. Тоді набір значень $4\sigma_i$ складає множину $\{4\sigma_i : 1 \leq i \leq 12\} = \{8; 17; 31; 15; 23; 35; 29; 20; 6; 22; 14; 2\}$.

У формулі (3.17) елемент $q_{yi} = y^2 - 4\sigma_i$ повинен бути нелишком у \mathbb{Z}_{37} (задовольняти співвідношенню (3.16)). Квадрати y^2 , $1 \leq y \leq 18$, задають усі лишки в \mathbb{Z}_{37} .

Враховуючи наслідок 3.9, обчислимо значення q_{yi} , $1 \leq y \leq 18$, $1 \leq i \leq 12$ і складемо таблицю 3.17.

Таблиця 3.17. Значення q_{yi}

	σ_i	2	32	17	13	15	18	35	5	20	24	22	19
y	$y^2 \backslash 4\sigma_i$	8	17	31	15	23	35	29	20	6	22	14	2
1	1	30	21	7	23	15	3	9	18	32	16	24	36
2	4	33	24	10	26	18	6	12	21	35	19	27	2
3	9	1	29	15	31	23	11	17	26	3	24	32	7
4	16	8	36	22	1	30	18	24	33	10	31	2	14
5	25	17	8	31	10	2	27	33	5	19	3	11	23
6	36	28	19	5	21	13	1	7	16	30	14	22	34
7	12	4	32	18	34	26	14	20	29	6	27	35	10
8	27	19	10	33	12	4	29	35	7	21	5	13	25
9	7	36	27	13	29	21	9	15	24	1	22	30	5
10	26	18	9	32	11	3	28	34	6	20	4	12	24
11	10	2	30	16	32	24	12	18	27	4	25	33	8
12	33	25	16	2	18	10	35	4	13	27	11	19	31
13	21	13	4	27	6	35	23	29	1	15	36	7	19
14	11	3	31	17	33	25	13	19	28	5	26	34	9
15	3	32	23	9	25	17	5	11	20	34	18	26	1
16	34	26	17	3	19	11	36	5	14	28	12	20	32
17	30	22	13	36	15	7	32	1	10	24	8	16	28
18	28	20	11	34	13	5	30	36	8	22	6	14	26

У кожному стовпці для $4\sigma_i$ таблиці 3.17 для значень q_{yi} рівно $l = 9$ разів ($p = 4 \cdot 9 + 1$) зустрічається нелишок. Це в точності відповідає зауваженню 3.10.

Розрахуємо значення функції N_q і частоти n_q нелишків $q \in \mathbb{Z}_{37}$ як значень функції $q = y^2 - 4\sigma$. Для цього, враховуючи наслідок 3.9, складемо таблицю 3.18 для можливих значень y , $1 \leq y \leq 18$, за всіма квадратичними нелишками $q \in \{2; 5; 6; 8; 13; 14; 15; 17; 18; 19; 20; 22; 23; 24; 29; 31; 32; 35\} \subset \mathbb{Z}_{37}$ та примітивними елементами $\sigma_i \in \{2; 32; 17; 13; 15; 18; 35; 5; 20; 24; 22; 19\} \subset \mathbb{Z}_{37}$.

Таблиця 3.18. Значення y

σ_i	2	32	17	13	15	18	35	5	20	24	22	19	
$q \backslash 4\sigma_i$	8	17	31	15	23	35	29	20	6	22	14	2	n_q
2	11		12		5						4	2	5
5			3		18	15	16	5	14	8		9	8
6				13		2		10	7	18			5
8	4	5						18		17		11	5
13	13	17	9	18	6	14		12			8		8
14						7		16		6	18	4	5
1			3	17	1		9		13				5
17	5	16	14		15		3						5
18	10		7	12	2	4	11	1		15			8
19	8	6		16			14		5	2	12	13	8
20	18						7	15	10		16		5
22	17		4						18	9	6		5
23		15		1	3	13						5	5
24		2			11		4	9	17	3	1	10	8
29		3		9		8	13	7					5
31		14	5	3						4		12	5
32	15	7	10	11		17			1		3	16	8
35					13	12	8		2		7		5

Кожен з 18 квадратичних нелішків $q \in \mathbb{Z}_{37}$ є розв'язком системи (3.17), який за заданого параметра $k \in \mathbb{Z}_{37}$ визначає відповідне значення параметра $b = \frac{q - k^2}{4}$. Отже, для $p = 37$ значення $N_q = 18$.

Потужність сімейства матричних полів $|\{F_{b,k}\}| = 18 \cdot 37$. Це відповідає рівності $|\{F_{b,k}\}| = \frac{p-1}{2} \cdot p$, що свідчить про досяжність верхньої оцінки (3.19).

У матричному полі $F_{b,k}$ існує рівно κ_q примітивних елементів виду

$$A(k) = \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}. \text{ У відповідності до оцінки (3.20) кратність } \kappa_q \leq \varphi(38) = 18.$$

Згідно з формулою (3.21) у прикладі 7 маємо:

1) для $q \in \{2; 6; 8; 14; 15; 17; 20; 22; 23; 29; 31; 35\}$ таких матриць рівно $2 \cdot 5 = 10$;

2) для $q \in \{5; 13; 18; 19; 24; 32\}$ таких матриць рівно $2 \cdot 8 = 16$.

Зокрема, для $q = 2$ поле $F_{b,k}$ з параметром $b = \frac{2-k^2}{4}$ має десять

примітивних елементів $A_y(k) = \begin{pmatrix} \frac{y-k}{2} & 1 \\ \frac{2-k^2}{4} & \frac{y+k}{2} \end{pmatrix}$, $y \in \{\pm 11; \pm 12; \pm 5; \pm 4; \pm 2\}$, а

саме $A_{11}(k) = \begin{pmatrix} \frac{\pm 11-k}{2} & 1 \\ \frac{2-k^2}{4} & \frac{\pm 11+k}{2} \end{pmatrix}$, $A_{12}(k) = \begin{pmatrix} \frac{\pm 12-k}{2} & 1 \\ \frac{2-k^2}{4} & \frac{\pm 12+k}{2} \end{pmatrix}$,

$A_5(k) = \begin{pmatrix} \frac{\pm 5-k}{2} & 1 \\ \frac{2-k^2}{4} & \frac{\pm 5+k}{2} \end{pmatrix}$, $A_4(k) = \begin{pmatrix} \frac{\pm 4-k}{2} & 1 \\ \frac{2-k^2}{4} & \frac{\pm 4+k}{2} \end{pmatrix}$,

$A_2(k) = \begin{pmatrix} \frac{\pm 2-k}{2} & 1 \\ \frac{2-k^2}{4} & \frac{\pm 2+k}{2} \end{pmatrix}$.

3.4.2. Загальний випадок методу вибору параметрів b і k матричного поля $F_{b,k}$ і примітивного елементу в ньому

Для довільного випадку, коли просте p не є числом Мерсенна

$(p = 2^m - 1)$ або $3 \leq \frac{p+1}{2} = \rho$ не є простим числом, метод вибору параметрів b

і k матричного поля $F_{b,k}$ і примітивного елементу в ньому полягає в наступному:

- 1) для визначеного простого значення p довільним чином обрати у \mathbb{Z}_p квадратичні нелишки q і r , причому $\frac{r}{4}$ є примітивним елементом у \mathbb{Z}_p , а $q+r \in \{QR\} \setminus 0$;
- 2) обрати довільним чином значення $k \in \mathbb{Z}_p$;
- 3) обчислити $b = \frac{q-k^2}{4} \in \mathbb{Z}_p$;
- 4) з виразу $(2a+k)^2 = q+r$ знайти значення $a \in \mathbb{Z}_p$;
- 5) перевірити $\text{period}(A) = p+1$.

Зазначимо, що наведений метод не гарантує досягнення максимального порядку породженої матрицею A циклічної підгрупи, проте значно звужує множину пошуку параметрів матриці.

Для перевірки умови $\text{period}(A) = p+1$ необхідно розкласти на прості множники число $p+1$ та для $a=0,1,\dots,p-1$ перевірити нерівність $A^{\frac{p+1}{n}}(a) \neq s \cdot E$ для всіх простих n -дільників $p+1$, де $s \in \mathbb{Z}_p$, E – одинична матриця (див. твердження 2.1).

Для цього випадку **алгоритм** вибору параметрів b і k поля $F_{b,k}$ і примітивного елемента в ньому наведено на рисунку 3.2.

1. Set prime p , $k \in \mathbb{Z}_p$
2. Factorize $p-1$, find $\frac{r}{4}$ as a primitive root in \mathbb{Z}_p , find quadratic non-residue q in \mathbb{Z}_p : $q+r$ is a non-zero quadratic residue in \mathbb{Z}_p
3. $b \leftarrow \frac{q-k^2}{4}$
4. Find $a \in \mathbb{Z}_p$: $(2a+k)^2 = q+r$
5. Factorize $p+1$
6. **for** $a=0$ to $p-1$

```

7.       $check \leftarrow success$ 
8.      for  $n \in \{(p+1) \text{ dividers}\}$ 
9.          if  $A^{\frac{p+1}{n}}(a) = s \cdot E$  then
10.               $check \leftarrow fail$ 
11.          end if
12.      end for
13.      if  $check = success$  then
14.           $A \leftarrow \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ 
15.          break
16.      end if
17. end for

```

Рисунок 3.2. Алгоритм вибору параметрів b і k поля $F_{b,k}$ та пошуку примітивного елементу в ньому для довільного p

Використовуючи наведені вище оцінки складності операцій у полі, прогнозований порядок часу виконання алгоритму на рисунку 3.2 дорівнює

$$L_p \left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}} \right] + O(\log^2 p) + O(\log p) + O(\log p) + O(\log p) = L_p \left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}} \right].$$

Приклад 8.

Прийmemo спочатку $p = 4l + 1$.

Нехай $p = 17$.

Для $p = 17$ ненульовими квадратичними лишками є: $\{QR\} \setminus 0 = \{1; 2; 4; 8; 9; 13; 15; 16\}$. Відповідно, квадратичними нелишками є: $\{QNR\} = \{3; 5; 6; 7; 10; 11; 12; 14\}$.

Тоді $q \in \{3; 5; 6; 7; 10; 11; 12; 14\}$.

Примітивними елементами \mathbb{Z}_{17} з $\{QNR\}$ є: $\{3; 5; 6; 7; 10; 11; 12; 14\}$. Тоді $r \in \{3; 5; 6; 7; 10; 11; 12; 14\}$.

У таблиці 3.19 наведено відомості про кількість наборів параметрів матриці A : $q, r \in \{3; 5; 6; 7; 10; 11; 12; 14\}$, $k \in \mathbb{Z}_{17}$, і $a \in \mathbb{Z}_{17} : (2a + k)^2 = q + r$ – для досягнення максимального порядку $\text{ord}(A) = p^2 - 1$. Відомості згруповано для пар $\{q, r\}$, випадки $q + r \in \{QR\} \setminus 0$ виділено сірим.

Таблиця 3.19. Кількість наборів параметрів матриці A для досягнення максимального порядку $\text{ord}(A) = 17^2 - 1$

$q \backslash r$	3	5	6	7	10	11	12	14
3	-	0	34	-	34	-	34	-
5	34	-	-	-	34	34	-	0
6	34	-	-	34	0	-	34	-
7	-	-	0	-	-	34	34	34
10	34	34	34	-	-	0	-	-
11	-	34	-	0	34	-	-	34
12	0	-	34	34	-	-	-	34
14	-	34	-	34	-	34	0	-

Наявність нулів у таблиці 3.19 для деяких пар $\{q; r\}$ свідчить про те, що для цих пар матриця A не може бути породжувальним елементом мультиплікативної циклічної групи максимального періоду $p^2 - 1$. Це обумовлено тим, що розроблений метод враховує базовий випадок (3.9) $\Delta_a = a(a + k) - b \neq t^2 \in \mathbb{Z}_p$, проте не охоплює загальну умову (див. формулу (3.8)).

Зауважимо, що згідно з теоремою Ферма [74] $t^{p-1} \in \{0; 1\}$, а $GCF(p-2, p-1) = GCF(p-2, 1) = 1$. Тому для $p \geq 5$ співвідношення (3.8) записуються як $\Delta_a \neq t^j \in \mathbb{Z}_p$, $2 \leq j \leq p-3$, $GCF(j, p-1) \neq 1$.

Так, наприклад, для $q = 7$, $r = 6$, $k = 0$ значення $\Delta_a = a(a + k) - b = 4(4 + 0) - 6 = 10$. Разом з тим, $10 \equiv 3^3 \pmod{17}$, звідки $A^{\frac{18}{3}} = 3 \cdot E$, а $A^{18} = (A^6)^3 = 10 \cdot E$.

Цей приклад є підтвердженням необхідності, проте не достатності умови (3.9) для досягнення максимального порядку матриці A . Разом з тим, як зазначено вище, наведений метод значно звужує множину пошуку параметрів матриці порівняно з їх повним перебором.

Потужність множини можливих значень параметрів матриці $A = \begin{pmatrix} a & 1 \\ b & a + k \end{pmatrix}$ в \mathbb{Z}_{17} становить 32 пари $\{q; r\}$, у той час, коли повний перебір параметрів $a, b, k \in \mathbb{Z}_{17}$ вимагає аналізу $17^3 = 4913$ комбінацій. Імовірність же вибору потрібної матриці A в \mathbb{Z}_{17} за запропонованим методом дорівнює $\frac{24}{32} = 0.75$ проти $\frac{816}{4913} \approx 0.166$ для повного перебору.

Розглянемо тепер приклади, коли $p = 4l + 3$.

Нехай $p = 11$.

Ненульовими квадратичними лишками є: $\{1; 3; 4; 5; 9\}$. Відповідно, квадратичними нелишками є: $\{2; 6; 7; 8; 10\}$.

Тоді $q \in \{2; 6; 7; 8; 10\}$.

Примітивними елементами \mathbb{Z}_{11} з $\{QNR\}$ є: $\{2; 6; 7; 8\}$. Відтак, $r \in \{2; 6; 8; 10\}$.

