DOI 10.31891/2307-5732-2024-343-6-29
УДК 004.681

ОБЕРИШИН РОКСОЛАНА
Національний університет “Львівська політехніка”
https://orcid.org/0000-0003-0732-6743
e-mail: roksoliana.r.oberyshyn@lpnu.ua
ПОПОВИЧ РОМАН
Національний університет “Львівська політехніка”
https://orcid.org/0009-0006-0992-0825
e-mail: rombp07@gmail.com

ПРО ОБОРОТНІ ЕЛЕМЕНТИ В ОДНОМУ КЛАСІ ГРУПОВИХ КІЛЕЦЬ

Досліджено питання пошуку оборотних елементів для часткових групових кілець, які можна задати будь-якими скінченним полем та скінченною циклічною групою. Розроблено програму в середовищі Python для виконання обчислень над елементами таких групових кільцях.

Ключові слова: скінченне поле, скінченна циклічна група , групове кільце, оборотний елемент.

OBERYSHYN ROKSOLANA, POPOVYCH ROMAN
Lviv Polytechnic National University

ON UNITS IN ONE CLASS OF GROUP RINGS

The basis of the vast majority of cryptographic information protection systems are the so-called computationally hard problems. One such problem is to find the discrete logarithm in a suitably chosen finite group. This problem consists in obtaining for two arbitrary elements of the group such a natural number that the first element to the power of this number is equal to the second element. Currently, research on discrete logarithm-based methods in groups with commutative or non-commutative operation is insufficient. The research of the mentioned issues of information protection is also affected by expectations regarding the appearance of powerful quantum computers that will be able to solve hard computational problems in polynomial time, which are beyond the capabilities of modern deterministic computers. Therefore, in particular, they study groups consisting of units of group rings specified by a certain ring with a unit and a group.

The issue of finding units for partial group rings, which can be defined by any finite field and finite cyclic group, is investigated. A program was developed in the Python environment for performing calculations on the elements of such group rings (raising an element to the power of a large natural number, finding out whether an element is a unit or not a unit, finding the number of different powers of an arbitrary element, factoring of polynomials that define a group ring into irreducible factors). With the use of this program, computational data were obtained, which made it possible to formulate assumptions about the exact number of elements in terms of the number of elements of the corresponding field and group. The application of the specified number will allow finding group ring units that would simultaneously have the large multiplicative order. Actually, these are needed when constructing a series of recently proposed asymmetric cryptosystems.

Keywords: finite field, finite cyclic group, group ring, unit.

Постановка проблеми

Основою переважної більшості криптографічних систем захисту інформації є так звані обчислювально складні проблеми. Однією з таких проблем є знаходження дискретного логарифму у належним чином обраній скінченній групі. Наразі дослідження методів на основі дискретного логарифму в групах з комутативною або некомутативною операцією є недостатніми. На дослідження питань захисту інформації також впливають очікування щодо появи потужних квантових комп'ютерів, що зможуть вирішувати за поліноміальний час складні обчислювальні завдання, які непосильні для сучасних детермінованих комп'ютерів. Тому, зокрема, вивчають групи, які складаються з оборотних елементів групових кілець, заданих певними кільцем з одиницею та групою.

Аналіз останніх джерел

Такий клас алгебраїчних структур, як групові кільця, не використовували в криптографії до другого десятиліття XXI століття. У [2] вперше запропоновано криптосистему з відкритим ключем, що використовує групові кільця. При шифруванні та дешифруванні використано оборотні елементи та обчислювальну складність дискретного логарифму у групових кільцях. Також розглянуто комбінування такої криптосистеми з відомою криптосистемою RSA. Крім того, запропоновано поєднання згаданої криптосистеми та завадостійкого кодування в одній системі. В [3] обговорено численні застосування групових кілець у сфері комунікацій та цифрового опрацювання сигналів. Також проводять дослідження, пов’язані з використанням матриць над груповими кільцями [4].

У статті [5] запропоновано дві асиметричні криптосистеми на основі групових кілець. Перша – це асиметрична криптосистема над груповим кільцем, яка поєднує еліптичні криві та конструкцію Ель-Гамаля, а друга – асиметрична криптосистема над груповим кільцем типу Ель-Гамаля без залучення еліптичних кривих. Обидві обчислювальні схеми використовують оборотні елементи групових кілець. Згадані дві криптосистеми мають більший рівень безпеки, ніж існуючі криптосистеми, оскільки невідомий ніякий квантовий алгоритм для вирішення проблеми дискретного логарифму у групових кільцях. У прийдешню еру квантових комп’ютерів цей підсилений захист відігравав би суттєву роль.

