ISSN 2078-3744. Вісник Львів. ун-ту. Серія мех.-мат. 2013. Випуск 78. С. 141–147
Visnyk of the Lviv Univ. Series Mech. Math. 2013. Issue 78. P. 141–147

УДК 512.624

НИЖНЯ МЕЖА ДЛЯ ПОРЯДКУ ЕЛЕМЕНТІВ У РОЗШИРЕННЯХ СКІНЧЕННИХ ПОЛІВ ВИГЛЯДУ F_{p^p}

Роман ПОПОВИЧ

Національний університет "Львівська політехніка",
вул. Бандери, 12, Львів, 79013
e-mail: rombp07@gmail.com

Явно будуємо в скінченних полях вигляду F_{p^p} для $p \geq 2$ елементи великого мультиплікативного порядку.

Ключові слова: скінченне поле, мультиплікативний порядок.

У низці прикладних застосувань із використанням скінченних полів часто потрібні елементи великого порядку [8, 9]. В ідеалі хотілось би мати змогу отримувати примітивний елемент для будь-якого скінченого поля. Якщо не маємо розвинення порядку мультиплікативної групи поля на прості множники, невідомо як досягти мети. Тому розглядають менш претензійне питання: збудувати елемент доказово великого порядку. У цьому разі достатньо отримати нижню межу для порядку. Питання розглядають для загальних і для спеціальних скінченних полів. Скінченне поле з q елементів позначаємо F_q.

С. Гао [7] дав алгоритм побудови елементів великого порядку для багатьох (згідно з висловленою ним, проте не доведеною, гіпотезою для всіх) загальних розширень F_{q^n} скінченого поля F_q з нижньою границею для порядку $\exp(\Omega((\log m)^2/\log\log m))$. Й. Волох [12] запропонував метод побудови елементів порядку принаймні $\exp(\Omega(\log m)^2))$.

Для часткових випадків скінченних полів можна збудувати елементи, які мають набагато більші порядки.

Розширення, пов'язані з поняттям гауссівського періоду, розглянуті в [3, 10]. Нижня границя на порядок дорівнює $\exp(\Omega(\sqrt{m}))$. Розширення на підставі полінома Куммера набувають вигляду $F_q[x]/(x^m - a)$. Їх, зокрема, застосовують у криптографії, що ґрунтується на спарюванні. У [6] з'ясували, як будувати елементи великого порядку в таких розширеннях за умови $q \equiv 1 (mod\ m)$. У цьому разі отримано нижню границю $\exp(\Omega(m))$. Елементи великого порядку збудовано в [5] для розширень вигляду $F_q[x]/(x^{2^t} - a)$ та $F_q[x]/(x^{3^t} - a)$ без умови $q \equiv 1 (mod\ m)$. Нижні границі на

мультиплікативні порядки дорівнюють $\exp(\Omega(\log m)^2))$, де $m = 2^t$ та $m = 3^t$, відповідно. Повністю умова $q \equiv 1(mod\ m)$ для розширень вигляду $F_q[x]/(x^m - a)$ знята в [11].

Групу, породжену елементом v, позначаємо $\langle v \rangle$. Кількість сполучень з n елементів по k елементів позначаємо $\begin{pmatrix} n \\ k \end{pmatrix}$.

Явно будуємо елементи великого порядку в спеціальних розширеннях Артіна-Шраєра скінченних полів, подаємо явну оцінку знизу на їхній мультиплікативний порядок. Для будь-якого простого числа p розширенням Артіна-Шраєра скінченого поля F_p є поле F_{p^p}. Відомо [8, 9], 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 $\theta = x(mod\ x^p - x - a)$. Зрозуміло, що $\theta^p = \theta + a$.