У таблиці 3.20 наведено відомості про кількість наборів параметрів матриці A : $q \in \{2; 6; 7; 8; 10\}$, $r \in \{2; 6; 8; 10\}$, $k \in \mathbb{Z}_{11}$, і $a \in \mathbb{Z}_{11} : (2a + k)^2 = q + r$ для досягнення максимального порядку $\text{ord}(A) = 11^2 - 1$. Відомості згруповано для пар $\{q, r\}$, випадки $q + r \in \{QR\} \setminus 0$ виділено сірим.

Таблиця 3.20. Кількість наборів параметрів матриці A для досягнення
максимального порядку $\text{ord}(A) = 11^2 - 1$

$q \backslash r$	2	6	8	10
2	22	-	-	22
6	-	22	22	0
7	22	-	0	-
8	-	0	22	-
10	0	22	-	22

Потужність множини можливих значень параметрів матриці A в \mathbb{Z}_{11} становить 12 пар $\{q; r\}$, у той час, коли повний перебір параметрів $a, b, k \in \mathbb{Z}_{11}$ вимагає аналізу $11^3 = 1331$ комбінацій. Імовірність же вибору потрібної матриці A в \mathbb{Z}_{11} за запропонованим методом дорівнює $\frac{8}{12} \approx 0.667$ проти $\frac{176}{1331} \approx 0.132$ для повного перебору.

Нехай тепер $p = 19$.

Ненульовими квадратичними лишками є: $\{1; 4; 5; 6; 7; 9; 11; 16; 17\}$.

Відповідно, квадратичними нелишками є: $\{2; 3; 8; 10; 12; 13; 14; 15; 18\}$.

Тоді $q \in \{2; 3; 8; 10; 12; 13; 14; 15; 18\}$.

Примітивними елементами \mathbb{Z}_{19} з $\{QNR\}$ є: $\{2; 3; 10; 13; 14; 15\}$. Відтак, $r \in \{2; 3; 8; 12; 14; 18\}$.

У таблиці 3.21 наведено відомості про кількість наборів параметрів матриці A : $q \in \{2; 3; 8; 10; 12; 13; 14; 15; 18\}$, $r \in \{2; 3; 8; 12; 14; 18\}$, $k \in \mathbb{Z}_{19}$, і $a \in \mathbb{Z}_{19} : (2a + k)^2 = q + r$ — для досягнення максимального порядку $\text{ord}(A) = 19^2 - 1$. Відомості згруповано для пар $\{q, r\}$, випадки $q + r \in \{QR\} \setminus 0$ виділено сірим.

Таблиця 3.21. Кількість наборів параметрів матриці A для досягнення
максимального порядку $\text{ord}(A) = 19^2 - 1$

$q \backslash r$	2	3	8	12	14	18
2	38	38	-	-	38	38
3	38	38	38	-	38	-
8	-	0	38	38	-	38
10	-	-	-	-	38	0
12	-	-	38	38	0	38
13	-	38	-	0	-	-
14	38	38	-	38	38	-
15	38	-	0	-	-	-
18	0	-	38	38	-	38

Потужність множини можливих значень параметрів матриці A в \mathbb{Z}_{19} становить 30 пар $\{q; r\}$, у той час, коли для повний перебір параметрів $a, b, k \in \mathbb{Z}_{19}$ вимагає аналізу $19^3 = 6859$ комбінацій. Імовірність же вибору потрібної матриці A в \mathbb{Z}_{19} за запропонованим методом дорівнює $\frac{24}{30} = 0.8$ проти $\frac{912}{6859} \approx 0.133$ для повного перебору.

Зауваження 3.13. Розглянутий в 3.2 алгоритм вибору параметрів поля $F_{b,k}$ і примітивного елементу в ньому не гарантують досягнення максимального порядку циклічної підгрупи, породженої матрицею A як спеціальним випадком примітивного елементу виду $t \cdot A = t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}$ для $t=1$. Разом з тим, усі $\varphi(p^2-1)$ примітивні елементи поля $F_{b,k}$ над \mathbb{Z}_p для заданих його параметрів визначаються виразом (3.1). З урахуванням наведених вище алгоритмів **модифікація методу** вибору параметрів b і k поля $F_{b,k}$ для **довільного** t , а також вибору примітивного елементу в ньому полягає в наступному:

- 1) для визначеного простого значення p довільним чином обрати у \mathbb{Z}_p квадратичний нелишок q ;
- 2) обрати довільним чином значення $k \in \mathbb{Z}_p$;
- 3) обчислити $b = \frac{q - k^2}{4} \in \mathbb{Z}_p$;
- 4) знайти $a \in \mathbb{Z}_p$, для якого $\text{period}(A(a)) = p + 1$;
- 5) знайти $t \in \mathbb{Z}_p \setminus 0$, для якого $t^2 \frac{r}{4}$ є примітивним елементом у \mathbb{Z}_p ;
- 6) матриця $t \cdot A = t \cdot \begin{pmatrix} a & 1 \\ b & a + k \end{pmatrix}$ є примітивним елементом поля $F_{b,k}$ (див. твердження 2.4).

Зауважимо, що для знаходження значення t в пункті 5 представленого методу необхідно виконати наступну процедуру. Оскільки визначник $\det(A) = \frac{r}{4}$ є квадратичним нелишком, для $t = 1, 2, \dots, p-1$ значення $\det(tA) = t^2 \frac{r}{4}$ утворюють усю множину нелишків \mathbb{Z}_p . Тому для того, щоб $t^2 \frac{r}{4}$ був примітивним елементом у \mathbb{Z}_p , потрібно розкласти число $p-1$ на прості множники та для послідовних значень $t = 1, 2, \dots, p-1$ перевірити нерівності $\left(t^2 \frac{r}{4}\right)^{\frac{p-1}{m}} \not\equiv 1 \pmod{p}$ для всіх простих m -ділників $p-1$, доки не буде визначено примітивний елемент $t^2 \frac{r}{4}$ в \mathbb{Z}_p .

У цьому випадку **алгоритм** вибору параметрів b і k поля $F_{b,k}$ і примітивного елемента в ньому має наступний вид.

1. Set prime p , $k \in \mathbb{Z}_p$
2. Find quadratic non-residue q in \mathbb{Z}_p

```

3.   $b \leftarrow \frac{q - k^2}{4}$ 
4.  Factorize  $p + 1$ 
5.  for  $a = 0$  to  $p - 1$ 
6.       $check \leftarrow success$ 
7.      for  $n \in \{(p + 1) \text{ dividers}\}$ 
8.          if  $A^{\frac{p+1}{n}}(a) = s \cdot E$  then
9.               $check \leftarrow fail$ 
10.         end if
11.     end for
12.     if  $check = success$  then
13.         break
14.     end if
15. end for
16. Factorize  $p - 1$ 
17. for  $t = 1$  to  $p - 1$ 
18.      $check \leftarrow success$ 
19.     for  $m \in \{(p - 1) \text{ dividers}\}$ 
20.         if  $\left(t^2 \frac{r}{4}\right)^{\frac{p-1}{m}} = 1 \pmod{p}$  then
21.              $check \leftarrow fail$ 
22.         end if
23.     end for
24.     if  $check = success$  then
25.         break
26.     end if
27. end for
28.  $A \leftarrow t \cdot \begin{pmatrix} a & 1 \\ b & a + k \end{pmatrix}$ 

```

Рисунок 3.3. Алгоритм вибору параметрів b і k поля $F_{b,k}$ і примітивного елементу в ньому для довільного значення t

Прогнозований порядок часу виконання алгоритму на рисунку 3.3 для великих p визначається часом факторизації чисел $p+1$ і $p-1$ і дорівнює

$$\begin{aligned} & O(\log p) + O(\log p) + L_p \left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}} \right] + O(\log^2 p) + L_p \left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}} \right] + O(\log^2 p) = \\ & = L_p \left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}} \right]. \end{aligned}$$

3.5. Порівняльний аналіз методів вибору примітивних елементів

Отримані результати цього розділу підтверджують ефективність запропонованого методу вибору параметрів скінченних полів матриць порядку 2. Основною перевагою є можливість одночасного визначення як параметрів поля, так і його примітивних елементів. Це суттєво спрощує процес побудови криптографічно стійких систем, що базуються на використанні скінченних полів.

Принципові відмінності отриманих результатів цього розділу від результатів розділу 2:

- підхід до формування поля $F_{b,k}$, висвітлений у розділі 2, розроблено для ситуації, коли параметри b і k є відомими, причому $D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p$. Цей розділ розглядає випадок, коли b і k попередньо не задані;
- розділ 2 дозволяє знайти примітивні елементи виду $t_{ji} \cdot A_j$. Цей же розділ позбавляє необхідності вибору відповідних коефіцієнтів $t_{ji} \in \mathbb{Z}_p$ і дозволяє відразу вказувати примітивні елементи виду $A(k)$, тобто для $t = 1$. Разом з тим, зважаючи на те, що наведений для $t = 1$ і довільного p алгоритм не гарантує досягнення максимального порядку породженої матрицею A циклічної підгрупи, зауваження 3.13 поширює отримані підходи на випадок довільних p і t ;

- цей розділ знаходить параметри сімейства скінченних полів матриць і множину їх примітивних елементів одночасно (як залежність від одного параметру k).

Таким чином, на відміну від підходу, викладеного в розділі 2, де необхідно попередньо визначити параметри поля $F_{b,k}$ та окремо шукати його примітивні елементи, розроблений метод дозволяє уникнути цього кроку. Такий підхід формує можливість зменшення обчислювальних витрат і підвищення швидкодії алгоритмів. Зокрема, процес знаходження примітивних елементів спрощується завдяки використанню символу Лежандра замість розв'язання квадратних рівнянь у полі. Зважаючи на це, запропонований метод демонструє високу ефективність навіть для великих значень параметрів b і k . Це важливо для сучасних криптографічних протоколів, де великі розміри полів є необхідною умовою забезпечення стійкості до атак.

Підвищення складності виконання дискретного логарифмування для циклічних груп у полях \mathbb{Z}_p і $F_{b,k}$ обумовлено наступним. У полі \mathbb{Z}_p одними з найшвидших алгоритмів дискретного логарифмування є алгоритм COS [85] і решето числового поля [86]. Складність алгоритму COS дорівнює $L_p\left[\frac{1}{2}, 1\right]$, решета числового поля – $L_p\left[\frac{1}{3}, 1.902\right]$. Циклічна ж група поля $F_{b,k}$ із є особливою групою матриць і має порядок $p^2 - 1$. У такому випадку для оцінювання складності дискретного логарифмування можна скористатися відомими алгоритмами для довільного скінченного поля. Зокрема, для поля $F_{b,k}$ алгоритм обчислення індексів [87] і алгоритм Ель Гамалія [88] дають складність $L_p\left[\frac{1}{2}, c\right]$. Разом з тим, алгоритм обчислення порядку є ефективним, якщо значення p є невеликим, а алгоритм Ель Гамалія застосовується для поля $GF(p^2)$ та може бути використаний у цій роботі, проте не для полів матриць

вищих порядків $GF(q)$, де $q = p^m$, $m > 2$. Тоді складність алгоритму дискретного логарифмування можна оцінити тільки як $O(\sqrt{q})$ [89].

Важливим аспектом є також аналіз кількості можливих параметрів, що задовольняють умові максимального порядку циклічної підгрупи. Отримані аналітичні оцінки показують, що потужність сімейства таких полів є достатньо великою, що забезпечує широкий вибір для побудови криптосистем із різними характеристиками.

3.6. Висновки до розділу 3

У третьому розділі розроблено метод вибору параметрів скінченного поля квадратних матриць порядку 2 над простим скінченним полем \mathbb{Z}_p і примітивного елемента в цьому матричному полі для довільного простого p , який за рахунок детального дослідження й використання властивостей суми квадратичних лишків і нелишків у \mathbb{Z}_p дозволяє перейти від окремого розв'язання завдання вибору поля та завдання пошуку примітивного елемента в цьому полі до їх узгодженого алгоритмічного розв'язання в межах єдиної процедури. Метод дозволяє суттєво звузити множину пошуку допустимих параметрів поля й забезпечує можливість знаходження примітивного елемента без повного перебору всіх елементів матричного поля.

Так, наприклад, для $p = 11$ імовірність вибору потрібної примітивної матриці за запропонованим методом дорівнює 0,667 проти 0,132 для повного перебору. Для $p = 17$ ці ймовірності складають 0,75 і 0,166, а для $p = 19$ – 0,8 і 0,133.

Окремо досліджено важливий випадок простих p , які є числами Мерсенна або для яких $3 \leq \frac{p+1}{2} = \rho$ також є простими числами. Показано, що

такі значення p зручні для побудови матричних полів $F_{b,k}$, а потужність сімейства скінченних матричних полів за цих умов не менша за $\left\lceil \frac{p}{4} \right\rceil \cdot p$.

Удосконалено метод вибору параметрів скінченного поля квадратних матриць порядку 2 над простим скінченим полем \mathbb{Z}_p і примітивного елементу в цьому матричному полі для випадку, коли p є числом Мерсенна або $(p+1)/2$ є простим числом, який за рахунок обчислення символу Лежандра замість процедури розв'язання квадратного рівняння в \mathbb{Z}_p дає змогу точно знаходити параметричне сімейство примітивних елементів поля.

У розділі особливу увагу приділено алгоритмам реалізації запропонованих методів. Для спеціального випадку, коли p є числом Мерсенна або $(p+1)/2$ є простим числом, побудовано алгоритм, у якому основні обчислювальні кроки зводяться до знаходження первісного кореня, перевірки квадратичної нелишковості за символом Лежандра, розв'язання допоміжного рівняння та обчислення параметрів матриці. Для загального випадку побудовано алгоритмічну процедуру, що включає факторизацію чисел $p-1$ та p^2-1 , перевірку умов максимального порядку циклічної підгрупи та примітивності визначника, внаслідок чого забезпечується конструктивний вибір параметрів поля і примітивного елемента в ньому.

Отримані оцінки складності підтверджують, що визначальним чинником часу виконання є факторизація відповідних чисел, а самі алгоритми придатні до використання в задачах комп'ютерної інженерії, пов'язаних із математичним моделюванням обчислювальних процесів, програмною реалізацією криптографічних перетворень і захистом інформації в комп'ютерних системах і мережах.

