УДК 512.624

Р. Б. Попович

ЕЛЕМЕНТИ ВЕЛИКОГО ПОРЯДКУ В РОЗШИРЕННЯХ АРТІНА-ШРАЄРА СКІНЧЕННИХ ПОЛІВ

R. B. Popovych. *Elements of high order in Artin-Shreier extensions of finite fields*, Mat. Stud. **39** (2013), 115–118.

We construct explicitly in any finite field of the form F_{p^p} elements with multiplicative order larger than 4^p.

Р. Б. Поповыч. *Элементы большого порядка в расширениях Артина-Шраера конечных полей* // Мат. Студії. – 2013. – Т.39, №2. – С.115–118.

В конечных полях F_{p^p} построены в явном виде элементы мультипликативного порядка большего чем 4^p.

Добре відомо, що задача ефективної побудови примітивного елемента заданого скінченого поля є серед важких задач обчислювальної теорії скінченних полів. Тому шукають відповідь на таке питання за менших обмежень: знайти елемент великого мультиплікативного порядку. У цьому випадку достатньо отримати нижню границю для такого порядку. Потреба в елементах великого порядку виникає у таких застосуваннях як теорія кодувань, генератори псевдовипадкових чисел та комбінаторика. Елементи великого порядку також використовують в алгоритмі AKS доведення простоти чисел, запропонованому М. Агравалом, Н. Кайалом та Н. Саксеною ([1]).

С. Гао ([5]) запропонував алгоритм побудови елементів великого порядку для багатьох (згідно з висловленою ним, проте не доведеною, *гіпотезою* для всіх) загальних розширень F_{q^m} скінченого поля F_q з нижньою границею для величини порядку $\exp(\Omega((\log m)^2/\log\log m))$. Й. Ф. Волох ([9]) запропонував метод побудови елементів порядку принаймні $\exp(\Omega(\log m)^2))$. Для часткових випадків скінченних полів можна побудувати елементи, що мають набагато більші порядки.

Розширення, пов'язані з поняттям гауссового періоду, розглянуті в [2, 7]. Нижня границя для величини порядку дорівнює $\exp(\Omega(\sqrt{m}))$. Розширення на основі поліномів Куммера мають вигляд $F_q[x]/(x^m - a)$. Їхні застосування в криптографії, зокрема, грунтуються на спарюванні. У [4] показано, як будувати елементи великого порядку в таких розширеннях за умови $q \equiv 1 (\mathrm{mod}\, m)$. У цьому випадку отримано нижню границю $\exp(\Omega(m))$. Елементи великого порядку побудовано в [8] для розширень на основі поліномів Куммера без умови $q \equiv 1 (\mathrm{mod}\, m)$. Нижня границя для величини мультиплікативного порядку дорівнює $\exp(\Omega(\sqrt[3]{m}))$.

2010 *Mathematics Subject Classification:* 11T30.
Keywords: finite field; multiplicative order.

Скінченне поле з q елементів позначаємо F_q. Групу, породжену елементом v, позначаємо $\langle v\rangle$. Кількість сполучень з n елементів по k елементів позначаємо $\binom{n}{k}$.

У цьому повідомленні в явному вигляді будуємо елементи великого порядку в розширеннях Артіна-Шраєра скінченних полів та даємо явну оцінку знизу для величини їхнього мультиплікативного порядку.

Беремо лінійний двочлен від елемента, який задає розширення, та всі його спряжені, що також належать до підгрупи, породженої цим двочленом, і будуємо різні їхні добутки. Усі спряжені вказаного лінійного двочлена також є лінійними двочленами. Ідею запропоновано П. Берізбейтіа ([3]) як вдосконалення алгоритму AKS ([1]) та розвинуто в [4] для розширень Куммера.

Для будь-якого простого числа p розширенням Артіна-Шраєра скінченого поля F_p є полем F_{p^p}. Відомо (див. [6]), що $x^p - x - a$ нерозкладний поліном над F_p для будь-якого ненульового елемента a з F_p. Тому з обчислювальної точки зору можна вважати, що $F_{p^p} = F_p[x]/(x^p - x - a)$. Нехай $\theta = x(\mathrm{mod}\ \ x^p - x - a)$. Зрозуміло, що $\theta^p = \theta + a$. Нескладно довести таку лему.