Точніше, йдеться про таке. В [1] довели таке: коли $p \geq 41$, то для будь-якого ненульового елемента b поля F_p елемент $\theta + b$ поля F_{p^p} має порядок більший від 4^p. Ми знімаємо умову $p \geq 41$, тобто даємо оцінку знизу для порядків елементів вигляду $\theta + b$ для розширень Артіна-Шраєра з характеристикою $p \geq 2$. Для отримання результатів використовуємо теоретичні міркування та комп'ютерні обчислення.

Приймаємо лінійний двочлен від елемента, який задає розширення, та всі його спряжені, що також належать до підгрупи, породженої цим двочленом, і будуємо їхні різні добутки. Усі спряжені згаданого лінійного двочлена також є лінійними двочленами. Ідею запропонував П. Берізбейтіа [4] як вдосконалення алгоритму AKS [2] та розвинута в [6, 11] для розширень Куммера.

Нагадаємо, що для поля F_q характеристики p автоморфізм Фробеніуса – це відображення $\varphi : F_q \to F_q$, яке кожному елементу α з F_q ставить у відповідність елемент α^p [8, 9]. Два елементи α, β з F_q називаємо спряженими (над F_p), якщо

$$\alpha = \varphi^t(\beta)$$

для деякого степеня φ^t автоморфізму Фробеніуса.

Лема 1. *У випадку поля $F_{p^p} = F_p[x]/(x^p - x - a)$ спряжені елемента $\theta + b$ ($b \in F_p$) набувають вигляду $\theta + b + ia$ для $i = 0, ..., p - 1$.*

Доведення. Доведемо, що $(\theta + b)^{p^i} = \theta + b + ia$, що 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 $i + 1$ отримаємо

$$(\theta + b)^{p^{i+1}} = [(\theta + b)^{p^i}]^p = (\theta + b + ia)^p = \theta^p + b + ia = \theta + b + (i + 1)a.$$

Отже, рівність правильна для будь-якого натурального i. □

Варто зауважити, що елементи $\theta + b + ia$ є різними для $i = 0, ..., p - 1$.

Лема 2. *Всі елементи вигляду $\theta + b + ia$ ($i = 0, ..., p - 1$) мають однаковий мультиплікативний порядок.*

Доведення. Приймемо довільні два елементи α, β згаданого вигляду. Згідно з лемою 1 ці елементи спряжені. Тобто існує такий степінь φ^t автоморфізму Фробеніуса, що

$$\alpha = \varphi^t(\beta).$$

Зрозуміло, що φ^t також є автоморфізмом. Якщо φ^t – автоморфізм і $\beta^k = 1$, то тоді $\varphi^t(\beta^k) = \alpha^k = 1$. □

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) $\sum_{i,f(i)\ge 0} f(i) \le p-1-c$.

В [1] доведено таку лему.

Лема 3. *Число елементів множини* $S(p, c_-, c)$ *дорівнює*

$$\begin{pmatrix} p \\ c_- \end{pmatrix} \begin{pmatrix} c \\ c_- \end{pmatrix} \begin{pmatrix} 2p-c_--c-1 \\ p-c-1 \end{pmatrix}.$$

Наступна лема дає оцінку знизу для числа елементів множини $S(p, c_-, c)$.

Лема 4. $S(p, c_-, c) > 4^p$ *для* $p \ge 13$.

Доведення. Приймемо у визарі з леми 3 $c_- = c = 4$. Тоді

$$S(p,\, c_-,\, c) = \begin{pmatrix} p \\ 4 \end{pmatrix} \begin{pmatrix} 2p-9 \\ p-5 \end{pmatrix} > \frac{p(p-1)(p-2)(p-3)}{4} \begin{pmatrix} 2(p-5) \\ p-5 \end{pmatrix}.$$