Проведений порівняльний аналіз показав, що запропоновані методи мають принципові переваги порівняно з підходом розділу 2, оскільки орієнтовані на випадок, коли параметри матричного поля наперед не задані, та

забезпечують одночасний вибір параметрів поля і примітивного елемента в ньому. Це спрощує побудову сімейства скінченних матричних полів порядку 2, розширює можливості їх застосування в криптографічних протоколах і створює підґрунтя для подальшої розробки ефективних програмно-алгоритмічних засобів.

Запропонований підхід до побудови сімейства скінченних полів квадратних матриць порядку 2 над \mathbb{Z}_p і множини їх примітивних елементів є універсальним і може бути застосований у різних криптографічних протоколах, зокрема для узгодження ключів і побудови стійких шифрів.

Основні результати досліджень цього розділу опубліковано в [49], [90].

РОЗДІЛ 4. КРИПТОГРАФІЧНІ ПРОТОКОЛИ В СКІНЧЕННИХ ПОЛЯХ КВАДРАТНИХ МАТРИЦЬ ДРУГОГО ПОРЯДКУ

4.1. Вступ

У четвертому розділі розглянуто можливість підвищення криптографічної стійкості класичних протоколів обміну ключами Діффі-Хеллмана [1] та електронного цифрового підпису Ель-Гамала [2] шляхом застосування операцій у скінченному полі квадратних матриць. Такий підхід дає змогу збільшити порядок циклічної мультиплікативної групи до $p^2 - 1$ замість $p - 1$, що ускладнює процедуру обчислення дискретного логарифма.

4.2. Протокол узгодження ключів

Протокол узгодження ключів Діффі-Хеллмана [1] для двох учасників – Аліси і Боба – полягає в наступному:

- 1) генерація власних ключів:
 - a. обрати примітивний елемент α у \mathbb{Z}_p ;
 - b. обрати випадкові $k_A, k_B \in (0; p - 1)$;
 - c. обчислити відкриті ключі $Y_A = \alpha^{k_A} \bmod p$, $Y_B = \alpha^{k_B} \bmod p$;
- 2) узгодження спільного ключа:
 - a. Аліса обчислює $Z_{AB} = Y_B^{x_A}$;
 - b. Боб обчислює $Z_{BA} = Y_A^{x_B}$;
 - c. $Z = Z_{AB} = Z_{BA}$.

У випадку використання поля

$$F_{b,k} = \left\{ t \cdot \begin{pmatrix} a & 1 \\ b & a+k \end{pmatrix}, s \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p, t, s, a, b, k \in \mathbb{Z}_p \right\} \text{ схема узгодження ключів}$$

Діффі-Хеллмана буде полягати в наступному:

- 1) генерація власних ключів:

- a. обрати примітивний елемент – матрицю α у $F_{b,k}$;
- b. обрати випадкові $k_A, k_B \in (0; p-1)$;
- c. обчислити відкриті ключі $Y_A = \alpha^{k_A} \bmod p$, $Y_B = \alpha^{k_B} \bmod p$;

2) узгодження спільного ключа:

- a. Аліса обчислює $Z_{AB} = Y_B^{x_A}$;
- b. Боб обчислює $Z_{BA} = Y_A^{x_B}$;
- c. $Z = Z_{AB} = Z_{BA}$.

4.3. Приклад реалізації протоколу узгодження ключів

Для прикладу приймемо параметри $b=9$, $k=3$, $p=13$. Примітивним елементом поля $F_{9,3}$ над \mathbb{Z}_{13} оберемо матрицю $\alpha = \begin{pmatrix} 11 & 1 \\ 9 & 1 \end{pmatrix}$.

Нехай Аліса обрала закритим ключем значення $k_A=17$, а Боб – значення $k_B=111$. Тоді Аліса обчислює $Y_A = \alpha^{k_A} = \begin{pmatrix} 11 & 1 \\ 9 & 1 \end{pmatrix}^{17} = \begin{pmatrix} 8 & 11 \\ 8 & 2 \end{pmatrix}$, а Боб – $Y_B = \alpha^{k_B} = \begin{pmatrix} 11 & 1 \\ 9 & 1 \end{pmatrix}^{111} = \begin{pmatrix} 11 & 2 \\ 5 & 4 \end{pmatrix}$. Значення Y_A та Y_B поміщують у відкритий довідник.

Аліса формує спільний ключ $Z_{AB} = Y_B^{k_A} = \begin{pmatrix} 11 & 2 \\ 5 & 4 \end{pmatrix}^{17} = \begin{pmatrix} 1 & 1 \\ 9 & 4 \end{pmatrix}$. У свою чергу, Боб обраховує $Z_{BA} = Y_A^{k_B} = \begin{pmatrix} 8 & 11 \\ 8 & 2 \end{pmatrix}^{111} = \begin{pmatrix} 1 & 1 \\ 9 & 4 \end{pmatrix}$. Процедуру узгодження ключа завершено: $Z = Z_{AB} = Z_{BA}$.

4.4. Протокол електронного цифрового підпису

Поля $F_{b,k}$ можуть бути представлені в вигляді:

$$F_{b,k} = \left\{ \begin{pmatrix} x_1 & x_2 \\ bx_2 & x_1 + kx_2 \end{pmatrix}, x_1, x_2, b, k \in \mathbb{Z}_p, D = k^2 + 4b \neq u^2 \in \mathbb{Z}_p \right\}, \quad (4.1)$$

де b і k – фіксовані параметри поля, обрані таким чином, щоб значення $D = k^2 + 4b$ було квадратичним нелишком у \mathbb{Z}_p .

Параметри x_1 і x_2 можуть приймати довільні значення в \mathbb{Z}_p , утворюючи p^2 різних пар. Тому порядок поля $\text{ord}(F_{b,k}) = p^2$.

Розглянемо схему формування ЕЦП Ель-Гамала за рахунок виконання операцій у скінченному полі матриць замість простого поля лишків \mathbb{Z}_p .

Відповідно до [2], оригінальна схема ЕЦП полягає в наступному (рисунок 4.1):

3) генерація ключів:

- a. обрати примітивний елемент α у \mathbb{Z}_p ;
- b. обрати випадкове $x \in (0; p-1)$;
- c. обчислити відкритий ключ $y = \alpha^x \bmod p$;

4) створення підпису:

- a. обчислити хеш-функцію $m = H(M)$ від повідомлення M ;
- b. обрати випадкове $h \in (0; p-1)$, причому $\gcd(h, p-1) = 1$;
- c. обчислити $r = \alpha^h \bmod p$;
- d. обчислити $s = (m - x \cdot r) \cdot h^{-1} \bmod (p-1)$;
- e. підписом є пара чисел $\{r; s\}$;

5) перевірка підпису:

- a. обчислити хеш-функцію $m = H(M)$;
- b. обчислити $v_1 = \alpha^m \bmod p$;
- c. обчислити $v_2 = y^r \cdot r^s \bmod p$;
- d. якщо $v_1 = v_2$, підпис вважається вірним.

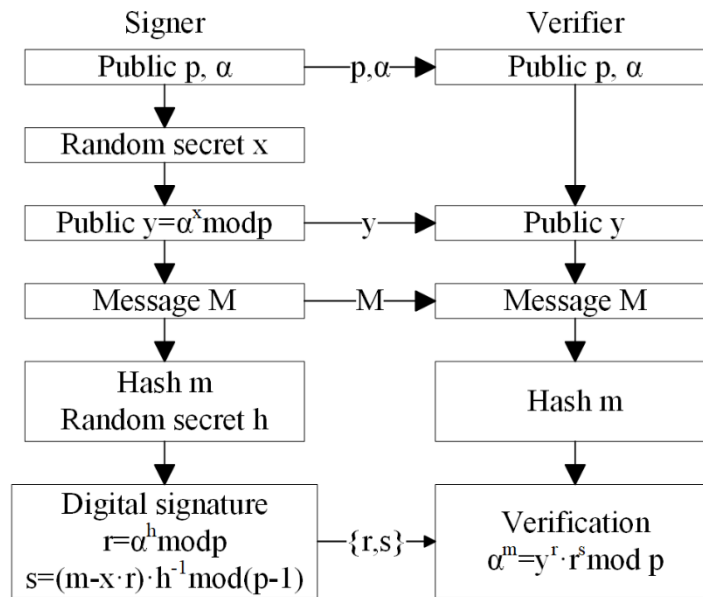


Рисунок 4.1. Схема формування ЕЦП Ель-Гамалія

У випадку використання поля $F_{b,k}$ схема ЕЦП Ель-Гамалія буде полягати в наступному:

1) генерація ключів:

- а. обрати примітивний елемент Σ у $F_{b,k}$. Помістити у відкритий довідник параметри поля b і k , а також матрицю Σ . Зауважимо, що відповідно до (4.1) будь-яку матрицю поля $F_{b,k}$ визначає її верхній рядок з елементів x_1 і x_2 . Тому замість матриці Σ у відкритий довідник можуть бути поміщені значення x_1 і x_2 , що однозначно її визначають;
- б. обрати випадкове $x \in (0; p^2 - 1)$;
- с. обчислити відкритий ключ $Y = \Sigma^x \in F_{b,k}^*$;

2) створення підпису:

- а. обчислити хеш-функцію $m = H(M)$ від повідомлення M ,
 $m \in (0; p^2 - 1)$;
- б. обрати випадкове $h \in (0; p^2 - 1)$, причому $\gcd(h, p^2 - 1) = 1$;

с. обчислити $R = \Sigma^h \in F_{b,k}^*$. Поклавши $R = \begin{pmatrix} x_1 & x_2 \\ bx_2 & x_1 + kx_2 \end{pmatrix}$

відповідно до (4.1), обчислення p -адичного числа $r = x_2 \cdot p + x_1$ за відомих b і k утворює бієкцію між матрицею R і числом r ;

d. обчислити $s = (m - x \cdot r) \cdot h^{-1} \bmod (p^2 - 1)$. Зауважимо, що оскільки $\gcd(h, p^2 - 1) = 1$, то існує обернений елемент h^{-1} : $h \cdot h^{-1} = 1 \bmod (p^2 - 1)$;

e. підписом є пара чисел $\{r; s\}$ (альтернативними еквівалентними формами підпису можуть бути набори $\{R; s\}$, $\{x_1; x_2; s\}$);

3) перевірка підпису:

a. обчислити хеш-функцію $m = H(M)$;

b. обчислити $\Upsilon_1 = \Sigma^m \in F_{b,k}^*$;

c. на основі відомого значення p -адичного числа r з підпису $\{r; s\}$ сформувати матрицю R ;

d. обчислити $\Upsilon_2 = Y^r \cdot R^s \in F_{b,k}^*$;

e. якщо $\Upsilon_1 = \Upsilon_2$, підпис вважається вірним.

Коректність: $\Upsilon_1 = \Sigma^m = Y^r \cdot R^s = \Sigma^{x \cdot r} \cdot \Sigma^{h \cdot s} = \Sigma^{x \cdot r + h \cdot (m - x \cdot r) \cdot h^{-1}} = \Sigma^m$.

4.5. Приклад реалізації ЕЦП

Розглянемо приклад реалізації ЕЦП для $p = 7057$. Нехай $b = 3934$, $k = 1$. Значення $D = k^2 + 4b = 15737$. Внаслідок закону квадратичної взаємності [72], значення символу Лежандра $\left(\frac{D}{p}\right) = -1$. Отже, $D = 15737$ є квадратичним

нелишком у \mathbb{Z}_{7057} , а $F_{3934,1}$ є матричним полем. Тоді

$$F_{3934,1} = \left\{ \begin{pmatrix} x_1 & x_2 \\ 3934x_2 & x_1 + x_2 \end{pmatrix}, x_1, x_2 \in \mathbb{Z}_p \right\}. \text{ Порядок поля } \text{ord}(F_{b,k}) = 49801249.$$

Відповідно до наведеної вище схеми виконаємо:

1) генерацію ключів:

а. оберемо примітивний елемент $\Sigma = \begin{pmatrix} 1 & 1 \\ 3934 & 2 \end{pmatrix}$. Його розрахунок

можна виконувати, наприклад, за методикою, наведеною в

розділі 2. При цьому важливо, що число $\rho = \frac{p+1}{2} = 3529$ є

простим, а елемент $\det(\Sigma)$ є примітивним елементом у \mathbb{Z}_{7057} .

Помістимо параметри $b = 3934$, $k = 1$, а також матрицю

$\Sigma = \begin{pmatrix} 1 & 1 \\ 3934 & 2 \end{pmatrix}$ у відкритий довідник (у відкритий довідник

замість цієї матриці Σ можуть бути поміщені $x_1 = 1$ і $x_2 = 1$);

б. оберемо випадкове $x \in (0; p^2 - 1)$. Нехай $x = 73$;

с. обчислимо відкритий ключ

$$Y = \Sigma^x = \begin{pmatrix} 1 & 1 \\ 3934 & 2 \end{pmatrix}^{73} = \begin{pmatrix} 1 & 1 \\ 3934 & 2 \end{pmatrix}^{64+8+1} = \begin{pmatrix} 2139 & 5571 \\ 4329 & 653 \end{pmatrix};$$

2) створення підпису:

а. нехай хеш-функція від повідомлення M дорівнює $m = 1868$;

б. оберемо випадкове $h \in (0; p^2 - 1)$, причому $\gcd(h, p^2 - 1) = 1$.

