УДК 512.624

Р. Б. Попович

# ПОБУДОВА ЕЛЕМЕНТІВ ВЕЛИКОГО ПОРЯДКУ В СКІНЧЕННИХ ПОЛЯХ ЗАГАЛЬНОГО ВИГЛЯДУ

*Розглянуто можливі варіанти побудови елементів великого мультиплікативного порядку в розширеннях скінченних полів загального вигляду без будь-яких недоведених припущень.*

Відомо, що мультиплікативна група скінченного поля є циклічна. Твірну цієї групи називають примітивним елементом. Ефективно побудувати примітивний елемент для заданого скінченного поля в обчислювальній теорії скінченних полів важко. Ось чому розглядають менш обмежувальне питання: знайти елемент великого мультиплікативного порядку [10]. У цьому випадку не вимагають обчислити точний порядок елемента: достатньо отримати нижню межу для порядку. Елементи великого порядку потрібні для низки застосувань, які, зокрема, охоплюють криптографію, теорію кодування, генератори псевдовипадкових чисел та комбінаторику.

Як $F_q$ позначимо поле з $q$ елементів, де $q$ – степінь простого числа $p$.

Відомо дуже мало результатів, коли жодне обмеження не накладене на степінь розширення поля. Гао [7] дав алгоритм побудови елементів великого порядку для загальних розширень $F_{q^m}$ скінченного поля $F_q$ з нижньою межею для порядку $\exp(\Omega((\log m)^2/\log\log m))$. Його алгоритм припускає виконання певної правдоподібної, але досі не доведеної гіпотези. Більш точно підхід з праці [7] спирається на таке припущення.

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

Зауважимо, що наведені обчислювальні дані [7] підтверджують гіпотезу лише для полів характеристики два, а для більшої від двох такі дані в літературі відсутні. Конфлітті [6], спираючись на вказану гіпотезу, виконав точніший аналіз результатів з праці [7]. Волох [14, 15] запропонував метод побудови елементів порядку принаймні $\exp(\Omega(\log m)^2))$ у скінченних полях на основі еліптичних кривих.

Для часткових скінченних полів можна збудувати елементи з набагато більшими порядками. Розширення, пов'язані з поняттям гауссового періоду, розглядали раніше [2, 4, 8, 11]. Нижня межа для порядку дорівнює $\exp(\Omega(\sqrt{m}))$. Ці розширення існують для нескінченної кількості чисел $m$, якщо для числа $q$ виконується гіпотеза Артіна (див. [5]). Розширення на основі поліномів Куммера розглянуто в працях [4, 12]. Узагальнення останніх наведено в [5]. Розширення існують для нескінченної кількості чисел $m$ без виконання будь-яких припущень.

Нижче розглядаємо можливі варіанти побудови елементів великого мультиплікативного порядку в скінченних полях загального вигляду. На відміну від досліджень [6, 7] не спираємося на жодну недоведену гіпотезу. Для отримання нижніх меж, зокрема, застосовуємо ABC теорему Стовера–Мейсона [3]. Наші основні результати – це теореми 4, 6.

Розглядаємо скінченне поле загального вигляду

$$F_{q^n} = F_q[x]/(f(x)),$$

де поліном $f(x)$ – нерозкладний над початковим полем $F_q$ та $\deg f(x)=n$. Через $\theta$ позначаємо клас елемента $x$ у вказаному фактор-кільці, яке є полем. Оскільки елемент $\theta$ задає розширення поля $F_q$ степеня $n$, то $\theta$ не може бути коренем ніякого полінома з коефіцієнтами з $F_q$ степеня, меншого за $n$.

Справедлива така теорема.

**Теорема** 1. Елемент $\theta$ має мультиплікативний порядок принаймні $n$.

Д о в е д е н н я. Покажемо, що елементи $1,\theta,\ldots,\theta^{n-1}$ є попарно різними. Припустимо, що це не так. Тоді для деяких $0\le i<j\le n-1$ виконується рівність $\theta^i=\theta^j$, тобто $\theta^{j-i}=1(\mathrm{mod}\ f(x))$. Оскільки $j-i<n=\deg f(x)$, то $x^{j-i}-1=0$. Таким чином, $\theta$ є коренем тотожно не рівного нулю полінома $x^{j-i}-1$ з коефіцієнтами з $F_q$ степеня щонайбільше $n-1$. Отримуємо суперечність, що завершує доведення теореми.

