УДК 681.322

Б. Р. Попович
Національний університет "Львівська політехніка",
кафедра спеціалізованих комп'ютерних систем

КОМП'ЮТЕРНА ПЕРЕВІРКА ПРИПУЩЕННЯ ГАО, ПОВ'ЯЗАНОГО З ОТРИМАННЯМ ЕЛЕМЕНТІВ ВЕЛИКОГО ПОРЯДКУ В СКІНЧЕННИХ ПОЛЯХ

Виконано комп'ютерні обчислення в середовищі Maple для перевірки припущення Гао у випадку скінченних полів характеристики 2, 3, 5 та наведено відповідні результати. Якщо це припущення справедливе, то можна явно збудувати в цих полях за поліноміальний час елементи великого мультиплікативного порядку, що використовуються в криптографії (протокол Діффі-Хелмана, криптосистема Ель-Гамаля з відкритим ключем, цифровий підпис Ель-Гамаля).

Ключові слова: криптографічний захист інформації, скінченне поле, мультиплікативний порядок

B. Popovych
Lviv Polytechnic National University,
specialized computer system department

COMPUTER VERIFICATION OF GAO ASSUMPTION, RELATED WITH OBTAINING OF HIGH ORDER ELEMENTS IN FINITE FIELDS

We have performed computer calculations in Maple environment for verification of Gao assumption for finite fields of characteristic 2, 3, 5 and presented correspondent results. If the assumption is true, then it is possible to construct explicitly in these fields in polynomial time elements of high multiplicative order that are used in cryptography (Diffie-Hellman protocol, El-Gamal public key cryptosystem, El-Gamal digital signature).

Key words: cryptographic information protection, finite field, multiplicative order

Вступ

Забезпечення конфіденційності, цілісності та автентичності інформації, криптографічний захист інформаційних зв'язків між компонентами сучасних комп'ютерних систем є актуальною задачею. У роботі розглянемо один з аспектів захисту інформації, пов'язаний з використанням певних алгебраїчних структур, які називають скінченними полями, або полями Галуа [5, 6].

Окреслення проблеми

Скінченне поле з q елементів позначаємо через F_q, а через F_{q^n} – розширення поля F_q степеня n. Твірні мультиплікативної групи $F_{q^n}^*$ називають примітивними елементами. Далі використано такі позначення: m – найближче більше ціле число до величини $\log_q n$, $l = q^m$

найменший степінь q,що більший або дорівнює n, $d = 2m$, t – найближче менше ціле число до величини $\log_d n$.

Відкрите питання: знайти ефективний алгоритм побудови примітивних елементів у скінченних полях. Алгоритм ефективний, якщо він поліноміальний, тобто час його виконання дорівнює $\log(q^n)^{O(1)}$ арифметичних операцій у F_{q^n}. Сьогодні задача ефективної побудови примітивного елемента заданого скінченного поля є обчислювально важкою [6]. Тому розглядають менш претензійне питання: збудувати елемент доказово великого мультиплікативного порядку. Визначення Гао [4]: під елементами "великого порядку" в F_{q^n} розуміємо елементи, мультиплікативні порядки яких повинні бути більші від будь-якого полінома від $\log(q^n)$, де q^n прямує до нескінченності. У цьому випадку не вимагається обчислити точний порядок елемента: достатньо отримати нижню оцінку для порядку.

Області застосування елементів великого порядку в скінченних полях є такими [5, 6]: криптографія (протокол Діффі–Хелмана, криптосистема Ель-Гамаля з відкритим ключем, цифровий підпис Ель-Гамаля); завадостійке кодування (зокрема, при побудові БЧХ-кодів); генератори псевдовипадкових чисел (різні степені елемента великого порядку можна розглядати як послідовність псевдовипадкових чисел); доведення простоти чисел [1]. Застосування елементів великого мультиплікативного порядку в криптографії ґрунтується на так званій задачі дискретного логарифмування в будь-якій скінченній циклічній групі.

Питання побудови елементів великого мультиплікативного порядку розглядають як для загальних [3, 4, 10], так і для часткових [2, 8, 9] випадків скінченних полів.

Завдання дослідження

Гао [4] дав алгоритм побудови елементів великого порядку для загальних розширень F_{q^n} скінченних полів F_q. Вказаний підхід ґрунтується на запропонованому ним, але ще не доведеному припущенні.

