УДК 512.44

Р. Б. Попович (Нац. ун-т "Львівська політехніка")

НИЖНЯ МЕЖА ДЛЯ МУЛЬТИПЛІКАТИВНОГО ПОРЯДКУ ЕЛЕМЕНТІВ У ВЕЖАХ СКІНЧЕННИХ ПОЛІВ ХАРАКТЕРИСТИКИ $p \geq 3$

We construct explicitely in towers of finite fields of characreristic $p \geq 3$ elements of high multiplicative order.

Ми явно будуємо у вежах скінченних полів характеристики $p \geq 3$ елементи великого мультиплікативного порядку.

У низці прикладних застосувань із використанням скінченних полів часто потрібні елементи великого порядку [1,2]. В ідеалі хотілось би мати можливість отримувати примітивний елемент для будь-якого скінченого поля. Проте, якщо не маємо розкладу порядку мультиплікативної групи поля на прості множники, невідомо як досягти мети. Тому розглядають менш претензійне питання: збудувати елемент доказово великого порядку. У цьому разі досить отримати нижню межу для порядку. Питання розглядають як для загальних [3,4], так і для спеціальних скінченних полів: пов'язаних з поняттям Гауссового періоду [5,6], на основі поліномів Куммера [7–9], розширень Артіна-Шраєра [10]. Скінченне поле з q елементів позначаємо F_q.

Гао [3] дав алгоритм побудови елементів великого порядку для багатьох (при справедливості сформульованої ним гіпотези для всіх) загальних розширень F_{q^n} скінченних полів F_q з нижньою межею для порядку $\exp(\Omega((\log m)^2/\log\log m))$. Волох [4] запропонував метод, який дозволяє збудувати елемент порядку принаймні $\exp((\log m)^2)$ у скінченних полях на основі еліптичних кривих.

Для часткових випадків скінченних полів, можна збудувати елементи з більшими мультиплікативними порядками. Розширення, пов'язані з поняттям Гауссового періоду, розглянуто в [5,6]. Нижня оцінка для порядку елементів дорівнює $\exp(\Omega(\sqrt{m}))$. Розширення на основі поліномів Куммера мають вигляд $F_q[x]/(x^m - a)$. Їх, зокрема, використовують у криптографії, що грунтується на спарюванні. У [7] показано як збудувати елементи великого порядку в таких розширеннях при виконанні умови $q \equiv 1(mod\ m)$. У цьому разі отримано нижню межу $\exp(\Omega(m))$. Елементи великого порядку збудовано в [8] для розширень вигляду $F_q[x]/(x^{2^t} - a)$ та $F_q[x]/(x^{3^t} - a)$ без умови $q \equiv 1(modm)$. Нижні границі на мультиплікативні порядки дорівнюють $\exp(\Omega(\log m)^2))$, де відповідно $m = 2^t$ та $m = 3^t$. Умову $q \equiv 1(mod\ m)$ для розширень вигляду $F_q[x]/(x^m - a)$ повністю знято в [9]. Елементи великого порядку утворено в [10] для скінченних полів вигляду F_{p^p}.

У даній роботі явно будуємо елементи великого порядку в недвійкових ($p \geq 3$) рекурсивних розширеннях скінченних полів $F_{p^{p^r}}$, даючи оцінку знизу на їх мультиплікативний порядок. Різні варіанти таких розширень, зокрема, розглядалися в [11,12].

Більш точно, розглядаємо скінченні поля, які будуємо рекурсивно:
$E_1 = F_p(x_1)$, де елемент x_1 задовольняє рівняння

$$x_1^p - x_1 - 1 = 0;$$

$E_r = E_{r-1}(x_r)$, $r = 2, 3, ...$, де елемент x_r задовольняє рівняння

$$x_r^p - x_r - \prod_{i=0}^{r-1} x_i^{p-1} = 0.$$

Тобто, отримуємо таку вежу скінченних полів недвійкової характеристики:

$$F_p \subset E_1 = F_p(x_1) \subset E_2 = E_1(x_2) \subset ...$$

З прикладної точки зору такі побудови дуже привабливі, оскільки операції над елементами скінченого поля можна виконувати рекурсивно, а тому ефективно [11].

Зауважимо, що число елементів мультиплікативної групи E_r^* $(r = 1, 2, ...)$ дорівнює $p^{p^r} - 1$. Наприклад, при $p = 3$ маємо $|E_0^*| = 3^{3^1} - 1 = 26$, $|E_1^*| = 3^{3^2} - 1 = 19682 = 26 \cdot 757$.