Використовуючи нерівність для центрального біноміального коефіцієнта

$$\begin{pmatrix} 2(p-5) \\ p-5 \end{pmatrix} \ge \frac{4^{p-5}}{2\sqrt{p-5}},$$

одержимо

$$S(p,\, c_-,\, c) > \frac{p(p-1)(p-2)(p-3)}{4096\sqrt{p-5}} 4^p.$$

Позаяк $p(p-1)(p-2(p-3) \ge 4096\sqrt{p-5}$ для $p \ge 13$ (оскільки p – просте число, то значення 12 не враховуємо), то отримуємо $S(p,\, c_-,\, c) > 4^p$. □

Лема 5. *У випадку поля* F_{p^p} *мультиплікативнй порядок всіх елементів вигляду* $\theta + b$ $(b \in F_p)$ *дорівнює:*

3 для $p = 2$,

13 для $p = 3$,

781 для $p = 5$,

137257 для $p = 7$,

28531167061 для $p = 11$.

Доведення. Розглянемо відповідні скінченні поля та виконані в них комп'ютерні обчислення.

1. Випадок поля F_{2^2}.

Характеристика поля дорівнює $p = 2$. Згідно з виконаними комп'ютерними обчисленнями кількість елементів мультиплікативної групи поля дорівнює $2^2 - 1 = 3$ і мультиплікативнй порядок елемента $\theta - 3$. Тоді згідно з лемою 3 мультиплікативний порядок всіх елементів вигляду $\theta + b$ $(b \in F_p)$ також дорівнює 3.

2. Випадок поля F_{3^3}.

Характеристика поля дорівнює $p = 3$. Згідно з виконаними комп'ютерними обчисленнями кількість елементів мультиплікативної групи поля дорівнює $3^3 - 1 = 26$, а мультиплікативний порядок елемента $\theta - 13$. Тоді згідно з лемою 2 мультиплікативний порядок всіх елементів вигляду $\theta + b$ ($b \in F_p$) також дорівнює 13.

3. Випадок поля F_{5^5}.

Характеристика поля дорівнює $p = 5$. Згідно з виконаними комп'ютерними обчисленнями кількість елементів мультиплікативної групи поля дорівнює $5^5 - 1 = 3124$, а мультиплікативнй порядок елемента $\theta - 781$. Тоді згідно з лемою 2 мультиплікативний порядок всіх елементів вигляду $\theta + b$ ($b \in F_p$) дорівнює 781.

4. Випадок поля F_{7^7}.

Характеристика поля дорівнює $p = 7$. Згідно з виконаними комп'ютерними обчисленнями кількість елементів мультиплікативної групи поля дорівнює $7^7 - 1 = 823542$, а мультиплікативнй порядок елемента $\theta - 137257$. Тоді згідно з лемою 2 мультиплікативний порядок всіх елементів вигляду $\theta + b$ ($b \in F_p$) також дорівнює 137257.

5. Випадок поля $F_{11^{11}}$.

Характеристика поля дорівнює $p = 11$. Згідно з виконаними комп'ютерними обчисленнями кількість елементів мультиплікативної групи поля дорівнює $11^{11} - 1 = 285311670610$, а мультиплікативнй порядок елемента $\theta - 28531167061$. Тоді згідно з лемою 2 мультиплікативний порядок всіх елементів вигляду $\theta + b$ ($b \in F_p$) дорівнює 28531167061. □

Теорема 1. *а) Якщо $p = 2$, то елементи поля F_{2^2} вигляду $\theta + b$ ($b \in F_2$) мають порядок 3;*

б) якщо $p = 3$, то елементи поля F_{3^3} вигляду $\theta + b$ ($b \in F_3$) мають порядок 13;

в) якщо $p = 5$, то елементи поля F_{5^5} вигляду $\theta + b$ ($b \in F_5$) мають порядок 781;

г) якщо $p \geq 7$, то елементи поля F_{p^p} вигляду $\theta + b$ ($b \in F_p$) мають порядок більший від 4^p.

Доведення. З леми 5 випливають частини (а), (б) і (в) теореми. З леми 5 випливає також частина (г) для $p = 7$ (оскільки $4^7 < 137257$) та для $p = 11$ (оскільки $4^{11} < 28531167061$).