Припущення. *Для довільного натурального числа* n *існує поліном* $g(x) \in F_q[x]$ *степеня щонайбільше* $d = 2m$ *такий, що* $x^{\bar{n}} - g(x)$ *має нерозкладний дільник* $f(x)$ *степеня* n.

Наведене припущення перевірене в [4] для $q = 2$ та $n \le 300$. Як бачимо, відомі обчислювальні дані підтверджують припущення лише для скінченних полів характеристики два, а для характеристики, більшої, ніж два, такі дані в літературі не наведені. Можливим поясненням є те, що для полів характеристики два доступні детальні таблиці нерозкладних над такими полями поліномів.

Отже, припущення Гао має слабке обчислювальне підкріплення. Завданням роботи є аналіз суттєвих моментів підходу Гао та виконання комп'ютерних обчислень, які підтвердили б справедливість згаданого припущення для значно більшої кількості випадків.

Розв'язання задачі

Проаналізуємо суттєві моменти підходу Гао. Схематично його проілюстровано на рис. 1. Центральним елементом у цій схемі є елемент розширеного поля, що дорівнює x. Щоб конкретно задати скінченне поле з q^n елементів крім q та n, слід задати нерозкладний над F_q поліном $f(x)$ степеня n. Відомо [5, 6], що його вибір неоднозначний. Власне підхід Гао полягає в наступному: вибрати поліном $f(x)$ так, щоб він ділив „зручний" поліном $x^l - g(x)$. Чи можна це завжди зробити, залишається на сьогодні відкритим питанням. Щоб вибрати поліном $f(x)$, слід отримати й поліном $g(x)$.

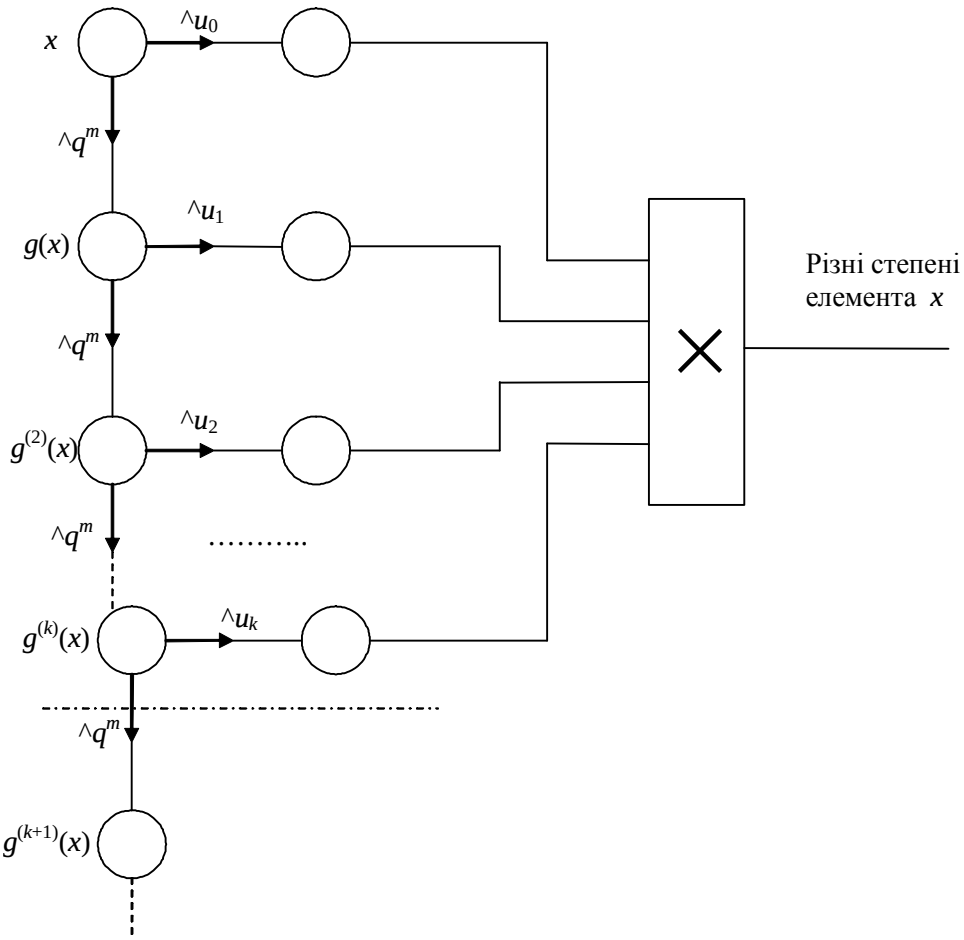

Рис. 1. Утворення різних степенів елемента x за методом Гао

Неважко показати, використовуючи властивості елементів поля F_{q^n}, що для будь-якого полінома $H(x)=\sum_{i=0}^{s} h_i x^i$ з коефіцієнтами з поля F_q справедлива рівність $(H(x))^{\overline{n}} = H(g(x))$.