Нехай $h = 613$;

с. обчислимо

$$R = \Sigma^h = \begin{pmatrix} 1 & 1 \\ 3934 & 2 \end{pmatrix}^{613} = \begin{pmatrix} 1 & 1 \\ 3934 & 2 \end{pmatrix}^{512+64+32+4+1} = \begin{pmatrix} 4778 & 6854 \\ 5896 & 4575 \end{pmatrix}.$$

Обчислимо $r = x_2 \cdot p + x_1 = 6854 \cdot 7057 + 4778 = 48373456$;

д. обчислимо

$$s = (m - x \cdot r) \cdot h^{-1} \bmod (p^2 - 1) = \\ = (1868 - 73 \cdot 48373456) \cdot 23885101 \bmod 49801248 = 11218924;$$

е. підписом є пара чисел $\{r; s\} = \{48373456; 11218924\}$;

3) перевірка підпису:

а. нехай обчислена хеш-функція $m = 1868$;

б. обчислимо

$$\Upsilon_1 = \Sigma^m = \begin{pmatrix} 1 & 1 \\ 3934 & 2 \end{pmatrix}^{1868} = \begin{pmatrix} 1 & 1 \\ 3934 & 2 \end{pmatrix}^{1024+512+256+64+8+4} = \begin{pmatrix} 4888 & 27 \\ 363 & 4915 \end{pmatrix}$$

;

с. на основі відомого $r = 6854 \cdot 7057 + 4778$ сформуємо матрицю

$$R = \begin{pmatrix} 4778 & 6854 \\ 5896 & 4575 \end{pmatrix};$$

д. обчислимо

$$\begin{aligned} \Upsilon_2 = Y^r \cdot R^s &= \begin{pmatrix} 2139 & 5571 \\ 4329 & 653 \end{pmatrix}^{48373456} \cdot \begin{pmatrix} 4778 & 6854 \\ 5896 & 4575 \end{pmatrix}^{11218924} = \\ &= \begin{pmatrix} 2139 & 5571 \\ 4329 & 653 \end{pmatrix}^{2^{25}+2^{23}+2^{22}+2^{21}+2^{17}+2^{12}+2^{11}+2^{10}+2^9+2^7+2^6+2^4} \times \\ &\times \begin{pmatrix} 4778 & 6854 \\ 5896 & 4575 \end{pmatrix}^{2^{23}+2^{21}+2^{19}+2^{17}+2^{16}+2^{13}+2^{11}+2^{10}+2^9+2^8+2^7+2^6+2^5+2^3+2^2} = \\ &= \begin{pmatrix} 2861 & 5698 \\ 2900 & 1502 \end{pmatrix} \cdot \begin{pmatrix} 1690 & 5114 \\ 6026 & 6804 \end{pmatrix} = \begin{pmatrix} 4888 & 27 \\ 363 & 4915 \end{pmatrix}; \end{aligned}$$

е. рівність $\Upsilon_1 = \Upsilon_2$ виконується, отже підпис вважається вірним.

4.6. Статистичні властивості піднесення матриці до степеня

Класична схема ЕЦП Ель-Гамала [2], як і схема узгодження криптографічними ключами Діффі-Хеллмана [1], базуються на складності обчислення дискретного логарифму.

Оскільки відображення $y = \alpha^x$ у \mathbb{Z}_p для примітивного елемента α є повною перестановкою, воно не “спотворює” ймовірностей. З точки зору теорії чисел, це пояснюється тим, що порядок $\text{ord}(\alpha) = p - 1$. Відповідно, піднесення до степеня α поводить як випадкова перестановка, коли x обирається випадково (і навпаки, якщо x випадкове, то й $x = \log_\alpha y$ випадкове) [83], [91]. Операція піднесення до степеня $y = \alpha^x \bmod p$ має дифузійну природу: невелика зміна вхідних даних (експоненти x) може значно вплинути на вихідний результат y [92].

Звертаючись до класичних праць теорії криптографії [93], [94], два загальноприйнятих принципи розробки практичних шифрів – це принципи конфузії та дифузії, запропоновані Шенноном. [95].

Конфузія: «статистика шифротексту повинна залежати від статистики відкритого тексту таким чином, щоб бути занадто складним для використання криптоаналітиком».

Дифузія: «кожен символ відкритого тексту та кожен символ секретного ключа повинні впливати на багато символів шифротексту». [94].

Засобом для перевірки виконання принципів конфузії та дифузії можуть слугувати статистичні критерії оцінювання випадковості послідовностей чисел, зокрема [96], [97], [98], [99], [100]. У цьому розділі розглянемо статистичні властивості значень функції піднесення матриці до степеня $Y = \Sigma^x$ у полі $F_{b,k}$ над \mathbb{Z}_p та порівняємо її з властивостями функції $y = \alpha^x$ у полі \mathbb{Z}_q . Для забезпечення максимальної близькості порядків досліджуваних мультиплікативних груп значення q оберемо максимально близьким простим числом, не меншим за p^2 . Перевірку будемо виконувати за допомогою тесту NIST STS [97].

Для цього використаємо наступні параметри:

- 1) для функції $Y = \Sigma^x$ у $F_{b,k}$ над \mathbb{Z}_p : $p = 7057$; $b = 999$; $k = 391$;

2) для функції $y = \alpha^x$ у $\mathbb{Z}_q : q = 49801259 = 7057^2 + 10$.

Оскільки найменшим первісним коренем у $\mathbb{Z}_{49801259}$ є $\sigma_0 = 2$, примітивні елементи поля $\mathbb{Z}_{49801259}$ можуть бути обрані з множини $\{2^i : \gcd(i, 49801259) = 1\}$.

Визначимо примітивні елементи поля $F_{b,k}$ над \mathbb{Z}_{7057} .

Згідно з [46], існує рівно $\varphi(7058) = 3528$ різних матриць $A_j = \begin{pmatrix} a_j & 1 \\ 999 & a_j + 391 \end{pmatrix}$ з періодом $\text{period}(A_j) = p + 1 = 7058$ і $\det(A_j) \neq u^2 \in \mathbb{Z}_{7057}$, що визначають усі $\varphi(p^2 - 1) = 14224896 = 2^9 \cdot 3^4 \cdot 7^3$ примітивних елементів поля $F_{b,k}$ над \mathbb{Z}_{7057} . Оскільки найменшим первісним коренем у \mathbb{Z}_{7057} є $\sigma_0 = 5$, примітивними елементами поля $F_{b,k}$ є матриці $t_{ji} \cdot A_j$, де $t_{ji} \in \left\{ \pm 5^{\frac{i-\gamma_j}{2}} : \gcd(i, 7056) = 1, \gamma_j = \text{ind}(\det(A_j)) \right\}$, $1 \leq j \leq 3528$.

Значення $\det(A_j)$ не є квадратичним лишком, наприклад, для $a_j = 1$. Тоді для $a_j = 1$ примітивні елементи $t_{ji} \cdot A_j$ поля $F_{999,391}$ визначають матриці $A_1 = \begin{pmatrix} 1 & 1 \\ 999 & 392 \end{pmatrix}$ і $A_{6665} = \begin{pmatrix} 6665 & 1 \\ 999 & 7056 \end{pmatrix}$. Значення $\det(A_1) = \det(A_{6665}) = 6450$ і $\gamma_1 = \text{ind}(6450) = 4537$ обумовлюють можливі t_{ji} .

Тест NIST STS [97] оперує бітовим потоком, тому значення елементів утворених мультиплікативних груп перетворено в двійковий вигляд. Для цього результат функції $y = \sigma^x$ у \mathbb{Z}_q приводився до діапазону $[0; 255]$ та перетворювався в байт. Оскільки елементи поля $F_{b,k}$ над \mathbb{Z}_p (4.1) визначаються значеннями x_1 і x_2 , матриця мультиплікативної групи перетворювалася в двійкову послідовність шляхом утворення p -адичного числа $x_2 \cdot p + x_1$, приведення його до діапазону $[0; 255]$ та перетворення в байт.

Для всіх тестів NIST STS [97] прийнято наступні параметри: the significance level: 0,01, кількість тестованих послідовностей: 100; кількість тестів: 188.

Графіки результатів частоти проходження тестів для функцій $y = \alpha^x$ у $\mathbb{Z}_{49801259}$ і $Y = \Sigma^x$ у $F_{999,391}$ над \mathbb{Z}_{7057} наведено на рисунку 4.2 і рисунку 4.3.

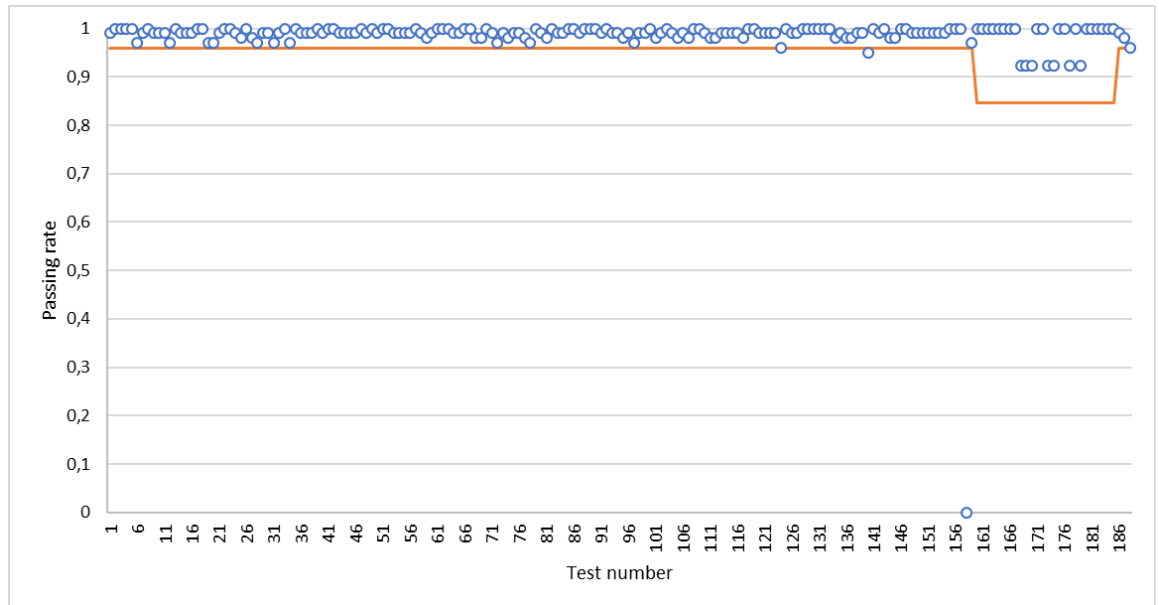


Рисунок 4.2. Частота проходження тестів NIST STS послідовністю

$$y = \alpha^x \bmod 49801259$$

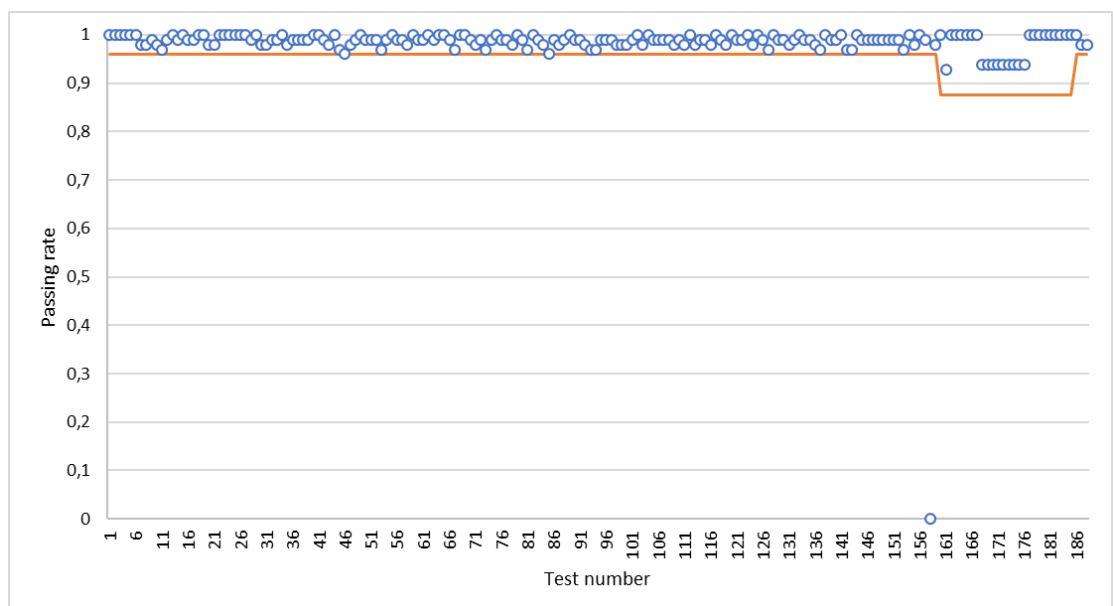


Рисунок 4.3. Частота проходження тестів NIST STS послідовністю

$$Y = \Sigma^x \in F_{999,391} \text{ над } \mathbb{Z}_{7057}$$

Обидві послідовності зі 100-відсотковою ймовірністю не пройшли Maurer's "Universal Statistical" Test [101]. Середня частота проходження тестів для проведених 50 експериментів з урахуванням перевірки Uniform Distribution of P-values становить 98,89% для перетворень у матричному полі $F_{999,391}$ над \mathbb{Z}_{7057} та 98,83% для перетворень у полі $\mathbb{Z}_{49801259}$.

Таким чином, отримані результати не виявляють відмінностей у статистичних портретах протестованих послідовностей. Це, зокрема, дозволяє застосовувати перетворення в матричному полі $F_{b,k}$ замість перетворень у полі \mathbb{Z}_p у схемі узгодження ключів і ЕЦП Ель-Гамалія.

4.7. Імітаційні програмні моделі протоколу узгодження ключів і протоколу електронного цифрового підпису

Для перевірки працездатності запропонованих криптографічних схем доцільно розробити їх імітаційні програмні моделі. Такі моделі дають змогу відтворити основні етапи функціонування протоколу узгодження ключів Діффі-Хеллмана та протоколу електронного цифрового підпису Ель-Гамалія у скінченному полі квадратних матриць другого порядку, а також перевірити коректність виконання операцій піднесення матриці до степеня, множення матриць, побудови відкритих і закритих ключів, формування спільного ключа та створення і перевірки підпису.

Імітаційна модель будується як програмна реалізація арифметики поля, елементи якого подаються квадратними матрицями другого порядку над полем лишків \mathbb{Z}_p . Кожна матриця поля однозначно визначається елементами верхнього рядка x_1 і x_2 та параметрами b і k , що задають структуру поля. Це

дозволяє реалізувати компактне програмне подання елементів поля та виконувати всі необхідні алгебраїчні операції засобами мови Python.