За лемою 4 отримаємо, що $S(p, c_-, c) > 4^p$ для $p \geq 13$. Звідси випливає твердження теореми. □

Комп'ютерні обчислення, описані в лемі 5, виконані на двоядерному процесорі Intel Pentium P6200 2,13 GHz у двох варіантах. У першому варіанті використано власну програму в середовищі Delphi. У другому варіанті для порівняння використано середовище Maple. В обидвох варіантах отримали однакові результати.

Оскільки не всі визнають доведення з застосуванням комп'ютерних обчислень, то подаємо також ескіз доведення леми 5 без комп'ютерних обчислень. Для цього достатньо взяти розклади відповідних порядків мультиплікативних груп скінченних полів на прості множники та обчислити степені елемента θ. Хоча ці результати отримали з використанням комп'ютерних обчислень, проте їх можна перевірити вручну. Зокрема, для піднесення до степеня можна використати відомий швидкий ("індійський") алгоритм послідовних піднесень до квадрата та множень.

Доведення леми 5 без застосування комп'ютерних обчислень. Розглянемо відповідні скінченні поля та порядки елементів у них.

1. Оскільки випадок поля F_{2^2} потребує нескладних обчислень, то їх не подаємо.

2. Випадок поля F_{3^3}.

Кількість елементів мультиплікативної групи поля дорівнює $26 = 2 \cdot 13$. Можна безпосередньо перевірити, що $\theta^{13} = 1$. Отож, мультиплікативний порядок елемента θ дорівнює 13. Тоді згідно з лемою 2 мультиплікативний порядок всіх елементів вигляду $\theta + b$ також дорівнює 13.

3. Випадок поля F_{5^5}.

Кількість елементів мультиплікативної групи поля дорівнює $3124 = 4 \cdot 11 \cdot 71$. Можна безпосередньо перевірити, що

$$\theta^{11} = \theta^3 + 2\theta^2 + \theta \neq 1,$$
$$\theta^{71} = 4\theta^4 + 2\theta^3 + 4\theta^2 + 3\theta + 1 \neq 1,$$
$$(\theta^{71})^{11} = 1.$$

Отже, мультиплікативний порядок елемента θ дорівнює $781 = 11 \cdot 71$. Тоді згідно з лемою 2 мультиплікативний порядок всіх елементів вигляду $\theta + b$ дорівнює 781.

4. Випадок поля F_{7^7}.

Кількість елементів мультиплікативної групи поля дорівнює $823542 = 2 \cdot 3 \cdot 29 \cdot 4733$. Можна безпосередньо перевірити, що

$$\theta^{29} = \theta^5 + 4\theta^4 + 6\theta^3 + 4\theta^2 + \theta \neq 1,$$
$$\theta^{4733} = \theta^6 + 5\theta^5 + 2\theta^4 + 5\theta^3 + 4\theta^2 + 2\theta + 5 \neq 1,$$
$$(\theta^{4733})^{29} = 1.$$

Отож, мультиплікативний порядок елемента θ дорівнює $137257 = 29 \cdot 4733$. Тоді згідно з лемою 2 мультиплікативний порядок всіх елементів вигляду $\theta + b$ також дорівнює 137257.

5. Випадок поля $F_{11^{11}}$.

Кількість елементів мультиплікативної групи поля дорівнює $285311670610 = 2 \cdot 5 \cdot 15797 \cdot 1806113$. Можна безпосередньо перевірити, що

$$\theta^{15797} = 2\theta^{10} + 3\theta^9 + 2\theta^8 + 3\theta^7 + 4\theta^6 + 8\theta^5 + 6\theta^4 + 4\theta^3 + 3\theta^2 + 8\theta \neq 1,$$
$$\theta^{18061137} = 3\theta^{10} + 4\theta^9 + 8\theta^8 + 8\theta^7 + 6\theta^6 + 7\theta^5 + \theta^4 + 5\theta^3 + 4\theta^2 + 6 \neq 1,$$
$$(\theta^{1806113})^{15797} = 1.$$

Отже, мультиплікативний порядок елемента θ дорівнює $28531167061 = 15797 \cdot 1806113$. Тоді згідно з лемою 2 мультиплікативний порядок всіх елементів вигляду $\theta + b$ дорівнює 28531167061.