Лема 1. *Якщо $g(x)$ та $h(x)$ не дорівнюють один одному в $F_p[x]$ та їхні степені менші за p, то класи цих поліномів в $F_p[x]/(x^p - x - a)$ також є різними.*

Лема 2. *Для будь-якого ненульового елемента b поля F_p спряжені до елемента $\theta + b$ мають вигляд $\theta + b + ia$ для $i \in \{0, ..., p-1\}$.*

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

Доведемо, що $(\theta + b)^{p^i} = \theta + b + ia$ для будь-якого натурального i. Доведемо це індукцією по i.

Очевидно, що для $i = 0$ рівність виконується. Припустимо, що вона виконується для деякого i. Тоді для $i + 1$ маємо $(\theta + b)^{p^{i+1}} = [(\theta + b)^{p^i}]^p = (\theta + b + ia)^p = \theta^p + b + ia = \theta + b + (i+1)a$. Отже, рівність правильна для будь-якого натурального i. На завершення доведення зауважимо, що елементи $\theta + b + ia$ є попарно різними для $i \in \{0, ..., p-1\}$. □

Зафіксуємо цілі числа $1 \le c_- \le c \le p - 1$. Нехай $S(p, c_-, c)$ множина таких відображень f з множини $\{0, ..., p-1\}$ в множину цілих чисел, що:

I) $|\{i | f(i) < 0\}| = c_-$; II) $-\sum_{i,f(i)<0} f(i) \le c$; III) $\sum_{i,f(i)\ge 0} f(i) \le p - 1 - c$.

Лема 3. *Число елементів множини $S(p, c_-, c)$ дорівнює* $\binom{p}{c_-}\binom{c}{c_-}\binom{2p - c_- - c - 1}{p - c - 1}$.

Доведення. Щоб задати елемент множини $S(p, c_-, c)$ спочатку вибираємо місця, на яких значення відображення від'ємні — це враховує множник $\binom{p}{c_-}$. Далі вибираємо значення від'ємних елементів так, щоб сума їхніх абсолютних значень не перевищувала c — це враховує множник $\binom{c}{c_-}$. Нарешті вибираємо невід'ємні значення відображення f на $p - c_-$ місцях так, щоб їх сума не перевищувала $p - 1 - c$ — це враховує множник $\binom{p - c_- + p - 1 - c}{p - 1 - c}$. □

Лема 4. $S(p, c_-, c) > 4^p$ *для* $p \ge 41$.

Доведення. Покладемо $c_- = c = 2$. Тоді

$$S(p,\, c_-,\, c) = \binom{p}{2}\binom{2p-5}{p-3} > \frac{p(p-1)}{2}\binom{2(p-3)}{p-3}.$$

Використовуючи нерівність для центрального біномного коефіцієнта

$$\binom{2(p-3)}{p-3} \geq \frac{4^{p-3}}{2\sqrt{p-3}},$$

маємо

$$S(p,\, c_-,\, c) > \frac{p(p-1)}{256\sqrt{p-3}}4^p.$$

Оскільки $p(p-1) \geq 256\sqrt{p-3}$ для $p \geq 41$, то отримуємо $S(p,\, c_-,\, c) > 4^p$. □

Зауважимо, що для $2 \leq p < 41$ можна, використовуючи комп'ютерні обчислення, явно побудувати примітивний елемент поля F_{p^p}. Тому немає сенсу у цьому випадку розглядати такі оцінки, як у лемі 4.

Теорема. *Нехай $p \geq 41$. Для будь-якого ненульового елемента b поля F_p елемент $\theta + b$ поля F_{p^p} має порядок більший за 4^p.*

Доведення. За лемою 2 спряжені елемента $\theta + b$ (включаючи сам елемент $\theta + b$) мають вигляд $\theta + b + ia$ для $i \in \{0, \ldots, p-1\}$. Зрозуміло, що всі вони належать до підгрупи $\langle \theta + b \rangle$.

Нехай $S(p,\, c_-,\, c)$ — множина відображень f з множини $\{0, \ldots, p-1\}$ в множину цілих чисел з описаними раніше властивостями I, II, III. Для кожного елемента f з множини $S(p,\, c_-,\, c)$ утворюємо добуток $\prod_{0\leq i\leq p-1}(\theta + b + ia)^{f(i)}$, який також належить до $\langle \theta + b \rangle$. Стверджуємо, що двом різним елементам f та g з множини $S(p,\, c_-,\, c)$ відповідають різні добутки.