Основу імітаційної моделі становлять такі програмні компоненти:

- модуль арифметики матричного поля, що реалізує множення матриць, піднесення до степеня, знаходження оберненого елемента та перетворення матриці в p -адичне число;
- модуль протоколу узгодження ключів, який імітує дії двох сторін – Аліси та Боба – під час формування відкритих ключів і спільного секрету;
- модуль протоколу електронного цифрового підпису, який реалізує генерацію ключів, створення підпису для повідомлення та його перевірку;
- модуль тестування, призначений для автоматичної перевірки коректності реалізації на контрольних прикладах.

У додатку А наведено приклад такої імітаційної реалізації мовою Python. Програму побудовано так, щоб вона відтворювала модель для перевірки математичної коректності запропонованих схем.

У наведеному лістингу реалізовано базовий клас `MatrixFieldElement`, який описує елемент поля матриць через пару елементів x_1 і x_2 . Така реалізація є зручною для імітаційної моделі, оскільки дає змогу одночасно працювати і з алгебраїчним поданням елемента, і з його матричним представленням. Додатково реалізовано p -адичне кодування, яке використовується в схемі ЕЦП для переходу від матриці до числа.

Наведена програма відтворює повну послідовність дій протоколу узгодження ключів. Спочатку кожен учасник обирає закритий ключ, після чого обчислює відкритий ключ як степінь примітивного елемента матричного поля. Далі кожна сторона формує спільний ключ шляхом піднесення отриманого відкритого ключа іншої сторони до власного секретного степеня.

Якщо реалізацію виконано правильно, результати Аліси та Боба збігаються, що підтверджує коректність моделі.

Реалізовано імітаційну модель матричного варіанта ЕЦП Ель-Гамала. Для кожного повідомлення обчислюється хеш-значення, після чого генерується випадкове число, взаємно просте з порядком мультиплікативної групи. Далі обчислюється матриця $R = \Sigma^h \in F_{b,k}^*$, яка переводиться в p -адичне число r , і формується друга компонента підпису s . Під час перевірки виконується відновлення матриці R з числа r , після чого перевіряється рівність $Y^r \cdot R^s = \Sigma^m$. Саме виконання цієї рівності підтверджує справжність підпису.

Застосування окремого тестового модуля дає змогу перевірити три критично важливі властивості моделі: збіг спільного ключа для обох сторін у протоколі Діффі-Хеллмана, успішну перевірку коректно сформованого підпису та відхилення підпису в разі зміни повідомлення. Таким чином, імітаційна програма може використовуватися як інструмент експериментального підтвердження правильності запропонованих криптографічних схем.

Таким чином, розроблення імітаційних програмних моделей запропонованих протоколу узгодження ключів та протоколу електронного цифрового підпису дало змогу практично реалізувати математичний апарат операцій у скінченному полі квадратних матриць другого порядку. Запропонована реалізація мовою Python забезпечує відтворення всіх основних етапів роботи протоколів: генерації ключів, формування відкритих параметрів, узгодження спільного ключа, створення електронного цифрового підпису та його перевірки. Це підтверджує, що описані в розділі теоретичні описи можуть бути безпосередньо перенесені в програмне середовище для подальших досліджень, тестування та аналізу обчислювальної складності.

4.8. Обчислювальна складність протоколів у матричному полі та порівняння з класичним випадком

Практична доцільність використання скінченного поля квадратних матриць другого порядку в протоколах Діффі-Хеллмана та ЕЦП Ель-Гамала визначається не лише зростанням порядку мультиплікативної групи, а й співвідношенням між досягнутим підвищенням криптографічної стійкості та додатковими обчислювальними витратами. У класичному випадку операції виконуються в полі лишків \mathbb{Z}_p , де порядок мультиплікативної групи дорівнює $p-1$. У запропонованому підході операції виконуються в полі $F_{b,k}$, реалізованому у вигляді скінченного поля квадратних матриць другого порядку над \mathbb{Z}_p , тому порядок відповідної мультиплікативної групи дорівнює p^2-1 . Отже, за фіксованого p порядок групи збільшується у $p+1$ разів, що безпосередньо розширює простір можливих значень степеня та ускладнює задачу дискретного логарифмування.

З алгоритмічної точки зору структура протоколів у класичному та матричному випадках залишається однаковою. У схемі узгодження ключів Діффі-Хеллмана кожен учасник один раз обчислює власний відкритий ключ і один раз – спільний секретний ключ, тобто виконує дві операції піднесення до степеня. Аналогічно, у схемі Ель-Гамала виконуються ті самі базові етапи: під час генерації ключів – одне піднесення до степеня, під час формування підпису – одне піднесення до степеня та обчислення оберненого елемента, під час перевірки – дві операції піднесення до степеня. Таким чином, перехід від \mathbb{Z}_p до $F_{b,k}$ не змінює алгоритмічної структури протоколів, а змінює лише вартість однієї групової операції.

Для обох варіантів домінують операції дискретне піднесення до степеня. Якщо використовувати стандартний алгоритм двійкового піднесення до степеня, то кількість групових множень має порядок $O(\log x)$, де x – показник степеня. Тому асимптотично і в класичному полі \mathbb{Z}_p , і в полі

матриць другого порядку складність піднесення до степеня є логарифмічною за довжиною експоненти. Відмінність полягає в тому, що в класичному випадку одна групова операція зводиться до множення двох елементів поля \mathbb{Z}_p , тоді як у матричному випадку одна групова операція є множенням двох матриць поля $F_{b,k}$, тобто потребує виконання сталої кількості арифметичних операцій у базовому полі \mathbb{Z}_p . Отже, асимптотична залежність від довжини експоненти не змінюється, але константа при оцінці часу виконання зростає.

Унаслідок цього для протоколу Діффі-Хеллмана можна стверджувати, що в класичному випадку обчислювальна складність однієї сторони визначається двома операціями піднесення до степеня в \mathbb{Z}_p , тоді як у матричному випадку – двома операціями піднесення матриці до степеня в $F_{b,k}$. З позицій асимптотики обидві оцінки мають однаковий логарифмічний характер, проте матричний варіант потребує більшої кількості модульних множень і додавань на кожному кроці. Разом з тим, така надбавка компенсується тим, що обчислення виконуються в групі більшого порядку $p^2 - 1$, а отже, за однакового базового модуля p досягається підвищення складності криптоаналізу без зміни самої структури протоколу.

Аналогічний висновок справедливий і для ЕЦП Ель-Гамала. Кількість основних обчислювальних кроків у матричній схемі збігається з класичною: формування відкритого ключа потребує одного піднесення до степеня, формування підпису – одного піднесення до степеня, обчислення оберненого елемента та кількох арифметичних операцій, перевірка – двох піднесення до степеня і одного множення. Додаткові витрати в матричному варіанті пов'язані з тим, що замість звичайного множення елементів \mathbb{Z}_p виконуються операції над матрицями, а також із необхідністю перетворення матриці в p -адичне число та у зворотному напрямі під час подання підпису. Проте ці перетворення мають допоміжний характер і не змінюють домінуючого внеску операції дискретного піднесення до степеня.

Порівняння з класичним випадком показує, що запропонований підхід має таке співвідношення переваг і витрат. Його перевагою є збільшення порядку мультиплікативної групи з $p-1$ до p^2-1 , тобто приблизно у $p+1$ разів, що ускладнює розв'язання задачі дискретного логарифмування і тим самим підвищує криптографічну стійкість схем. Недоліком є збільшення вартості однієї групової операції, оскільки матричне множення є обчислювально важчим за множення двох скалярних елементів поля \mathbb{Z}_p . Отже, запропонований підхід не зменшує асимптотичну складність протоколів, але змінює їхню практичну продуктивність за рахунок збільшення сталої при часових оцінках. Саме тому використання матричного поля є доцільним у тих застосуваннях, де критичним є підвищення стійкості до атак на дискретний логарифм, а додаткове обчислювальне навантаження є прийнятним.

З огляду на наведене, можна зробити висновок, що перехід від класичних протоколів над \mathbb{Z}_p до їх реалізації в скінченному полі квадратних матриць другого порядку не змінює логіку побудови алгоритмів і не потребує зміни послідовності криптографічних кроків, однак призводить до переходу до більшої за порядком циклічної групи. Це забезпечує вигравш у криптографічній стійкості при збереженні загальної алгоритмічної структури протоколів Діффі-Хеллмана та Ель-Гамала, що підтверджує перспективність застосування матричних полів у задачах захисту інформації в комп'ютерних системах і мережах.

Для наочнішого порівняння класичного випадку реалізації протоколів у полі \mathbb{Z}_p та запропонованого підходу з використанням скінченного поля квадратних матриць другого порядку доцільно зіставити їх за основними обчислювальними характеристиками. Результати такого порівняння наведено в таблиці 4.1.

Таблиця 4.1. Порівняльна характеристика підходів

Операція / характеристика	Класичний випадок \mathbb{Z}_p	Матричний випадок $F_{b,k}$ у вигляді поля квадратних матриць 2-го порядку	Коментар
Носій криптографічних операцій	Просте поле \mathbb{Z}_p	Скінченне поле порядку p^2 , реалізоване через квадратні матриці 2-го порядку над \mathbb{Z}_p	У матричному випадку зберігається структура поля, але елементами є матриці.
Порядок мультиплікативної групи	$p-1$	p^2-1	Перехід до матричного поля збільшує порядок групи приблизно у $p+1$ разів, що ускладнює задачу дискретного логарифмування.
Базова групова операція	Множення елементів поля \mathbb{Z}_p	Множення матриць поля $F_{b,k}$	У матричному випадку одна групова операція є обчислювально важчою, оскільки виконується через кілька арифметичних операцій у базовому полі.
Домінуюча операція в протоколах	Піднесення елемента до степеня	Піднесення матриці до степеня	У обох випадках саме операція дискретного піднесення до степеня визначає основну частину обчислювальних витрат.
Асимптотика піднесення до степеня	$O(\log x)$ групових множень при двійковому алгоритмі	$O(\log x)$ групових множень при двійковому алгоритмі	Асимптотика за довжиною експоненти не змінюється; змінюється лише вартість одного множення.
Генерація відкритого ключа в Діффі-Хеллмана	Одне піднесення до степеня	Одне піднесення до степеня	Структура алгоритму та сама, але в матричному випадку відкритий ключ є матрицею.
Формування спільного ключа в Діффі-Хеллмана	Одне піднесення до степеня	Одне піднесення до степеня	Кожен учасник, як і в класичному випадку, виконує дві операції піднесення до степеня загалом.
Генерація відкритого ключа в Ель-Гамала	Одне піднесення до степеня	Одне піднесення матриці до степеня	Алгоритмічна структура не змінюється.

Операція / характеристика	Класичний випадок \mathbb{Z}_p	Матричний випадок $F_{b,k}$ у вигляді поля квадратних матриць 2-го порядку	Коментар
Формування підпису в Ель-Гамалі	Одне піднесення до степеня, обчислення оберненого елемента, кілька арифметичних операцій	Одне піднесення матриці до степеня, обчислення оберненого елемента, додаткове подання матриці через p -адичне число	Додаткові витрати матричного випадку пов'язані не лише з матричним множенням, а й з перетворенням подання матриці.
Перевірка підпису в Ель-Гамалі	Два піднесення до степеня і одне множення	Два піднесення матриць до степеня і одна матрична операція	Верифікація також зберігає класичну послідовність дій, але кожна групова операція дорожча.
Складність підготовки параметрів	Вибір примітивного елемента в \mathbb{Z}_p	Вибір параметрів поля (a,b) і примітивного елемента за алгоритмами розділу 3	У матричному випадку підготовчий етап складніший, але він виконується одноразово під час побудови системи.
Визначальний чинник часової складності підготовки параметрів	Факторизація $p-1$ та пошук генератора	Факторизація $p-1$ і p^2-1 , перевірка максимального порядку та примітивності визначника	Прогнозований час визначається факторизацією відповідних чисел.
Криптографічна перевага	Стандартний порядок групи	Більший порядок групи й ширший простір параметрів	Це дає підстави очікувати підвищення стійкості до атак на дискретний логарифм.
Обчислювальний недолік	Менша вартість однієї операції	Більша константа часу для однієї групової операції	Отже, виграш у стійкості досягається ціною збільшення практичного часу обчислень.
Загальний висновок	Менше обчислювальне навантаження, менший порядок групи	Та сама алгоритмічна схема, але більший порядок групи й вища вартість операцій	Матричний підхід доцільний тоді, коли пріоритетом є підвищення криптографічної стійкості за збереження класичної логіки протоколів.

Як видно з таблиці 4.1, застосування матричного поля не змінює загальної алгоритмічної структури протоколів Діффі-Хеллмана та ЕЦП Ель-Гамала, однак збільшує порядок мультиплікативної групи з $p-1$ до p^2-1 . Це підвищує криптографічну стійкість схем, хоча й супроводжується збільшенням вартості однієї групової операції та ускладненням етапу підготовки параметрів.

4.9. Висновки до розділу 4

Проведене дослідження підтвердило, що перенесення протоколів Діффі-Хеллмана та ЕЦП Ель-Гамала зі звичайного простого поля \mathbb{Z}_p до скінченного поля квадратних матриць другого порядку $F_{b,q}$ є практично змістовним підходом. Його основна прикладна перевага полягає в тому, що без зміни базового підходу класичних криптографічних схем вдається перейти до мультиплікативної групи більшого порядку. Це означає розширення простору допустимих параметрів і, як наслідок, підвищення стійкості до атак, що ґрунтуються на розв'язанні задачі дискретного логарифмування.

З практичної точки зору особливо важливим є те, що запропонований підхід не потребує побудови принципово нової криптосистеми. Натомість він дає змогу модифікувати вже відомі та добре досліджені механізми узгодження ключів і цифрового підпису, зберігаючи їхню алгоритмічну структуру. Це спрощує використання такого підходу в прикладних програмних й апаратних рішеннях, де вже використовуються схеми Діффі-Хеллмана та Ель-Гамала, але існує потреба в підвищенні криптографічної стійкості.