Список використаної літератури

1. *Попович Р.* Елементи великого порядку в розширеннях Артіна-Шраєра скінченних полів / *Р. Попович* // Матем. студії. – 2013. – Т. 39, №2. – С. 115-118.
2. *Agrawal M.* PRIMES is in P. / *M. Agrawal, N. Kayal, N. Saxena* // Ann. of Math. – 2004. – Vol. 160, №2. – P. 781-793.
3. *Ahmadi O.* Multiplicative order of Gauss periods / *O. Ahmadi, I.E. Shparlinski, J.F. Voloch* // Int. J. Number Theory. – 2010. – Vol. 6, №4. – P. 877-882.

4. *Berrizbeitia P.* Sharpening Primes is in P for a large family of numbers / *P. Berrizbeitia* // Math. Comp. – 2005. – Vol. 74:252. – P. 2043-2059.
5. *Burkhart F.* Finite field elements of high order arising from modular curves / *F. Burkhart et al.* // Designs, Codes and Cryptography. – 2009. – Vol. 51, №3. – P. 301-314.
6. *Cheng Q.* On the construction of finite field elements of large order / *Q. Cheng* // Finite Fields Appl. – 2005. – Vol. 11, №3. – P. 358-366.
7. *Gao S.* Elements of provable high orders in finite fields / *S. Gao* // Proc. Amer. Math. Soc. – 1999. – Vol. 127, №6. – P. 1615-1623.
8. *Lidl R.* Finite Fields / *R. Lidl, H. Niederreiter.* – CRC Press, 2013. – 755 p.
9. *Mullen G.L.* Handbook of finite fields. / *G.L. Mullen, D. Panario.* – Cambridge University Press, 1997. – 1068 p.
10. *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$ / *R. Popovych* // Finite Fields Appl. – 2012. – Vol. 18, №4. – P. 1615-1623.
11. *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$ / *R. Popovych* // Finite Fields Appl. – 2013. – Vol. 19, №1. – P. 86-92.
12. *Voloch J.F.* Elements of high order on finite fields from elliptic curves / *J.F. Voloch* // Bull. Austral. Math. Soc. – 2010. – Vol. 81, №3. – P. 425-429.

Стаття: надійшла до редакції 10.10.2013
прийнята до друку 11.12.2013

LOWER BOUND FOR ELEMENTS ORDER IN FINITE FIELDS EXTENSIONS OF THE FORM F_{p^p}

Roman POPOVYCH

Lviv Polytechnic National University,
Bandery Str., 12, Lviv, 79013
e-mail: rombp07@gmail.coml

We construct explicitly in any finite field of the form F_{p^p} for $p \geq 2$ elements with high multiplicative order.

Key words: finite field, multiplicative order.

ISSN 2078-3744. Вісник Львів. ун-ту. Серія мех.-мат. 2013. Випуск 78

НИЖНЯЯ ГРАНИЦА ДЛЯ ПОРЯДКА ЭЛЕМЕНТОВ В РАСШИРЕНИЯХ КОНЕЧНЫХ ПОЛЕЙ ВИДА F_{p^p}

Роман ПОПОВЫЧ

Национальный университет "Львовская политехника",
ул. Бандеры, 12, Львов, 79013
e-mail: rombp07@gmail.com

Явно строим в конечных полях вида F_{p^p} для $p \geq 2$ элементы большого мультипликативного порядка.

Ключевые слова: конечное поле, мультипликативный порядок.