Наявна значна кількість публікацій про структуру групи оборотних елементів групових кілець, але дуже мало статей, у яких групу оборотних елементів обчислюють явно в термінах елементів групового кільця. Разом з тим останнє є більш важливим для використання групових кілець у криптографії. Тому потрібно

набагато більше зусиль для явного зображення групи оборотних елементів у термінах елементів групового кільця.

Власне інтерес складає мультиплікативна група для групового кільця: множина елементів групового кільця, для яких існує обернений відносно множення. Відомі роботи [1, 5], де наведено опис згаданої мультиплікативної групи. У цих роботах описано, як шукати оборотні елементи для низки групових кілець. Зокрема, використовують відомі середовища для математичних обчислень GAP (пакети LAGUNA, Wedderga), Magma, Matlab. Так, використовуючи пакет LAGUNA середовища GAP [5], група оборотних елементів групового кільця, заданого скінченним полем з p елементів для деякого простого числа p та скінченною p-групою, може бути ефективно обчислена для невеликих значень p. Але зі збільшенням цього числа середовище GAP стає неефективним [5]. Тому актуальною задачею є дослідження питання знаходження оборотних елементів для різних класів групових кілець.

Метою роботи є: подальше дослідження питання пошуку оборотних елементів у групових кільцях, які утворені скінченним полем та скінченною циклічною групою.

Виклад основного матеріалу

Якщо задані кільце з одиницею R та група G, то множину всеможливих скінченних сум

$$RG = \{\sum_{i=0}^{t} r_i g_i \,|t = 0,1,2,\dots, r_i \in R, g_i \in G\}$$

називають груповим кільцем [1]. Елемент $u \in RG$ називають оборотним, якщо існує такий елемент $v \in RG$, що $uv = vu = 1$. Через F_q, де $q = p^n$ для деякого простого числа p та натурального числа n, позначаємо скінченне поле з q елементів [6].

Розглядаємо частковий випадок, коли кільце $R = F_q$ є скінченним полем, а група $G = C_r = \langle x \rangle = \{x^i | 0 \le i \le r-1\}$ є скінченною циклічною групою з r елементами. При використанні позначення $g_i = x^i$ групове кільце має вигляд $RG = F_q[x]/(x^r - 1)$. Воно складається з многочленів від змінної x з коефіцієнтами з поля F_q степеня не більшого $r-1$. Кількість елементів цього групового кільця дорівнює q^r. Оборотними елементами цього фактор-кільця є ті многочлени, які взаємно прості з $x^r - 1$. З'ясувати, чи многочлен оборотний та одночасно знайти обернений до нього, можна, використовуючи розширений алгоритм Евкліда для многочленів [1].

Вказаний многочлен $x^r - 1$ має відомий розклад [6] на нерозкладні над полем раціональних чисел множники (так звані циклотомічні многочлени): $x^r - 1 = \prod_{d|r} \Phi_r(x)$. Степінь множника $\Phi_r(x)$ дорівнює $\phi(r)$ – значенню функції Ейлера для числа r.Зокрема, якщо r – просте число, то $x^r - 1 = (x-1)(x^{r-1} + \dots + x + 1)$. Проте, це розклад над полем раціональних чисел, тобто на многочлени з цілими коефіцієнтами. Якщо ж говорити про розклад над скінченним полем F_q (q не ділиться на r), то $\Phi_r(x)$ може далі розкладатися [6] на $\frac{\phi(r)}{d}$ нерозкладних множників степеня d, де d мультиплікативний порядок числа q за модулем r ($d = ord_r(q)$). Многочлен $\Phi_r(x)$ нерозкладний над F_q тоді тільки тоді, коли $ord_r(q) = \phi(r)$.

Добуток двох оборотних елементів є оборотним елементом. Як наслідок, степінь оборотного елемента є оборотним елементом. Усі оборотні елементи групового кільця утворюють групу $U(RG)$. Добуток двох необоротних елементів є необоротним елементом і, зокрема, степінь необоротного елемента є необоротним елементом.