Для довільних простого числа p та натурального числа n введемо числа вигляду

$$N_{p,r} = \frac{p^{p^r} - 1}{p^{p^{r-1}} - 1}.$$

З одного боку їх можна розглядати як узагальнення чисел Ферма [13]

$$N_{2,r} = \frac{2^{2^r} - 1}{2^{2^{r-1}} - 1} = 2^{2^{r-1}} + 1,$$

а з іншого боку - як узагальнення чисел вигляду $N_{p,1} = \frac{p^p - 1}{p-1}$, які є мінімальним періодом послідовності чисел Белла за модулем p [14]. Зауважимо, що

$$N_{p,r} = \sum_{i=0}^{p-1} (p^{p^{r-1}})^i.$$

Далі даємо в леммах 1-4 доведення допоміжних для даної роботи результатів.

Лема 1. *Для довільного натурального числа r справедлива така рівність*

$$p^{p^r} - 1 = (p-1) \prod_{i=1}^{r} N_{p,i}. \tag{1}$$

Доведення. Виконуємо індукцією по r. При $r = 1$ маємо справедливу рівність

$$p^p - 1 = (p-1)(1 + p + ... + p^{p-1}) = (p-1)N_{p,r}.$$

Припустимо, що рівність (1) справджується для $r = s - 1$, тобто

$$p^{p^{s-1}} - 1 = (p-1) \prod_{i=1}^{s-1} N_{p,i}. \tag{2}$$

Тоді $p^{p^s} - 1 = (p^{p^{s-1}} - 1)N_{p,s}$. Враховуючи (2), отримуємо, що рівність (1) виконується для $r = s$.

Лема 2. *Нехай p – просте число та p ділить q. Тоді числа $q-1$ та $\sum_{j=0}^{p-1} q^j$ взаємно прості.*

Доведення. Виконуємо методом від протилежного. Нехай t - спільний дільник чисел $q-1$ та $\sum_{j=0}^{p-1} q^j$. Тоді $q \equiv 1(mod\ t)$. Звідси маємо $\sum_{j=0}^{p-1} q^j \equiv p(mod\ t)$. Оскільки t ділить $\sum_{j=0}^{p-1} q^j$, то $t = p$. Отримуємо, що p одночасно ділить $q-1$ та q – суперечність.

Лема 3. *Числа $p-1$, $N_{p,1}$, $N_{p,2}, \ldots,$ є попарно взаємно простими.*

Доведення. Зауважимо, що згідно з рівністю (1) маємо $(p-1)N_{p,r-1} = p^{p^{r-1}} - 1$. Позначимо $q = p^{p^{r-1}} - 1$. Тоді $(p-1)N_{p,r-1} = q-1$ та $N_{p,r} = \sum_{i=0}^{p-1} q^i$. Зрозуміло, що p ділить q. Застосовуючи лему 2, отримуємо, що $q-1$ та $N_{p,r}$ взаємно прості. Тому взаємно простими є числа $N_{p,r-1}$ та $N_{p,r}$. Також взаємно простими є $p-1$ і $N_{p,r}$.

Лема 4. *Нехай r – довільне натуральне число та $u_r = \prod_{i=1}^{r} x_i$. Мультиплікативний порядок елемента u_r дорівнює $O(u_r) = \prod_{i=1}^{r} O(x_i)$.*

Доведення. Як наслідок з леми 3 маємо, що група E_r^* $(r = 1, 2, ...)$ є внутрішнім прямим добутком підгрупи F_p^* з $p-1$ елемента та підгруп з $N_{p,i}$ $(i = 1, ..., r)$ елементів. Елемент x_i належить до підгрупи порядку $N_{p,i}$. Значить, порядок елемента u_r дорівнює добутку порядків елементів x_i $(i = 1, ..., r)$.

Основні результати даної роботи даємо в теоремі 1 та теоремі 2.

Теорема 1. *Нехай p – непарне просте число. Тоді будь-який простий дільник числа $N_{p,r}$ має вигляд $2kp^r + 1$ для деякого натурального числа k.*

Доведення. Нехай q – просте число, яке ділить $N_{p,r}$. Позначимо $s = p^{p^{r-1}}$ та $t = sp - s$. Тоді $sp \equiv s \mod t$ та $s^i \equiv s \mod t$ для $i = 2, ..., p-1$. Маємо

$$N_{p,r} = 1 + \sum_{i=1}^{p-1} s^i \equiv 1 + \sum_{i=1}^{p-1} s = 1 + s(p-1) \equiv 1 \mod s.$$

Звідси $(N_{p,r}, s(p-1)) = 1$ і $(q, s(p-1)) = 1$. Число q непарне (бо є дільником непарного числа $N_{p,r}$) та $q \neq p^{p^{r-1}}$.