Наведені в четвертому розділі схеми та приклади обчислень показали, що всі ключові процедури – генерація відкритих параметрів, побудова спільного ключа, формування підпису та його перевірка – можуть бути реалізовані в матричному полі коректно й послідовно. Це свідчить про

придатність запропонованого підходу до практичної реалізації в засобах захисту інформації.

Окреме практичне значення має встановлений факт, що перехід до матричного поля не погіршує статистичних властивостей результатів піднесення до степеня. Отримані результати тестування свідчать, що з позицій випадковості, конфузії та дифузії матричне перетворення не поступається класичному випадку.

Водночас дослідження показало, що виграш у стійкості досягається ціною збільшення обчислювальних витрат на одну групову операцію. У практичному сенсі це означає, що матричний підхід є найбільш доцільним не для всіх без винятку систем, а насамперед для тих застосувань, де пріоритетом є саме підвищена стійкість, а помірне зростання часу обчислень є допустимим. До таких застосувань можна віднести системи обміну ключами в критичній інфраструктурі, спеціалізовані захищені мережі, засоби довготривалого захисту даних, а також сервіси електронного підпису, в яких вимоги до надійності переважають над вимогами до максимальної швидкодії.

Розроблені імітаційні програмні моделі запропонованих схем узгодження ключів та електронного цифрового підпису дали змогу практично реалізувати математичний апарат операцій у скінченному полі квадратних матриць другого порядку. Запропонована реалізація мовою Python забезпечує відтворення всіх основних етапів роботи криптографічних схем: генерації ключів, формування відкритих параметрів, узгодження спільного ключа, створення електронного цифрового підпису та його перевірки. Це підтверджує, що описані в розділі теоретичні описи можуть бути безпосередньо перенесені в програмне середовище.

Основні результати досліджень цього розділу опубліковано в [50].

ВИСНОВКИ

Дисертація вирішує актуальну науково-технічне завдання підвищення криптографічної стійкості засобів захисту інформації в комп'ютерних системах і мережах за рахунок використання скінченних полів квадратних матриць другого порядку та їх примітивних елементів, що забезпечують розширення порядку мультиплікативної групи, придатної для реалізації криптографічних протоколів узгодження ключів і електронного цифрового підпису.

Найбільш значущими результатами дисертації є наступні.

1. Розроблено метод вибору примітивних елементів скінченних полів матриць другого порядку, який за рахунок послідовної перевірки дискримінанта характеристичного рівняння, максимального періоду матриці в квадратичному розширенні та примітивності її визначника в базовому полі дає змогу конструктивно формувати множину примітивних елементів поля без повного перебору всіх його елементів.

Встановлено умови, за яких матриця другого порядку є генератором мультиплікативної групи скінченного поля матриць. Показано, що матриці, для яких дискримінант характеристичного рівняння є квадратичним лишком у полі \mathbb{Z}_p , не можуть забезпечувати максимальний порядок у полі матриць, тоді як у випадку нерозкладного характеристичного многочлена примітивність матриці зводиться до одночасного виконання двох умов: досягнення максимального періоду $p+1$ та примітивності її визначника в базовому полі \mathbb{Z}_p . Одержано еквівалентні критерії перевірки цих умов через степені матриці, значення сліду степенів матриці та перевірку показників, пов'язаних із простими дільниками числа $p+1$.

Розроблено методику вибору примітивних елементів скінченних полів матриць другого порядку, орієнтовану на практичну й програмну реалізацію. Методика охоплює формування множини матриць-кандидатів, обчислення їх сліду, визначника та дискримінанта, перевірку умови максимального періоду,

визначення порядку визначника та побудову примітивних елементів за допомогою скалярних коефіцієнтів із базового поля. Встановлено співвідношення, які дозволяють контролювати повноту сформованої множини примітивних елементів і уникати дублювання результатів під час обчислень.

Розроблений метод і методика дають змогу формувати всі примітивні елементи скінченного поля матриць другого порядку для їх подальшого використання в криптографічних алгоритмах комп'ютерних систем і мереж. Використання поля матриць порядку 2 над \mathbb{Z}_p забезпечує збільшення порядку мультиплікативної групи з $p-1$ до p^2-1 порівняно з базовим полем, що створює передумови для розширення можливостей криптографічних перетворень і потенційного підвищення їх криптографічної стійкості.

2. Розроблено метод вибору параметрів скінченного поля квадратних матриць порядку 2 над скінченим полем \mathbb{Z}_p і примітивного елементу в цьому матричному полі для довільного простого p , який за рахунок детального дослідження й використання властивостей суми квадратичних лишків і нелишків у \mathbb{Z}_p дозволяє перейти від окремого розв'язання завдання вибору поля та завдання пошуку примітивного елементу в цьому полі до їх узгодженого алгоритмічного розв'язання в межах єдиної процедури. Метод дозволяє суттєво звужити множину пошуку допустимих параметрів поля й забезпечує можливість знаходження примітивного елементу без повного перебору всіх елементів матричного поля.

Так, наприклад, для $p=11$ імовірність вибору потрібної примітивної матриці за запропонованим методом дорівнює 0,667 проти 0,132 для повного перебору. Для $p=17$ ці ймовірності складають 0,75 і 0,166, а для $p=19$ – 0,8 і 0,133.

3. Удосконалено метод вибору параметрів скінченного поля квадратних матриць порядку 2 над скінченим полем \mathbb{Z}_p і примітивного елементу в цьому матричному полі для випадку, коли p є числом Мерсенна або $(p+1)/2 \in$

простим числом, який за рахунок обчислення символу Лежандра замість процедури розв'язання квадратного рівняння в \mathbb{Z}_p дає змогу точно знаходити параметричне сімейство примітивних елементів поля.

Для спеціального випадку, коли p є числом Мерсенна або $(p+1)/2$ є простим числом, побудовано алгоритм реалізації запропонованого методу, в якому основні обчислювальні кроки зводяться до знаходження первісного кореня, перевірки квадратичної нелишковості за символом Лежандра, розв'язання допоміжного рівняння та обчислення параметрів матриці. Для загального випадку побудовано алгоритмічну процедуру, що включає факторизацію чисел $p-1$ та p^2-1 , перевірку умов максимального порядку циклічної підгрупи та примітивності визначника, внаслідок чого забезпечується конструктивний вибір параметрів поля і примітивного елемента в ньому.

Отримані оцінки складності підтверджують, що визначальним чинником часу виконання є факторизація відповідних чисел, а самі алгоритми придатні до використання в задачах комп'ютерної інженерії, пов'язаних із математичним моделюванням обчислювальних процесів, програмною реалізацією криптографічних перетворень і захистом інформації в комп'ютерних системах і мережах.

Запропонований підхід до побудови сімейства скінченних полів квадратних матриць порядку 2 над \mathbb{Z}_p і множини їх примітивних елементів є універсальним і може бути застосований у різних криптографічних протоколах, зокрема для узгодження ключів і побудови стійких шифрів.

4. Практична цінність проведеного дослідження полягає в тому, що використання скінченного поля квадратних матриць другого порядку дає змогу посилити класичні протоколи Діффі–Хеллмана та Ель-Гамала без зміни їх базової алгоритмічної структури. Перехід до матричного поля забезпечує збільшення порядку мультиплікативної групи з $p-1$ до p^2-1 , а отже,

ускладнює атаки на основі задачі дискретного логарифмування. Наведені схеми та приклади підтвердили коректність реалізації узгодження ключів і цифрового підпису в матричному полі. Результати статистичного тестування показали, що такі перетворення зберігають належні властивості випадковості, конфузії та дифузії. Отже, запропонований підхід є доцільним для застосувань, де пріоритетом є підвищення криптографічної стійкості за умови допустимого зростання обчислювальних витрат.

СПИСОК ДЖЕРЕЛ

- [1] W. Diffie і M. Hellman, «New directions in cryptography», *IEEE Trans. Inform. Theory*, т. 22, вип. 6, С. 644—654, листоп. 1976, doi: 10.1109/TIT.1976.1055638.
- [2] T. Elgamal, «A public key cryptosystem and a signature scheme based on discrete logarithms», *IEEE Transactions on Information Theory*, т. 31, вип. 4, С. 469—472, лип. 1985, doi: 10.1109/TIT.1985.1057074.
- [3] N. Koblitz, «Elliptic curve cryptosystems», *Math. Comp.*, т. 48, вип. 177, С. 203—209, 1987, doi: 10.1090/S0025-5718-1987-0866109-5.
- [4] V. S. Miller, «Use of Elliptic Curves in Cryptography», у *Advances in Cryptology — CRYPTO '85 Proceedings*, т. 218, Н. С. Williams, Ред., у Lecture Notes in Computer Science, vol. 218. , Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, С. 417—426. doi: 10.1007/3-540-39799-X_31.
- [5] «Advanced Encryption Standard (AES)». U.S. Department of Commerce, 2001. 26 листоп. Дата звернення: 2025. 26 квіт. [URL]. Доступний у: <https://nvlpubs.nist.gov>
- [6] R. Lidl і H. Niederreiter, *Finite fields*, 2е вид. у Encyclopedia of mathematics and its applications, no. 20. Cambridge: Cambridge University Press, 1997.
- [7] G. L. Mullen, *Handbook of finite fields*. у Discrete mathematics and its applications. Boca Raton London New York: CRC Press, 2013.
- [8] H. W. Lenstra і R. J. Schoof, «Primitive normal bases for finite fields», *Math. Comp.*, т. 48, вип. 177, С. 217—231, 1987, doi: 10.1090/S0025-5718-1987-0866111-3.
- [9] T. Hansen і G. L. Mullen, «Primitive polynomials over finite fields», *Math. Comp.*, т. 59, вип. 200, С. 639—643, 1992, doi: 10.1090/S0025-5718-1992-1134730-7.
- [10] X. Cao і P. Wang, «Primitive elements with prescribed trace», *AAECC*, т. 25, вип. 5, С. 339—345, листоп. 2014, doi: 10.1007/s00200-014-0228-1.

- [11] S. D. Cohen, «Primitive elements and polynomials with arbitrary trace», *Discrete Mathematics*, т. 83, вип. 1, С. 1—7, лип. 1990, doi: 10.1016/0012-365X(90)90215-4.
- [12] S. Fan i W. Han, «Primitive polynomial with three coefficients prescribed», *Finite Fields and Their Applications*, т. 10, вип. 4, С. 506—521, жовт. 2004, doi: 10.1016/j.ffa.2003.10.003.
- [13] F. Shuqin i H. Wenbao, «Primitive Polynomials over Finite Fields of Characteristic Two», *Applicable Algebra in Engineering, Communication and Computing*, т. 14, вип. 5, С. 381—395, січ. 2004, doi: 10.1007/s00200-003-0140-6.
- [14] S. Gao i S. A. Vanstone, «On orders of optimal normal basis generators», *Math. Comp.*, т. 64, вип. 211, С. 1227—1233, 1995, doi: 10.1090/S0025-5718-1995-1297469-6.
- [15] S. Gao, J. Von Zur Gathen, i D. Panario, «Gauss periods: orders and cryptographical applications», *Math. Comp.*, т. 67, вип. 221, С. 343—352, 1998, doi: 10.1090/S0025-5718-98-00935-1.
- [16] D. Jungnickel i S. A. Vanstone, «On primitive polynomials over finite fields», *Journal of Algebra*, т. 124, вип. 2, С. 337—353, серп. 1989, doi: 10.1016/0021-8693(89)90136-1.
- [17] D. Bigatti i L. Susskind, «Review of matrix theory», *Strings, Branes and Dualities*, С. 277—318, 1999.
- [18] A. Hock, «Matrix field theory», 2020. [URL]. Доступний у: <https://doi.org/10.48550/arXiv.2005.07525>
- [19] D. Serre i D. Serre, *What are matrices*. Springer, New York, 2010.
- [20] W. P. Wardlaw, «Matrix representation of finite fields», *Mathematics Magazine*, т. 67, вип. 4, С. 289—293, 1994, doi: 10.1080/0025570X.1994.11996233.
- [21] L. Brickman, «On the field of values of a matrix», *Proceedings of the American Mathematical Society*, т. 12, вип. 1, С. 61—66, 1961, doi: 10.2307/2034125.
- [22] R. Bellman, *Introduction to matrix analysis*. SIAM, 1997.

- [23] R. J. McEliece, «A public-key cryptosystem based on algebraic», *Coding Thv*, т. 4244, вып. 1978, С. 114—116, 1978.
- [24] R. J. McEliece, *Finite fields for computer scientists and engineers*, т. 23. Springer Science & Business Media, 2012.
- [25] M. K. Singh, «Public key cryptography with matrices», y *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004.*, IEEE, 2004, С. 146—152. doi: 10.1109/IAW.2004.1437810.
- [26] A. Stakhov, «Fibonacci matrices, a generalization of the “Cassini formula”, and a new coding theory», *Chaos, Solitons & Fractals*, т. 30, вып. 1, С. 56—66, 2006, doi: 10.1016/j.chaos.2005.12.054.
- [27] A. Stakhov, «The “golden” matrices and a new kind of cryptography», *Chaos, Solitons & Fractals*, т. 32, вып. 3, С. 1138—1146, 2007, doi: 10.1016/j.chaos.2006.03.069.
- [28] A. Naseri, A. Abbasi, i R. Atani, «A new public key cryptography using Mq matrix», *Journal of Mathematical Modeling*, т. 11, вып. 4, С. 681—693, 2023, doi: 10.22124/jmm.2023.23982.2142.
- [29] M. Durcheva i K. Danilchenko, «Secure Key Exchange in Tropical Cryptography: Leveraging Efficiency with Advanced Block Matrix Protocols», *Mathematics*, т. 12, вып. 10, С. 1429, 2024, doi: 10.3390/math12101429.
- [30] M. Maxrizal, «Public Key Cryptosystem Based on Singular Matrix», *Trends in Sciences*, т. 19, вып. 3, С. 2147, 2022, doi: 10.48048/tis.2022.2147.
- [31] M. Abu-Faraj, A. Al-Hyari, i Z. Alqadi, «A complex matrix private key to enhance the security level of image cryptography», *Symmetry*, т. 14, вып. 4, С. 664, 2022, doi: 10.3390/sym14040664.
- [32] F. Al-Shaarani i A. Gutub, «Securing matrix counting-based secret-sharing involving crypto steganography», *Journal of King Saud University - Computer and Information Sciences*. King Saud bin Abdulaziz University, 2021. . doi: 10.1016/j.jksuci.2021.09.009.