За цією рівністю утворюємо з елемента $x = g^{(0)}(x)$ піднесенням до степеня l елемент $g(x) = g^{(1)}(x)$. Потім утворюємо з останнього піднесенням до степеня l елемент $g(g(x)) = g^{(2)}(x)$. Продовжуючи, отримуємо нескінченну послідовність елементів $g^{(i)}(x), i = 0,1,\ldots$. У праці [4] доведено, що всі елементи цієї послідовності є мультиплікативно незалежними. З них беремо лише перші k, де k задовольняє умову $d^k < n$. Виконання останньої умови необхідне, бо з перших k елементів утворюємо усі можливі добутки степеня, меншого за n. Оскільки кільце $F_q[x]$ має однозначний розклад на прості множники, то всі утворені добутки різні, а отже, вони різні й за модулем полінома $f(x)$, тобто в полі F_{q^n}. Очевидно, що всі вони є степенями елемента x. Залишається оцінити їх кількість. Це відома комбінаторна задача знаходження кількості розв'язків лінійного діофантового рівняння. Найкраще відому сьогодні нижню межу для кількості розв'язків наведено в [7]. Її модифікацію $\binom{n+t-1}{t}\prod_{i=0}^{t-1}\frac{1}{d^i}$ для побудови елементів великого порядку отримано в [10]. Слабшу (але більш явну) оцінку $n^{\frac{\log_q n}{4\log_q d}-\frac{1}{2}}$ наведено в праці [4].

Можна зробити висновок, що ключовим моментом у підході Гао є виконання припущення про існування відповідного полінома $g(x)$. Тому перевірка припущення Гао для скінченних полів різних характеристик (а не тільки характеристики, що дорівнює 2) є важливою.

Для перевірки нами виконано обчислення як для скінченних полів характеристики 2 (для $q=2$ та $300<n\le 525$), так і більшої характеристики (для $q=3$ та $n\le 300$, для $q=5$ та $n\le 100$). Гіпотеза Гао підтверджена і для цих випадків. Деякі з отриманих результатів наведено в таблиці (можна порівняти з табл. 1 з праці [4]).

Поліном $g(x)\in F_q[x]$ (q=2,3,5) найменшого степеня такий, що $x^l-g(x)$ має нерозкладний дільник степеня n