Доведемо це методом від супротивного. Припустимо, що елементи f та g різні, але відповідні до них добутки однакові

$$\prod_{0\leq i\leq p-1}(\theta + b + ia)^{f(i)} = \prod_{0\leq i\leq p-1}(\theta + b + ia)^{g(i)}. \tag{1}$$

Оскільки поліном $x^p - x - a$ є характеристичним поліномом для θ, то можемо записати

$$\prod_{0\leq i\leq p-1}(x + b + ia)^{f(i)} = \prod_{0\leq i\leq p-1}(x + b + ia)^{g(i)} (\mathrm{mod}(x^p - x - a)).$$

Тоді

$$\prod_{0\leq i\leq p-1,\, f(i)\geq 0}(x + b + ia)^{f(i)} \prod_{0\leq i\leq p-1,\, g(i)<0}(x + b + ia)^{-g(i)} =$$

$$= \prod_{0\leq i\leq p-1,\, f(i)<0}(x + b + ia)^{-f(i)} \prod_{0\leq i\leq p-1,\, g(i)\geq 0}(x + b + ia)^{g(i)} (\mathrm{mod}(x^p - x - a)). \tag{2}$$

Оскільки маємо поліном степеня

$$\sum_{0\leq i\leq p-1,\, f(i)\geq 0} f(i) + \sum_{0\leq i\leq p-1,\, g(i)<0}(-g(i)) \leq p - 1 < \deg(x^p - x - a)$$

у лівій частині та поліном степеня

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

у правій частині рівності (2), то за лемою 1 ці поліноми однакові як поліноми над F_p, тобто

$$\prod_{0\le i\le p-1,\, f(i)\ge 0} (x+b+ia)^{f(i)} \prod_{0\le i\le p-1,\, g(i)<0} (x+b+ia)^{-g(i)} =$$
$$= \prod_{0\le i\le p-1,\, f(i)<0} (x+b+ia)^{-f(i)} \prod_{0\le i\le p-1,\, g(i)\ge 0} (x+b+ia)^{g(i)}. \qquad (3)$$

У рівності (3) маємо нерозкладні та попарно різні множники $\theta+b+ia$, $i \in \{0, ..., p-1\}$. Ця рівність суперечить однозначності розкладу поліномів над полем F_p, що робить рівність (1) неможливою. Отже, добутки, які відповідають різним елементам множини $S(p,\, c_-,\, c)$, не можуть бути однаковими.

Тому, кількість різних розглянутих добутків, які належать до підгрупи $\langle\theta + b\rangle$, дорівнює кількості елементів у множині $S(p,\, c_-,\, c)$. За лемою 3 кількість елементів у множині $S(p,\, c_-,\, c)$ дорівнює

$$\binom{p}{c_-}\binom{c}{c_-}\binom{2p-c_--c-1}{p-c-1},$$

а за лемою 4 маємо $S(p,\, c_-,\, c) > 4^p$ для $p \ge 41$. Звідси випливає твердження теореми. □

ЛІТЕРАТУРА

1. Agrawal M., Kayal N., Saxena N. *PRIMES is in P*// Ann. of Math. – 2004. – V.160, №2. – P. 781–793.
2. Ahmadi O., Shparlinski I.E., Voloch J.F. *Multiplicative order of Gauss periods*// Int. J. Number Theory. – 2010. – V.6, №4. – P. 877–882.
3. Berrizbeitia P. *Sharpening Primes is in P for a large family of numbers*// Math. Comp. – 2005. – V.74, №252. – P. 2043–2059.
4. Cheng Q. *On the construction of finite field elements of large order*// Finite Fields Appl. – 2005. – V.11, №3. – P. 358–366.
5. Gao S. *Elements of provable high orders in finite fields*// Proc. Amer. Math. Soc. – 1999. – V.127, №6. – P. 1615–1623.
6. Lidl R., Niederreiter H., Finite Fields. – Cambridge University Press, 1997. – 755 p.
7. Popovych R. *Elements of high order in finite fields of the form* $F_q[x]/\Phi_r(x)$// Finite Fields Appl. – 2012. – V.18, №4. – P. 700–710.
8. Popovych R. *Elements of high order in finite fields of the form* $F_q[x]/(x^m - a)$// Finite Fields Appl. – 2013. – V.19, №1. – P. 86–92.
9. Voloch J.F. *Elements of high order on finite fields from elliptic curves*// Bull. Austral. Math. Soc. – 2010. – V.81. – P. 425–429.

Lviv Polytechnic National University
rombp07@gmail.com

Надійшло 15.05.2012