Насправді можемо збудувати для поля $F_{q^n}=F_q[x]/(f(x))$ багато елементів з мультиплікативним порядком принаймні $n$.

**Теорема** 2. Нехай $b$ – довільний ненульовий елемент скінченного поля $F_q$. Тоді $\theta+b$ має мультиплікативний порядок принаймні $n$.

Д о в е д е н н я. Покажемо, що елементи $1,\theta+b,\ldots,(\theta+b)^{n-1}$ є попарно різні. Припустимо, що це не так. Тоді для деяких $0\le i<j\le n-1$ виконується рівність $(\theta+b)^i=(\theta+b)^j$. Таким чином, $\theta$ є коренем тотожно не рівного нулю полінома $(x+b)^{j-i}-1$ з коефіцієнтами з $F_q$ степеня щонайбільше $n-1$. Отримуємо суперечність, що й завершує доведення теореми.

Згідно з працею [9, теорема 3.86] справедлива така теорема.

**Теорема** 3. Нехай $F_q$ – скінченне поле характеристики $p$. Для будь-якого цілого $n\ge 2$ такого, що $2n(n-1)$ не ділиться на $p$, нехай $T_n(q)$ позначає кількість елементів $a\in F_q$, для яких тричлен $x^n+x+a$ нерозкладний над $F_q$. Тоді існує така константа $B_n$, залежна лише від $n$, що

$$\left|T_n(q)-\frac{q}{n}\right|\le B_n\sqrt{q}\ .$$

Формулювання теореми 3 означає, що для більшості скінченних полів поліном, який задає поле, має вигляд $f(x)=x^n+x+a$. Тоді справедлива рівність $\theta^n=-(\theta+a)$.

Зауважимо, що теорема 3 не виконується для випадку $n=p$, який окремо розглянуто в праці [1] (розширення полів на основі поліномів Артіна–Шраєра). Показано, що можна явно збудувати елементи з мультиплікативним порядком принаймні $4^p$. Якщо $n$ ділиться на $p$ (але $n$ не збігається з $p$), тобто маємо розширення $F_{p^{p^t}}$ для деякого цілого числа $t$, то можемо, взявши підполе $F_{p^p}$, отримати елемент порядку принаймні $4^p$. Проте загальну ситуацію у цьому разі не розглянуто. Також не досліджено випадок, коли $n-1$ ділиться на $p$.

**Теорема** 4. Нехай скінченне поле має вигляд $F_{q^n} = F_q[x]/(x^n + x + a)$. Тоді $\theta$ має мультиплікативний порядок принаймні $\frac{(n-1)n}{2}$.

Д о в е д е н н я. Зрозуміло, що підгрупа, породжена елементом $\theta$, містить елементи $\theta, \ldots, \theta^{n-1}$ і, оскільки $\theta^n = -(\theta + a)$, також елементи $-(\theta + a), \ldots, (-1)^{n-1}(\theta + a)^{n-1}$.

Розглянемо множину з таких добутків цих елементів: $(-1)^j \theta^i (\theta + a)^j$, $i, j \geq 0, i + j \leq n - 1$. Покажемо, що всі добутки з наведеної множини різні.

Припустимо, що для деяких різних пар $(i_1, j_1)$ та $(i_2, j_2)$ таких, що $i_1, j_1 \geq 0, i_1 + j_1 \leq n-1$ та $i_2, j_2 \geq 0, i_2 + j_2 \leq n-1$, маємо однакові добутки, тобто $(-1)^{j_1} \theta^{i_1} (\theta + a)^{j_1} = (-1)^{j_2} \theta^{i_2} (\theta + a)^{j_2}$. Розглянемо можливі принципово різні випадки.

1) $i_1 > i_2, j_1 = j_2$.

Тоді $\theta$ є коренем тотожно не рівного нулю полінома $x^{i_1 - i_2} - 1$ з коефіцієнтами з $F_q$ степеня щонайбільше $n - 1$. Отримуємо суперечність.

2) $i_1 > i_2, j_1 > j_2$.

У цьому разі $\theta$ є коренем тотожно не рівного нулю полінома $(-1)^{j_1 - j_2} x^{i_1 - i_2} (x + a)^{j_1 - j_2} - 1$ з коефіцієнтами з $F_q$ степеня щонайбільше $n - 1$. Отримуємо суперечність.

3) $i_1 > i_2, j_1 < j_2$.