- [33] T. Kumar i S. Chauhan, «Image cryptography with matrix array symmetric key using chaos based approach», *International Journal of Computer Network and Information Security*, т. 13, вип. 3, С. 60, 2018, doi: 10.5815/ijcnis.2018.03.07.
- [34] А. Білецький, А. Білецький, і Р. Кандиба, «Матричні аналоги протоколу Діффі-Хеллмана», *Автоматика, вимірювання та керування: Вісник нац. ун-ту "Львівська політехніка"*, вип. 741, С. 128—133, 2012.
- [35] S. D. Cohen i S. Huczynska, «The strong primitive normal basis theorem», *Acta Arith.*, т. 143, вип. 4, С. 299—332, 2010, doi: 10.4064/aa143-4-1.
- [36] S. D. Cohen i G. Kapetanakis, «The trace of 2-primitive elements of finite fields», *Acta Arith.*, т. 192, вип. 4, С. 397—419, 2020, doi: 10.4064/aa190307-23-5.
- [37] A. Fernandes i L. Reis, «On primitive elements of finite fields avoiding affine hyperplanes», *Finite Fields and Their Applications*, т. 76, С. 101911, груд. 2021, doi: 10.1016/j.ffa.2021.101911.
- [38] P. Shihui, Z. Hongwei, i Z. Yongzhe, «Public key cryptography based on ergodic matrices over finite field», *Wuhan Univ. J. Nat. Sci.*, т. 11, вип. 6, С. 1525—1528, листоп. 2006, doi: 10.1007/BF02831812.
- [39] G. Chun-sheng, Y. Zhi-ming, J. Zheng-jun, i G. Jixing, «Cryptanalysis on Public Key Encryption Scheme Using Ergodic Matrices over GF(2)», у *Advances in Technology and Management*, т. 165, Н. Kim, Ред., у *Advances in Intelligent and Soft Computing*, vol. 165. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, С. 129—135. doi: 10.1007/978-3-642-29637-6_17.
- [40] E. Sakalauskas, A. Mihalkovich, i A. Venčkauskas, «Improved Asymmetric Cipher Based on Matrix Power Function with Provable Security», *Symmetry*, т. 9, вип. 1, С. 9, січ. 2017, doi: 10.3390/sym9010009.
- [41] E. Sakalauskas, L. Dindienė, A. Kilčiauskas, i K. Lukšys, «Perfectly Secure Shannon Cipher Construction Based on the Matrix Power Function», *Symmetry*, т. 12, вип. 5, С. 860, трав. 2020, doi: 10.3390/sym12050860.

- [42] L. Dindiene, A. Mihalkovich, K. Luksys, i E. Sakalauskas, «Matrix Power Function Based Block Cipher Operating in CBC Mode», *Mathematics*, т. 10, вип. 12, С. 2123, чер. 2022, doi: 10.3390/math10122123.
- [43] S. Ali, A. S. Alali, A. A. Khan, I. E. Wijayanti, i K. B. Wong, «XOR count and block circulant MDS matrices over finite commutative rings», *MATH*, т. 9, вип. 11, С. 30529—30547, 2024, doi: 10.3934/math.20241474.
- [44] A. Shcherba, E. Faure, A. Skutskyi, i O. Kharin, «Families of Square Commutative 2x2 Matrices», *CEUR Workshop Proceedings*, т. 3550, С. 289—296, 2023.
- [45] E. Faure, A. Shcherba, A. Skutskyi, i A. Lavdanskyi, «A Finite Field of Square Matrices of Order 2», *CEUR Workshop Proceedings*, т. 3550, С. 306—312, 2023.
- [46] A. Shcherba, E. Faure, T. Vartiainen, i V. Khaliavka, «Primitive Elements in the Finite Field of Square Matrices of Order 2 for Cryptographic Applications», у *Information Technology for Education, Science, and Technics*, т. 222, E. Faure, Y. Tryus, T. Vartiainen, O. Danchenko, M. Bondarenko, C. Bazilo, i G. Zaspas, Ред., у *Lecture Notes on Data Engineering and Communications Technologies*, vol. 222. , Cham: Springer Nature Switzerland, 2024, С. 250—265. doi: 10.1007/978-3-031-71804-5_17.
- [47] А. І. Щерба, Е. В. Фауре, і В. В. Халявка, «Примітивні елементи скінченного поля квадратних матриць порядку 2 для криптографічних застосувань», у *Тези доповідей VII Міжнародної науково-практичної конференції «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2024), (Черкаси, 23-24 травня 2024 р.)*, Черкаси: ЧДТУ, 2024, С. 183—185.
- [48] Е. В. Фауре і В. В. Халявка, «Метод вибору примітивних елементів у полях матриць 2×2 для криптографічних протоколів», у *Збірник тез доповідей IV Міжнар. наук.-практич. конфер. «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-*

- 2025)» (25 лист. 2025 р., м. Черкаси), М-во освіти і науки України, Черкас. держ. технол. ун-т. Черкаси : ЧДТУ, 2025, С. 273—275.
- [49] A. Baikenov, E. Faure, A. Shcherba, V. Khaliavka, S. Tynymbayev, і O. Abramkina, «A Unified Method for Selecting Parameters and Primitive Elements in 2×2 Matrix Fields for Cryptographic Protocols», *Symmetry*, т. 17, вип. 8, С. 1212, лип. 2025, doi: 10.3390/sym17081212.
- [50] A. Baikenov та ін., «ElGamal Digital Signature Scheme in a Matrix Finite Field», у *2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Paris, France: IEEE, лип. 2025, С. 1—6. doi: 10.1109/ICECET63943.2025.11472340.
- [51] V. S. Miller, «Use of Elliptic Curves in Cryptography», у *Advances in Cryptology — CRYPTO '85 Proceedings*, т. 218, Н. С. Williams, Ред., у Lecture Notes in Computer Science, vol. 218. , Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, С. 417—426. doi: 10.1007/3-540-39799-X_31.
- [52] S. Duval і G. Leurent, «MDS Matrices with Lightweight Circuits», *ToSC*, С. 48—78, чер. 2018, doi: 10.46586/tosc.v2018.i2.48-78.
- [53] M. Y. Malik і J.-S. No, «Dynamic MDS Matrices for Substantial Cryptographic Strength», 2011. , *arXiv*. doi: 10.48550/ARXIV.1108.6302.
- [54] L. T. Thi і L. N. Van, «Advanced 8×8 circulant MDS matrices and key-dependent AES enhancement», *Cryptogr. Commun.*, т. 18, вип. 2, С. 457—488, берез. 2026, doi: 10.1007/s12095-025-00847-x.
- [55] M. Rasslan і A. Youssef, «Cryptanalysis of a Public Key Encryption Scheme Using Ergodic Matrices», *IEICE Trans. Fundamentals*, т. E94-A, вип. 2, С. 853—854, 2011, doi: 10.1587/transfun.E94.A.853.
- [56] C. Gu, Z. Jing, і Z. Yu, «Polynomial time algorithm for the two-side exponentiation problem about ergodic matrices over finite field», *Wuhan Univ. J. Nat. Sci.*, т. 17, вип. 3, С. 233—237, чер. 2012, doi: 10.1007/s11859-012-0834-3.
- [57] Huang, Hua-Wei, Peng, Chang-Wen, Qu, Yun-Yun, і Li, Chun-Hua, «Security of the cryptosystems based on ergodic matrices», *Tongxin Xuebao/Journal on*

- Communications*, т. 36, вип. 8, С. 61, 2015, doi: 10.11959/j.issn.1000-436x.2015128.
- [58] A. Mihalkovich, E. Sakalauskas, i A. Venckauskas, «New Asymmetric Cipher Based On Matrix Power Function and Its Implementation in Microprocessors Efficiency Investigation», *ELEKTRON ELEKTROTECH*, т. 19, вип. 10, С. 119—122, груд. 2013, doi: 10.5755/j01.eee.19.10.5906.
- [59] J. Liu, H. Zhang, i J. Jia, «A Linear Algebra Attack on the Non-commuting Cryptography Class Based on Matrix Power Function», у *Information Security and Cryptology*, т. 10143, К. Chen, D. Lin, i M. Yung, Ред., у *Lecture Notes in Computer Science*, vol. 10143. , Cham: Springer International Publishing, 2017, С. 343—354. doi: 10.1007/978-3-319-54705-3_21.
- [60] E. Sakalauskas i A. Mihalkovich, «Improved Asymmetric Cipher Based on Matrix Power Function Resistant to Linear Algebra Attack», *Informatica*, т. 28, вип. 3, С. 517—524, січ. 2017, doi: 10.15388/Informatica.2017.142.
- [61] E. Sakalauskas, «Enhanced Matrix Power Function for Cryptographic Primitive Construction», *Symmetry*, т. 10, вип. 2, С. 43, лют. 2018, doi: 10.3390/sym10020043.
- [62] A. Mihalkovich, J. Zitkevicius, i E. Sakalauskas, «The security analysis of the key exchange protocol based on the matrix power function defined over a family of non-commuting groups», *MATH*, т. 9, вип. 10, С. 26961—26982, 2024, doi: 10.3934/math.20241312.
- [63] D. S. Yadav, R. K. Sharma, i W. Shukla, «On Applications of Singular Matrices over Finite Fields in Cryptography», у *Security Aspects in Information Technology*, т. 7011, М. Joye, D. Mukhopadhyay, i M. Tunstall, Ред., у *Lecture Notes in Computer Science*, vol. 7011. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, С. 181—185. doi: 10.1007/978-3-642-24586-2_16.
- [64] М.-С. Chang, «On a matrix product question in cryptography», *Linear Algebra and its Applications*, т. 439, вип. 7, С. 1742—1748, жовт. 2013, doi: 10.1016/j.laa.2013.05.013.

- [65] M. Zeriouh, A. Chillali, i A. Boua, «Cryptography based on the Matrices», *B Soc Paran Mat*, т. 37, вып. 3, С. 75—83, верес. 2017, doi: 10.5269/bspm.v37i3.34542.
- [66] S. Lipschutz, *Schaum's outline of theory and problems of linear algebra*, 2nd ed. y Schaum's outline series. New York: McGraw-Hill, 1991.
- [67] F. R. Gantmacher, *The theory of matrices*, Reprinted., т. 1. Providence, RI: American Mathematical Soc, 1959.
- [68] J. M. Laughlin, «Combinatorial identities deriving from the n -th power of a 2×2 matrix», *Integers*, т. 4, С. 1—15, 2004, doi: 10.48550/ARXIV.1812.11168.
- [69] V. I. Arnold, «Fermat dynamics, matrix arithmetics, finite circles, and finite Lobachevsky planes», *Functional Analysis and Its Applications*, т. 38, вып. 1, С. 1—13, 2004, doi: 10.1023/B:FAIA.0000024863.06462.68.
- [70] S. Wright, *Quadratic Residues and Non-Residues*, т. 2171. y Lecture Notes in Mathematics, vol. 2171. Cham: Springer International Publishing, 2016. doi: 10.1007/978-3-319-45955-4.
- [71] R. A. Horn i C. R. Johnson, *Matrix Analysis*. Cambridge University Press, 2012.
- [72] K. F. Ireland i M. I. Rosen, *A classical introduction to modern number theory*, 2nd вид. y Graduate texts in mathematics, no. 84. New York: Springer-Verlag, 1990.
- [73] R. A. Horn i C. R. Johnson, *Matrix analysis*, 2nd ed. Cambridge ; New York: Cambridge University Press, 2012.
- [74] D. M. Burton, *The history of mathematics: an introduction*, 7th ed. New York: McGraw-Hill, 2011.
- [75] F. Viete, *Opera Mathematica in unum volumen congesta*. Leiden: Bonaventure & Abraham Elzevier, 1646.
- [76] I. M. Vinogradov, *Elements of number theory*, Dover edition. y Dover books on mathematics. Mineola, New York: Dover Publications, Inc, 2016.

- [77] J. H. Silverman i J. T. Tate, *Rational Points on Elliptic Curves*. y Undergraduate Texts in Mathematics. Cham: Springer International Publishing, 2015. doi: 10.1007/978-3-319-18588-0.
- [78] H. Davenport, *Multiplicative Number Theory*, т. 74. y Graduate Texts in Mathematics, vol. 74. New York, NY: Springer New York, 1980. doi: 10.1007/978-1-4757-5927-3.
- [79] R. Takloo-Bighash, *A Pythagorean Introduction to Number Theory: Right Triangles, Sums of Squares, and Arithmetic*. y Undergraduate Texts in Mathematics. Cham: Springer International Publishing, 2018. doi: 10.1007/978-3-030-02604-2.
- [80] D. E. Knuth, *The Art of Computer Programming : Seminumerical Algorithms*, 3rd Ed., т. 2. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1997.
- [81] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*, 20th anniversary edition. Indianapolis, IN: Wiley, 2015.
- [82] A. K. Lenstra, *The Development of the Number Field Sieve*. y Lecture Notes in Mathematics Ser, no. v. 1554. Berlin, Heidelberg: Springer Berlin / Heidelberg, 1993.
- [83] J. Hoffstein, J. Pipher, i J. H. Silverman, *An Introduction to Mathematical Cryptography*. y Undergraduate Texts in Mathematics. New York, NY: Springer New York, 2014. doi: 10.1007/978-1-4939-1711-2.
- [84] D. J. Bernstein i A. K. Lenstra, «A general number field sieve implementation», y *The development of the number field sieve*, т. 1554, A. K. Lenstra i H. W. Lenstra, Ред., y Lecture Notes in Mathematics, vol. 1554. , Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, С. 103—126. doi: 10.1007/BFb0091541.
- [85] D. Coppersmith, A. M. Odlyzko, i R. Schroepel, «Discrete logarithms in $GF(p)$ », *Algorithmica*, т. 1, вып. 1—4, С. 1—15, листоп. 1986, doi: 10.1007/BF01840433.