q	n	l	$g(x)$	q	n	l	$g(x)$
2	301	2^9	$x^{10}+x^9+x^8+x^7+x^6+x^2+1$	3	111	3^5	x^6+2x^2+x+2
2	314	2^9	$x^9+x^7+x^6+x^5+x^3+x^2+x+1$	3	112	3^5	x^4+x^3+2x+1
2	325	2^9	$x^7+x^5+x^3+1$	3	113	3^5	$x^5+x^4+2x^3+2x+1$
2	337	2^9	$x^8+x^7+x^5+x^3+x^2+1$	3	114	3^5	$2x^5+x^3+x+1$
2	349	2^9	$x^7+x^6+x^4+x+1$	3	210	3^5	$x^7+x^4+2x^3+2$
2	356	2^9	$x^9+x^7+x^6+x^4+x^3+x^2+1$	3	261	3^6	$x^7+x^6+x^5+x^4+x^3+x^2+2x+1$
2	361	2^9	$x^6+x^4+x^2+x+1$	3	273	3^6	$x^5+x^3+x^2+x+1$
2	365	2^9	$x^9+x^7+x^6+x^5+x^3+1$	3	281	3^6	x^4+x^2+2x+1
2	370	2^9	$x^9+x^6+x^5+x^4+x^3+1$	3	287	3^6	$x^5+x^3+x^2+1$
2	389	2^9	$x^8+x^4+x^3+x^2+1$	3	295	3^6	x^5+1
2	400	2^9	$x^9+x^8+x^6+x^5+x^4+x+1$	3	296	3^6	$2x^5+x^2+2$
2	403	2^9	$x^{10}+x^9+x+1$	3	297	3^6	$x^7+2x^5+x^2+2$
2	411	2^9	$x^{11}+x^{10}+x^9+x^8+x^5+x^3+x^2+x+1$	3	298	3^6	$2x^7+x^4+x^3+x^2+1$
2	412	2^9	$x^7+x^5+x^3+x^2+x+1$	3	300	3^6	$x^6+x^4+x^3+2x^2+1$
2	413	2^9	x^9+x^7+x+1	5	11	5^2	x^2+3
2	414	2^9	$x^8+x^6+x^5+x^4+1$	5	16	5^2	x^3+2x+2
2	415	2^9	$x^5+x^3+x^2+x+1$	5	19	5^2	x^3+1
2	416	2^9	x^7+x^6+1	5	22	5^2	x^2+x+1
2	470	2^9	$x^{10}+x^8+x^6+x^5+x^4+x^2+1$	5	25	5^2	$2x^3+2x+1$
2	471	2^9	$x^7+x^6+x^5+x^3+1$	5	37	5^3	x^3+4x+1
2	472	2^9	$x^9+x^7+x^5+x^4+x^3+x^2+x+1$	5	49	5^3	x^4+x^2+1
2	473	2^9	$x^{10}+x^5+x^3+x+1$	5	63	5^3	x^5+2x^3+x+2
2	474	2^9	$x^{10}+x^7+x^3+x^2+x+1$	5	80	5^3	x^3+1
2	501	2^9	$x^{10}+x^6+x^3+x+1$	5	87	5^3	x^5+x^4+2x+3
2	510	2^9	$x^8+x^6+x^4+x^3+x^2+x+1$	5	93	5^3	$2x^3+4x+1$
2	517	2^{10}	$x^{11}+x^8+x^7+x^6+x^5+x^4+x^3+x+1$	5	97	5^3	x^4+3x^2+4x+3
2	525	2^{10}	$x^7+x^3+x^2+1$	5	100	5^3	$x^5+x^4+2x^2+3$

Зокрема, з таблиці видно, що для випадку $q=p=2$, $n=525$ маємо $l=2^{10}=1024$ та $x^l-g(x)=x^{1024}-(x^7+x^3+x^2+1)$. Многочлен $x^l-g(x)$ розкладається на множники степеня 525, 51, 448. Множник $f(x)$ степеня 525 має 252 ненульові коефіцієнти. Елемент x є елементом великого порядку в скінченному полі $F_2[x]/(f(x))$ із 2^{525} елементів.

Для $q=p=3$, $n=298$ маємо $l=3^6=729$, $x^l-g(x)=x^{729}-(2x^7+x^4+x^3+x^2+1)$. Многочлен $x^l-g(x)$ розкладається на множники степеня 10, 310, 298, 22, 25, 4, 60. Множник $f(x)$ степеня 298 має 190 ненульових коефіцієнтів. Елемент x є елементом великого порядку в скінченому полі $F_3[x]/(f(x))$ із 3^{298} елементів.

Для перевірки гіпотези використано середовище Maple 13, зокрема функцію Factors (a) mod p. Ця функція обчислює розклад полінома a над простим полем характеристики p на нерозкладні множники. Тобто, це середовище взято тому, що в ньому є готова функція розкладу поліномів над

полем на прості множники. Самому реалізувати такий алгоритм є досить проблематичним. Приклад вікна середовища з отриманим результатом наведено на рис. 2.