Нами розроблено програму в середовищі Python для виконання обчислень над довільними елементами групових кілець, які задані скінченним полем та скінченною циклічною групою. Метою є отримання обчислювального матеріалу для можливих подальших теоретичних узагальнень та підтвердження достовірності теоретичних результатів. Зокрема, кожен елемент можна підносити до степеня великого натурального числа. У результаті для будь-якого елемента можна визначити, є він оборотним чи ні. Якщо елемент є оборотнім, то для нього підраховуємо його порядок, тобто кількість попарно різних степенів. Якщо ж елемент необоротній, то обчислюємо кількість його різних степенів. Також реалізовано розклад многочленів, які задають групове кільце, на нерозкладні множники. Кожен елемент групового кільця реалізовано як масив цілих чисел довжини r. Деякі з отриманих результатів наведено в табл. 1.

Розглянемо більш детально приклад для випадку $q = 2$ та $r = 11$. Деякі відомості про цей модельний приклад наведені також у праці [5]. У цьому разі групове кільце $RG = F_2[x]/(x^{11} - 1)$ має 2048 елементів. Многочлен $x^{11} - 1$ має розклад $x^{11} - 1 = (x-1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ над полем раціональних чисел. Оскільки $ord_{11}(2) = \phi(11) = 10$, то другий співмножник далі не розкладається на F_2.

У цьому груповому кільці є як оборотні, так і необоротні елементи. Як було зауважено раніше, елемент оборотний тоді і тільки тоді, коли він взаємно простий з $x^{11} - 1$.

Елемент $h = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ не є взаємно простим з $x^{11} - 1$ і тому необоротний. Цей елемент має лише один різний степінь: $h^2 = h$. Елемент 0 необоротний і має один різний степінь. Елемент $x + 1$ не взаємно простий з $x^{11} - 1$ і тому необоротний. Він має 341 різний степінь. Усі степені цього елемента є необоротними. Справедлива рівність $(x+1)^{341} = x + 1$.

Таблиця 1

Кількість оборотних елементів у групових кільцях

q	r	$ord_r(q)$	$\|U(RG)\|$
2	3	2	3
2	5	4	15
2	7	3	49(63)
2	11	10	1023
2	13	12	4095
2	17	8	62025 (65535)
3	2	1	4
3	5	4	160
3	7	6	1456
3	11	5	117128(118096)
3	13	3	913952(1062882)
5	2	1	16
5	3	2	96
5	7	6	62496

Елемент $g_1 = x^3 + x + 1$ взаємно простий з $x^{11} - 1$ і тому оборотний. Він має порядок 1023: $(g_1)^{1023} = 1$. Всі його степені є оборотними. Елемент $g_2 = x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$ взаємно простий з $x^{11} - 1$ і тому оборотний. Порядок цього елемента дорівнює 341: $(g_2)^{341} = 1$. Елемент x оборотний і має порядок 11: $x^{11} = 1$.

Таким чином, кількість необоротних елементів дорівнює 1025, а кількість оборотних – 1023. Оборотні елементи утворюють групу, кількість елементів у якій дорівнює 1023. Зауважимо, що $1023 = 3 \cdot 341 = 3 \cdot 11 \cdot 13$. За наслідком з теореми Лагранжа для скінченних груп, можливі порядки елементів у цій групі дорівнюють 1, 3, 11, 31, 33, 93, 341, 1023. Для кожного з наведених чисел є елементи відповідного порядку. Зокрема, є елементи максимально можливого порядку 1023.

Наведений обчислювальні дані показують, що кількість оборотних елементів залежить від кількості множників у розкладі многочлена $x^r - 1$. Якщо є розклад лише на два множники, то можна припустити, що ця кількість дорівнює $(q-1)(q^{r-1} - 1)$. Із збільшенням кількості множників у розкладі вказана кількість зменшується. Це, зокрема, видно для низки випадків у табл. 1.

Так, для випадку $q = 2$ та $r = 17$ маємо $ord_r(q) = 8$. У цьому разі многочлен

$$x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + +x^5 + x^4 + +x^3 + x^2 + x + 1 =$$
$$= (x^8 + x^5 + x^4 + x^3 + 1)(x^8 + x^7 + x^6 + x^4 + x^2 + x + 1)$$

розкладається на два множники. Замість очікуваної кількості 65535 оборотних елементів маємо 65025.

При $q = 3$ та $r = 11$ маємо $ord_r(q) = 5$. У цьому разі многочлен

$$x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + +x^5 + x^4 + +x^3 + x^2 + x + 1 =$$
$$= (x^5 - x^3 + x^2 - x - 1)(x^5 + x^4 - x^3 + x^2 - 1)$$

розкладається на два множники. Замість очікуваної кількості 118096 оборотних елементів маємо 117128.