Тут $\theta$ є коренем полінома $x^{i_1 - i_2} - (-1)^{j_2 - j_1} (x + a)^{j_2 - j_1}$ з коефіцієнтами з $F_q$ степеня щонайбільше $n - 1$. Цей поліном тотожно не рівний нулю, оскільки при $i_1 - i_2 > j_2 - j_1$ його доданок найбільшого степеня дорівнює $x^{i_1 - i_2}$, при $j_2 - j_1 > i_1 - i_2$ – дорівнює $(-1)^{j_2 - j_1 + 1} x^{j_2 - j_1}$, а при $i_1 - i_2 = j_2 - j_1$ – дорівнює $-a x^{j_2 - j_1 - 1}$ для парного $j_2 - j_1$ та $2x^{j_2 - j_1}$ для непарного $j_2 - j_1$. Отримуємо суперечність.

Обчислимо тепер кількість цих добутків. Якщо зафіксуємо $0 \leq i \leq n - 1$, то $j$ може набувати значення від 0 до $n - i - 1$. Таким чином, загальна кількість добутків дорівнює сумі $\sum_{i=0}^{n-1} (n - i - 1) = \frac{(n-1)n}{2}$. Доведення завершене.

Початково ідея використання ABC теореми Стовера–Мейсона для підсилення оцінки для порядку певних мультиплікативних підгруп скінченних кілець висловлена в праці [13]. Далі цю думку розвинув Д. Бернштейн [3]. Пропозицію використати ABC теорему для поліпшення оцінки для порядку гауссового періоду навели як відкрите питання автори праці [2].

Згідно з працею [3, теорема 2.1] справедлива така теорема. Як звичайно $\operatorname{rad} L$ позначає найбільший вільний від квадратів зі старшим коефіцієнтом 1 дільник $L$, тобто, добуток всіх нерозкладних поліномів зі старшим коефіцієнтом 1, які ділять $L$.

**Теорема** 5. Нехай $K$ – поле, а $h$ – елемент додатного степеня з поліноміального кільця $K[x]$. Припустимо, що $1, 2, 3, \ldots, 3\deg h - 2$ є оборотними в полі $K$. Нехай $A, B, C$ – різні ненульові елементи з $K[x]$. Якщо $\gcd(A, B, C) = 1$ та $A \equiv B \equiv C \pmod h$, то

$\max\{\deg A, \deg B, \deg C\} > 2\deg h - \deg \operatorname{rad}(ABC)$.

У припущенні $p \geq 3n-1$ можна, застосувавши наслідок з ABC теореми [3], отримати кращу нижню оцінку для порядку елемента $\theta$.

**Теорема** 6. Нехай скінченне поле має вигляд

$$F_{q^n} = F_q[x]/(x^n + x + a)$$

та $p \geq 3n-1$. Тоді $\theta$ має мультиплікативний порядок принаймні

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

Д о в е д е н н я. Покладемо

$$K = F_{q^n} = F_q[x]/(h(x))$$

та $h(x) = x^n + x + a$. Елемент 1 тривіально має обернений у полі $K$. Якщо $p \geq 3\deg h - 1$, то елементи $2,3,...,3\deg h - 2$ також мають обернені в полі $K$. Згідно з теоремою 5, якщо $A, B, C$ – різні ненульові елементи поля $F_{q^n} = F_q[x]/f(x)$, для яких виконуються умови $\gcd(A,B,C) = 1$ та $A \equiv B \equiv C (\operatorname{mod} f(x))$, то $\max\{\deg A, \deg B, \deg C\} > 2n - \deg \operatorname{rad}(ABC)$.

Покладемо $u = x$ та $v = -(x + a)$. Зрозуміло, що $\gcd(u,v) = 1$, $\operatorname{rad}(uv) = x(x + a)$ та $\deg \operatorname{rad}(uv) = 2$.

Розглянемо множину з таких добутків елементів $u$ та $v$: $(-1)^j u^i v^j, i, j \geq 0, i + j \leq 2n - 2$.