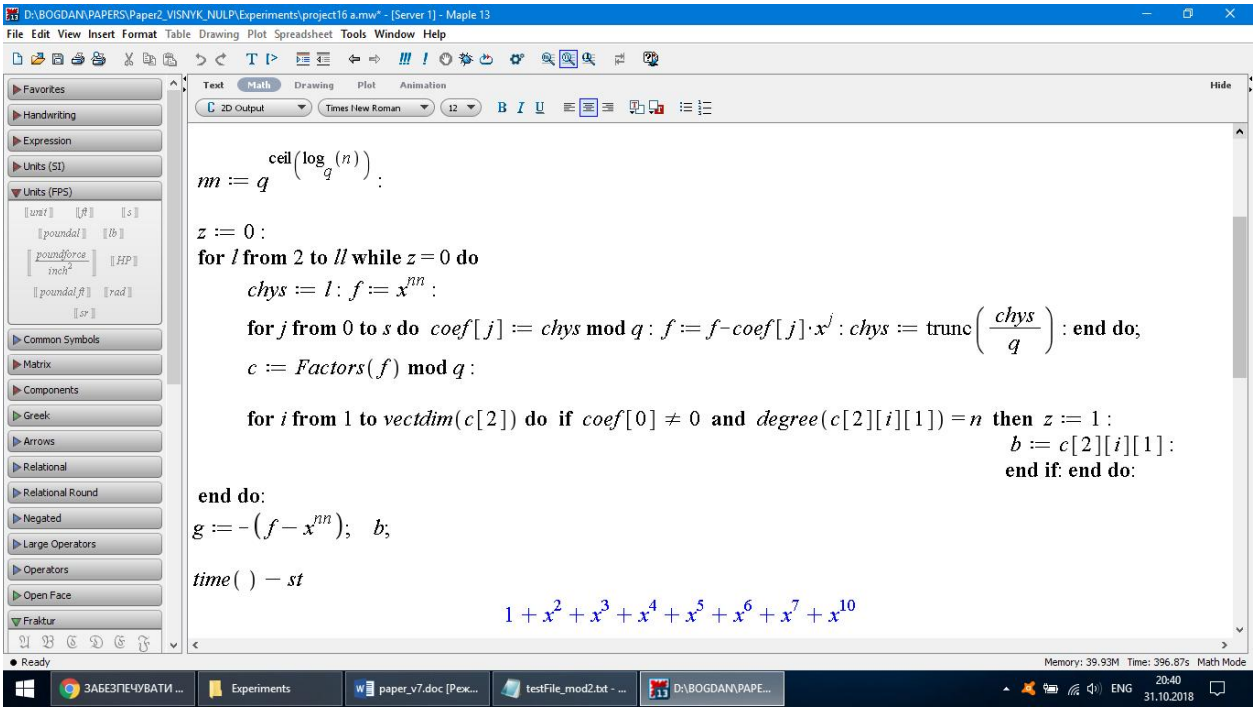

Рис. 2. Вікно середовища Maple з обчисленим поліномом $g(x)$

Висновки

Проаналізовано особливостей підходу Гао, який при справедливості певного припущення дає поліноміальний алгоритм побудови елементів великого порядку в мультиплікативній групі довільного скінченного поля. Такі елементи використовують у низці криптографічних примітивів (протокол Діффі–Хелмана, криптосистема Ель-Гамаля з відкритим ключем, цифровий підпис Ель-Гамаля). Виконано комп'ютерні обчислення, які підтвердили справедливість згаданого припущення для значно більшої кількості випадків, ніж це було відомо раніше.

1. Agrawal M., Kayal N., Saxena N. PRIMES is in P // Annals of Mathematics, vol. 160, no. 2, 2004, p. 781–793. 2. Ahmadi O., Shparlinski I. E., Voloch J. F.Multiplicative order of Gauss periods // International Journal of Number Theory, vol. 6, no. 4, 2010, p. 877 – 882. 3. Conflitti A. On elements of high order in finite fields // in Cryptography and Computational Number Theory, vol. 20 of Progr. Comput. Sci. Appl. Logic, Birkhauser, Basel, 2001, p. 11–14. 4. Gao S. Elements of provable high orders in finite fields // Proceeding of American Math. Soc., vol. 127, no. 6, 1999, p. 1615–1623. 5. Lidl R., Niederreiter H. Finite Fields. – Cambridge: Cambridge University Press, 1997. – 755 P. 6. Mullen G. L., Panario D. Handbook of finite fields. – Boca Raton: CRC Press, 2013. – 1068 P. 7. Lambe T. A. Bounds on the Number of Feasible Solutions to a Knapsack Problem // SIAM Journal of Applied Mathematics, vol. 26, no. 2, 1974, p. 302–305. 8. Popovych R. Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$ // Finite Fields and Their Applications, vol. 18, no. 4, 2012, p. 700–710. 9. Popovych R. Elements of high order in finite fields of the form $F_q[x]/(x^m-a)$ // Finite Fields and Their Applications, vol. 19, no. 1, 2013, p. 86–92. 10. Popovych R. On elements of high order in general finite fields // Algebra and Discrete Mathematics, vol. 18, no. 2, 2014, p.295–300.