- [86] D. Coppersmith, «Modifications to the Number Field Sieve», *J. Cryptology*, т. 6, вип. 3, С. 169—180, берез. 1993, doi: 10.1007/BF00198464.
- [87] L. Adleman, «A subexponential algorithm for the discrete logarithm problem with applications to cryptography», у *20th Annual Symposium on Foundations of Computer Science (sfcs 1979)*, San Juan, Puerto Rico: IEEE, жовт. 1979, С. 55—60. doi: 10.1109/SFCS.1979.2.
- [88] T. ElGamal, «On Computing Logarithms Over Finite Fields», у *Advances in Cryptology — CRYPTO '85 Proceedings*, т. 218, Н. С. Williams, Ред., у *Lecture Notes in Computer Science*, vol. 218. , Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, С. 396—402. doi: 10.1007/3-540-39799-X_28.
- [89] J. Buchmann, M. Jacobson, і E. Teske, «On some computational problems in finite abelian groups», *Math. Comp.*, т. 66, вип. 220, С. 1663—1687, 1997, doi: 10.1090/S0025-5718-97-00880-6.
- [90] А. І. Щерба, Е. В. Фауре, і В. В. Халявка, «Примітивні елементи скінченного поля квадратних матриць порядку 2 для криптографічних застосувань», у *Збірник тез доповідей IV Міжнар. наук.-практич. конфер. «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2025)» (25 лист. 2025 р., м. Черкаси)*, Черкаси: ЧДТУ, 2025, С. 273—275.
- [91] D. R. Stinson і M. B. Paterson, *Cryptography: theory and practice*, Fourth edition, First issued in paperback. Boca Raton, FL: Chapman & Hall/CRC Press, 2022.
- [92] A. Odlyzko, «Discrete Logarithms: The Past and the Future», *Designs, Codes and Cryptography*, т. 19, вип. 2/3, С. 129—145, 2000, doi: 10.1023/A:1008350005447.
- [93] Н. С. А. Van Tilborg і S. Jajodia, Ред., *Encyclopedia of Cryptography and Security*. Boston, MA: Springer US, 2011. doi: 10.1007/978-1-4419-5906-5.
- [94] J. L. Massey, «Cryptography: Fundamentals and applications», у *Copies of transparencies, Advanced Technology Seminars*, 1993, С. 119.

- [95] C. E. Shannon, «Communication theory of secrecy systems», *Bell Systems Technical Journal*, т. 28, С. 656—715, 1948.
- [96] «The Marsaglia Random Number CDROM including the Diehard Battery of Tests». Дата звернення: 2016. 24 лют. [URL]. Доступний у: <http://stat.fsu.edu/pub/diehard/>
- [97] L. E. Bassham III та ін., «Special Publication (NIST SP) - 800-22 Rev 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications», National Institute of Standards & Technology, Gaithersburg, MD, United States, 2010.
- [98] P. L'Ecuyer і R. Simard, «TestU01: A C library for empirical testing of random number generators», *ACM Transactions on Mathematical Software (TOMS)*, т. 33, вип. 4, С. 22, 2007.
- [99] E. V. Faure, A. I. Shcherba, і V. M. Rudnytskyi, «The Method and Criterion for Quality Assessment of Random Number Sequences», *Cybernetics and Systems Analysis*, т. 52, вип. 2, С. 277—284, 2016, doi: 10.1007/s10559-016-9824-3.
- [100] E. Faure, I. Myronets, і A. Lavdanskyi, «Autocorrelation criterion for quality assessment of random number sequences», *CEUR Workshop Proceedings*, т. 2608, С. 675—689, 2020, doi: 10.32782/cmis/2608-52.
- [101] U. M. Maurer, «A universal statistical test for random bit generators», *J. Cryptology*, т. 5, вип. 2, С. 89—105, 1992, doi: 10.1007/BF00193563.

ДОДАТКИ

Додаток А. Лістинги експериментальних моделей

А.1. Лістинг модуля базових операцій у полі квадратних матриць другого порядку

```

from dataclasses import dataclass
import hashlib
import math
import random
@dataclass(frozen=True)
class MatrixFieldElement:
    x: int
    y: int
    p: int
    a: int
    b: int

    def __post_init__(self):
        object.__setattr__(self, "x", self.x % self.p)
        object.__setattr__(self, "y", self.y % self.p)

    def to_matrix(self):
        return [
            [self.x % self.p, self.y % self.p],
            [(self.b * self.y) % self.p, (self.x + self.a * self.y) % self.p]
        ]

    @staticmethod
    def one(p: int, a: int, b: int):
        return MatrixFieldElement(1, 0, p, a, b)

    @staticmethod
    def zero(p: int, a: int, b: int):
        return MatrixFieldElement(0, 0, p, a, b)

    def __mul__(self, other):
        if (self.p, self.a, self.b) != (other.p, other.a, other.b):
            raise ValueError("Несумісні параметри поля")

        x = (self.x * other.x + self.b * self.y * other.y) % self.p
        y = (self.x * other.y + self.y * other.x + self.a * self.y * other.y) % self.p
        return MatrixFieldElement(x, y, self.p, self.a, self.b)

```

```

def __pow__(self, exponent: int):
    if exponent < 0:
        return self.inverse() ** (-exponent)

    result = MatrixFieldElement.one(self.p, self.a, self.b)
    base = self
    e = exponent

    while e > 0:
        if e & 1:
            result = result * base
            base = base * base
            e >>= 1

    return result

def inverse(self):
    norm = (self.x * self.x + self.a * self.x * self.y - self.b * self.y * self.y) % self.p
    if norm == 0:
        raise ZeroDivisionError("Елемент не має оберненого")

    norm_inv = pow(norm, -1, self.p)
    inv_x = ((self.x + self.a * self.y) * norm_inv) % self.p
    inv_y = ((-self.y) * norm_inv) % self.p
    return MatrixFieldElement(inv_x, inv_y, self.p, self.a, self.b)

def encode_p_adic(self) -> int:
    return self.x + self.y * self.p

    @staticmethod
    def decode_p_adic(n: int, p: int, a: int, b: int):
        x = n % p
        y = (n // p) % p
        return MatrixFieldElement(x, y, p, a, b)

def __repr__(self):
    return f'MF({self.x}, {self.y}; p={self.p}, a={self.a}, b={self.b})'

def hash_message(message: str, modulus: int) -> int:
    digest = hashlib.sha256(message.encode("utf-8")).digest()
    return int.from_bytes(digest, "big") % modulus

```

A.2. Лістинг моделі протоколу узгодження ключів

```
def diffie_hellman_matrix_demo(p: int, a: int, b: int, g: MatrixFieldElement,
                               alice_secret: int, bob_secret: int):

    # Формування відкритих ключів
    alice_public = g ** alice_secret
    bob_public = g ** bob_secret

    # Формування спільного секрету
    alice_shared = bob_public ** alice_secret
    bob_shared = alice_public ** bob_secret

    return {
        "alice_secret": alice_secret,
        "bob_secret": bob_secret,
        "alice_public": alice_public,
        "bob_public": bob_public,
        "alice_shared": alice_shared,
        "bob_shared": bob_shared,
        "shared_equal": alice_shared == bob_shared
    }

if __name__ == "__main__":
    # Приклад параметрів
    p = 5
    a = 1
    b = 2

    # Умовний примітивний елемент поля
    g = MatrixFieldElement(2, 1, p, a, b)

    # Закриті ключі учасників
    alice_secret = 7
    bob_secret = 11

    result = diffie_hellman_matrix_demo(p, a, b, g, alice_secret, bob_secret)

    print("=== Протокол узгодження ключів ===")
    print("Відкритий ключ Аліси:", result["alice_public"])
    print("Відкритий ключ Боба :", result["bob_public"])
    print("Спільний ключ Аліси :", result["alice_shared"])
    print("Спільний ключ Боба :", result["bob_shared"])
    print("Ключі збігаються   :", result["shared_equal"])
```

A.3. Лістинг моделі протоколу ЕЦП Ель-Гамал

```

def generate_coprime_k(order_minus_one: int) -> int:
    while True:
        k = random.randint(1, order_minus_one - 1)
        if math.gcd(k, order_minus_one) == 1:
            return k

def elgamal_matrix_keygen(p: int, a: int, b: int, g: MatrixFieldElement, x:
int):
    y = g ** x
    return x, y

def elgamal_matrix_sign(message: str, p: int, a: int, b: int,
                        g: MatrixFieldElement, x: int):

    # Формування підпису
    group_order = p * p - 1
    h = hash_message(message, group_order)

    k = generate_coprime_k(group_order)
    R = g ** k
    r = R.encode_p_adic()

    k_inv = pow(k, -1, group_order)
    s = ((h - x * r) * k_inv) % group_order

    return (r, s)

def elgamal_matrix_verify(message: str, signature: tuple[int, int],
                        p: int, a: int, b: int,
                        g: MatrixFieldElement, y: MatrixFieldElement) -> bool:

    # Перевірка підпису
    group_order = p * p - 1
    r, s = signature

    h = hash_message(message, group_order)
    R = MatrixFieldElement.decode_p_adic(r, p, a, b)

    left = (y ** r) * (R ** s)
    right = g ** h

    return left == right

```

```

if __name__ == "__main__":
    p = 5
    a = 1
    b = 2
    g = MatrixFieldElement(2, 1, p, a, b)

    x = 9
    _, y = elgamal_matrix_keygen(p, a, b, g, x)

    message = "Test message for matrix ElGamal signature"
    signature = elgamal_matrix_sign(message, p, a, b, g, x)
    verified = elgamal_matrix_verify(message, signature, p, a, b, g, y)

    print("\n=== Протокол ЕЦП Ель-Гамалія ===")
    print("Відкритий ключ:", y)
    print("Підпис (r, s):", signature)
    print("Результат перевірки:", verified)

```

А.4. Лістинг модуля перевірки працездатності імітаційної моделі

```

def self_test():
    p = 5
    a = 1
    b = 2
    g = MatrixFieldElement(2, 1, p, a, b)

    # Перевірка узгодження ключів
    dh = diffie_hellman_matrix_demo(
        p=p,
        a=a,
        b=b,
        g=g,
        alice_secret=3,
        bob_secret=8
    )
    assert dh["shared_equal"], "Помилка: спільні ключі не збігаються"

    # Перевірка ЕЦП
    x = 4
    _, y = elgamal_matrix_keygen(p, a, b, g, x)
    msg = "Matrix cryptography"
    signature = elgamal_matrix_sign(msg, p, a, b, g, x)
    assert elgamal_matrix_verify(msg, signature, p, a, b, g, y), \

```

```

        "Помилка: підпис не проходить перевірку"

# Перевірка модифікованого повідомлення
assert not elgamal_matrix_verify("Modified message", signature, p, a, b, g,
y), \
    "Помилка: хибний підпис прийнято як правильний"

print("Усі тести успішно пройдено.")

if __name__ == "__main__":
    self_test()

```


Додаток Б. Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації

- [1] A. Shcherba, E. Faure, T. Vartiainen, i V. Khaliavka, «Primitive Elements in the Finite Field of Square Matrices of Order 2 for Cryptographic Applications», Lecture Notes on Data Engineering and Communications Technologies, т. 222, Cham: Springer Nature Switzerland, 2024, С. 250-265. doi: [10.1007/978-3-031-71804-5_17](https://doi.org/10.1007/978-3-031-71804-5_17). (Scopus)
- [2] A. Baikenov, E. Faure, A. Shcherba, V. Khaliavka, S. Tynymbayev, i O. Abramkina, «A Unified Method for Selecting Parameters and Primitive Elements in 2×2 Matrix Fields for Cryptographic Protocols», Symmetry, т. 17, вип. 8, 1212, 2025, doi: [10.3390/sym17081212](https://doi.org/10.3390/sym17081212). (Scopus, Web of Science, Q2)

Наукові праці, які засвідчують апробацію матеріалів дисертації

- [1] Щерба А.І., Фауре Е.В., Халявка В.В. Примітивні елементи скінченного поля квадратних матриць порядку 2 для криптографічних застосувань // Тези доповідей VII Міжнародної науково-практичної конференції «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2024), (Черкаси, 23-24 травня 2024 р.) [Електронний ресурс]. Черкаси : ЧДТУ, 2024. С. 183-185. [Online]. Доступний за: https://er.chdtu.edu.ua/bitstream/ChSTU/5863/1/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D1%82%D0%B5%D0%B7%D0%86%D0%A2%D0%9E%D0%9D%D0%A2-2024_%D0%BC%D0%B0%D0%BA%D0%B5%D1%82.pdf#page=183
- [2] Фауре Е. В., Халявка В. В. Метод вибору примітивних елементів у полях матриць 2×2 для криптографічних протоколів // Збірник тез доповідей IV Міжнар. наук.-практич. конфер. «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2025)» (25 лист. 2025 р.,

м. Черкаси) [Електронний ресурс] / упоряд. : Т. О. Прокопенко, О. І. Підкуйко. М-во освіти і науки України, Черкас. держ. технол. ун-т. Черкаси : ЧДТУ, 2025. С. 273-275. [Online]. Доступний за:
https://drive.google.com/file/d/1vfK7HzALRZHFTE8SKi6P_c-D3X4K3YPK/view

- [3] A. Baikenov, E. Faure, A. Shcherba, A. Lavdanskyi, S. Tynymbayev, V. Khaliavka, O. Abramkina. ElGamal Digital Signature Scheme in a Matrix Finite Field // 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), Paris, France, 2025. P. 1-6. DOI: [10.1109/ICECET63943.2025.11472340](https://doi.org/10.1109/ICECET63943.2025.11472340).

Апробацію результатів дисертації проведено на:

- VII Міжнародній науково-практичній конференції «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2024), (Черкаси, 23-24 травня 2024 р.);
- IV Міжнародній науково-практичній конференції «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2025)» (25 лист. 2025 р., м. Черкаси);
- V International Conference on Electrical, Computer and Energy Technologies (ICECET 2025), (3-6 July 2025, Paris-France).