При $q = 3$ та $r = 13$ маємо $ord_r(q) = 4$. У цьому разі многочлен

$$x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + +x^5 + x^4 + x^3 + x^2 + x + 1 =$$
$$= (x^3 - x - 1)(x^3 + x^2 - 1)(x^3 - x^2 - x - 1)(x^3 + x^2 + x - 1)$$

розкладається на чотири множники. Замість очікуваної кількості 1062882 оборотних елементів маємо 913952.

Маючи точну кількість елементів у групі $U(RG)$ та розклад цього числа на прості множники, можна, на основі теореми Лагранжа для скінченних груп, виписати всі можливі порядки оборотних елементів. Це дозволить достатньо швидко знайти оборотний елемент великого (максимально можливого) порядку. Власне такі елементи потрібні для реалізації криптографічних примітивів у групових кільцях. При пошуку треба обчислювати великі степені оборотних елементів. Для цього слід використати швидкий алгоритм піднесення до степеня [1].

Висновки

Досліджено питання пошуку оборотних елементів для часткових групових кілець (утворених скінченним полем та скінченною циклічною групою). Розроблена програма в середовищі Python для обчислення різних степенів довільних елементів таких групових кілець. Користуючись цією програмою, отримано обчислювальні дані, які дозволили сформулювати припущення про точну кількість елементів у термінах кількості елементів відповідних поля та групи. Це дозволить при подальших дослідженнях з'ясувати, як знаходити в групових кільцях оборотні елементи, які б одночасно мали великий порядок. Власне такі

потрібні при побудові нещодавно запропонованих криптосистем. Публікацій у цьому напрямку є невелика кількість.

Література

1. Galbraith S. D. Mathematics of Public Key Cryptography / S. D. Galbraith. – New York: Cambridge University Press, 2012. – 630 p.

2. Hurley B. Group ring cryptography / B. Hurley, T. Hurley // Int. J. Pure Appl. Math. – 2011. – Vol. 69, No. 1. – P. 67–86.

3. Hurley T. Group rings for communications / T. Hurley // Int. J. Group Theory. – 2015. – Vol. 4, No. 4. – P. 1–23. DOI: https://doi.org/10.22108/IJGT.2015.5453

4. Inam S. A New ElGamal-like Cryptosystem Based on Matrices over Groupring / S. Inam, R. Ali // Neural Computing and Applications. – 2018. – Vol. 29. – P. 1279-1283. DOI: https://doi.org/10.1007/s00521-016-2745-2

5. Mittal G., Kumar Sunil, Narain S., Kumar Sandeep. Group ring based public key cryptosystems / G. Mittal, Sunil Kumar, S. Narain, Sandeep Kumar / Journal of Discrete Mathematical Sciences and Cryptography. – 2022. – Vol. 25, Issue 6. P. 1–22. DOI: https://doi.org/10.1080/09720529.2020.1796868

6. Mullen G. Handbook of Finite Fields / G. Mullen, D. Panario. – Boca Raton: CRC Press, 2013. – 1048 p.

References

1. Galbraith S. D. Mathematics of Public Key Cryptography / S. D. Galbraith. – New York: Cambridge University Press, 2012. – 630 p.

2. Hurley B. Group ring cryptography / B. Hurley, T. Hurley // Int. J. Pure Appl. Math. – 2011. – Vol. 69, No. 1. – P. 67–86.

3. Hurley T. Group rings for communications / T. Hurley // Int. J. Group Theory. – 2015. – Vol. 4, No. 4. – P. 1–23. DOI: https://doi.org/10.22108/IJGT.2015.5453

4. Inam S. A New ElGamal-like Cryptosystem Based on Matrices over Groupring / S. Inam, R. Ali // Neural Computing and Applications. – 2018. – Vol. 29. – P. 1279-1283. DOI: https://doi.org/10.1007/s00521-016-2745-2

5. Mittal G., Kumar Sunil, Narain S., Kumar Sandeep. Group ring based public key cryptosystems / G. Mittal, Sunil Kumar, S. Narain, Sandeep Kumar / Journal of Discrete Mathematical Sciences and Cryptography. – 2022. – Vol. 25, Issue 6. P. 1–22. DOI: https://doi.org/10.1080/09720529.2020.1796868

6. Mullen G. Handbook of Finite Fields / G. Mullen, D. Panario. – Boca Raton: CRC Press, 2013. – 1048 p.