Обчислимо кількість цих добутків. Якщо зафіксуємо $0 \leq i \leq 2n-2$, то $j$ може набувати значень від 0 до $2n-2-i$. Таким чином, загальна кількість добутків

$$\sum_{i=0}^{2n-2} (2n - i - 2) = \frac{(2n-1)(2n-2)}{2}.$$

Зрозуміло, що для будь-яких трьох добутків $A, B, C$ з вказаної множини маємо $\gcd(A,B,C) = 1$ та $\operatorname{rad}(ABC) = \operatorname{rad}(uv)$. Тоді $\deg \operatorname{rad}(ABC) = 2$. Згідно з теоремою 5 пари добутків із розглянутої множини можуть бути рівними за модулем $h(x) = x^n + x + a$, а жодна трійка добутків – не може бути рівною за модулем $h(x)$. Це означає, що кількість різних добутків з цієї множини за модулем $h(x)$ дорівнює в найгіршому випадку половині від загальної кількості добутків:

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

Отримали межу, наведену в формулюванні теореми.

На завершення зауважимо, що можна додатково використати для посилення нижньої межі для порядку елементів поля $F_{q^n} = F_q[x]/(x^n + x + a)$ елементи вигляду

$$(\theta + b)^{q^t} = \theta^{q^t} + b,$$

де $t > \lfloor \log_q n \rfloor$. Наприклад, при $q = 3$, $n = 100$, $t > 4$ такими елементами, зокрема, є $(\theta + b)^{3^5} = (\theta + a)^2 \theta^{43} + b$, $(\theta + b)^{3^6} = (\theta + a)^6 \theta^{86} + b$, $(\theta + b)^{3^7} = (\theta + a)^{20} \theta^{58} + b$.

1. *Попович Р.* Елементи великого порядку в розширеннях Артіна–Шраєра скінченних полів // Матем. студії – 2013. – 39, № 2 – С. 115–118.
2. *Ahmadi O., Shparlinski I. E., Voloch J. F.* Multiplicative order of Gauss periods // Int. J. Number Theory. – 2010. – 6, № 4 – P. 877–882.
3. *Bernstein D.* Sharper ABC-based bounds for congruent polynomials // J. Theor. Nombres de Bordeaux. – 2005. – 17, № 3 – P. 721–725.
4. *Cheng Q.* On the construction of finite field elements of large order // Finite Fields Appl. – 2005. – 11, № 3 – P. 358–366.
5. *Cheng Q., Gao S., Wan D.* Constructing high order elements through subspace polynomials // Discrete algorithms: Proc. 23rd ACM-SIAM Symp. (Kyoto, Japan, 17–19 January 2012). – Omnipress, Philadelphia, USA, 2011 – P. 1457–1463.
6. *Conflitti A.* On elements of high order in finite fields. // Cryptography and computational number theory: Proc. Workshop (Singapore, 22–26 November 1999). – Birkhauser, Basel, 2001. – P. 11–14.
7. *Gao S.* Elements of provable high orders in finite fields // Proc. Amer. Math. Soc. – 1999. – 127, № 6 – P. 1615–1623.
8. *Gathen J., Shparlinski I. E.* Orders of Gauss periods in finite fields // Appl. Algebra Engrg. Comm. Comput. – 1998. – 9, № 1 – P. 15–24.
9. *Lidl R., Niederreiter H.* Finite Fields. – Cambridge University Press, Cambridge, 1997. – 755 p.
10. *Mullen L., Panario D.* Handbook of finite fields. – CRC Press, London, 2013. – 1068 p.
11. *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$ // Finite Fields Appl. – 2012. – 18, № 4 – P. 700–710.
12. *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$ // Ibid. – 2013. – 19, № 1 – P. 86–92.
13. *Voloch J F.* On some subgroups of the multiplicative group of finite rings // J. Theor. Nombres de Bordeaux. – 2004. – 16, № 1 – P. 233–239.
14. *Voloch J. F.* On the order of points on curves over finite fields // Integers. – 2007. – 7 – A49.
15. *Voloch J. F.* Elements of high order on finite fields from elliptic curves // Bull. Austral. Math. Soc. – 2010. – 81, № 3 – P. 425–429.

**ПОСТРОЕНИЕ ЕЛЕМЕНТОВ БОЛЬШОГО ПОРЯДКА В КОНЕЧНЫХ ПОЛЯХ ОБЩЕГО ВИДА**

*Рассмотрены возможные варианты построения элементов большого мультипликативного порядка в расширениях конечных полей общего вида без каких-либо недоказанных предположений.*

**CONSTRUCTION OF HIGH ORDER ELEMENTS IN FINITE FIELDS OF GENERAL FORM**

*We consider possible variants of construction of high multiplicative order elements in finite field extensions of general form without any unproved assumptions.*

Нац. ун-т "Львівська політехніка", Львів

Одержано 10.09.13