Оскільки $p^{p^{r-1}} \equiv 1 \mod N_{p,r}$ та $q | N_{p,r}$, то $p^{p^{r-1}} \equiv 1 \mod q$. Нехай d найменше натуральне число, для якого $p^d \equiv 1 \mod q$. Не може бути $d | p^{r-1}$, бо, виходячи з леми 3, q не ділить $p^{p^{r-l}} - 1$ для $l = 1, ..., r$. Але $d | p^r$ і тому $d = p^r$.

Згідно з малою теоремою Ферма $p^{q-1} \equiv 1 \mod q$. З цього випливає , що $p^r | q-1$. Відношення $(q-1)/p^r$ парне, бо числа p та q непарні. Таким чином, $q = 2kp^r + 1$ для деякого натурального k.

Теорема 2. *Нехай r – довільне натуральне число. Елемент $u_r = \prod_{i=1}^{r} x_i$ поля E_r має мультиплікативний порядок принаймні $\prod_{i=1}^{r}(2p^i + 1)$.*

Доведення. Згідно з лемою 4 $O(u_r) = O\left(\prod_{i=1}^{r} x_i\right) = \prod_{i=1}^{r} O(x_i)$. За теоремою Лагранжа для скінченних груп, $O(x_i)$ є дільником $N_{p,i}$. Тоді, виходячи з теореми 1, $O(x_i)$ має вигляд $2kp^i + 1 \geq 2p^i + 1$. Звідси отримуємо потрібний результат.

Як було зауважено раніше, елемент x_i належить до підгрупи, порядок якої дорівнює $N_{p,i}$. Узагальнення на недвійкові поля відкритого питання, поставле-

ного Відеманом [12, 15] для полів характеристики два, полягає в такому: чи мультиплікативний порядок $O(x_i)$ елемента x_i дорівнює $N_{p,i}$. Якщо це так, то au_r, де a примітивний елемент поля F_p, є примітивним елементом поля E_r.

У випадку $r = 1$, тобто для розширень вигляду $E_1(x_1) = F_{p^p}$, нами виконано комп'ютерні обчислення порядку елемента x_1 для всіх простих $p < 126$. При цьому використано відомі [14] розклади чисел $N_{p,1}$ на прості множники. У всіх розглянутих випадках $O(x_1) = N_{p,1}$. Також виконано обчислення для $p = 3$ та $r = 2, 3, 4$. Отримано, що $O(x_i) = N_{p,i}$ при $i = 2, 3, 4$.

1. *Lidl R., Niederreiter H.* Finite Fields. – Cambridge: Cambridge University Press, 1997. – 755 p.
2. *Mullen G.L., Panario D.* Handbook of finite fields. – London: CRC Press, 2013. – 1068 p.
3. *Gao S.* Elements of provable high orders in finite fields // Proc. Amer. Math. Soc. – 1999. – **107**, №6. – P. 1615–1623.
4. *Voloch J. F.* Elements of high order on finite fields from elliptic curves // Bull. Austral. Math. Soc. – 2010. – **81**, №3. – P. 425–429.
5. *Ahmadi O., Shparlinski I. E., Voloch J. F.* Multiplicative order of Gauss periods // Intern. J. Number Theory – 2010. – **6**, №4. – P. 877–882.
6. *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.
7. *Burkhart J. F. et al.* Finite field elements of high order arising from modular curves // Des. Codes Cryptogr. – 2009. – **51**, №3. – P. 301–314.
8. *Cheng Q.* On the construction of finite field elements of large order // Finite Fields Appl. – 2005. – **11**, №3. – P. 358–366.
9. *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$ // Finite Fields Appl. – 2013. – **19**, №1. – P. 86–92.
10. *Попович Р.* Елементи великого порядку в розширеннях Артіна-Шраєра скінченних полів // Мат. студії – 2013. – **39**, №2. – С. 115–118.
11. *Ito H., Kajiwara T., Song H. A.* Tower of Artin-Schreier extensions of finite fields and its applications // JP J. Algebra Number Theory Appl. – 2011. – **22**, №2. – P. 111–125.
12. *Wiedemann D.* An iterated quadratic extension of GF(2) // Fibonacci Quart. – 1988. – **26**, №4. – P. 290–295.
13. *Crandall R., Pomerance C.* Prime Numbers, A Computational Perspective. – Berlin: Springer-Verlag Verlag, 2005. – 596 p.
14. *Montgomery P. L., Nahm S., Wagstaff S. S. Jr.* The period of the Bell numbers modulo a prime // Math. Comp. – 2010. – **79**, №271. – P. 1793–1800.
15. *Mullen G. L., Shparlinski I. E.* Open problems and conjectures in finite fields // In: Finite Fields and Applications, London Math. Soc. Lecture Note Ser. – 1996. – **233**. – P. 243–268.

Одержано 28.04.2014