ВІСНИК НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
"ЛЬВІВСЬКА ПОЛІТЕХНІКА"
"Фізико-математичні науки"
№ 871, 2017, с. 99–102

JOURNAL OF LVIV POLYTECHNIC
NATIONAL UNIVERSITY
"Physical and mathematical sciences"
№ 871, 2017, p. 99–102

ОБМЕЖЕННЯ НА ПОРЯДОК ЕЛЕМЕНТІВ У ВЕЖАХ ВІДЕМАНА СКІНЧЕННИХ ПОЛІВ

Р. Б. Попович

Національний університет "Львівська політехніка"
вул. С. Бандери, 12, 79013, Львів, Україна

(Отримано 27 жовтня 2015 р.)

У визначених Відеманом вежах скінченних полів характеристики два отримуємо певні обмеження на мультиплікативний порядок елементів та, як наслідок, нижню межу для порядку.

Ключові слова: скінченне поле, мультиплікативний порядок, вежа Відемана.

2000 MSC: 11T30

УДК: 512.624

Вступ

Елементи великого порядку часто потрібні у низці прикладних застосувань, що використовують скінченні поля [8, 9]. В ідеалі хотілось би мати можливість отримати примітивний елемент для будь-якого скінченого поля. Проте, якщо немає розкладу порядку мультиплікативної групи скінченного поля на прості множники, невідомо, як досягти бажаного результату. Ось чому розглядають менш амбітне питання: знайти елемент доказово великого порядку. У цьому разі достатньо отримати нижню межу для порядку. Задачу розглядають як для загальних, так і для часткових скінченних полів. Використовуватимемо F_q для позначення скінченного поля з q елементів. Гао [5] запропонував алгоритм, який будує елементи великого порядку для багатьох (гіпотетично для всіх) загальних розширень F_{q^n} скінченного поля F_q з нижньою межею для порядку $\exp(\Omega((\log m)^2/\log\log m))$. Волох [13] запропонував метод, що утворює елементи порядку принаймні $\exp((\log m)^2)$ у скінченних полях з еліптичних кривих.

Для часткових випадків скінченних полів можна збудувати елементи, які мають доказово значно більші порядки. Розширення, пов'язані з поняттям гауссового періоду, розглянуто в [1, 11]. Нижня межа для порядку дорівнює $\exp(\Omega(\sqrt{m}))$. Розширення на основі полінома Куммера мають вигляд $F_q[x]/(x^m - a)$. У [3] показано, як збудувати елементи великого порядку в таких розширеннях за умови $q \equiv 1(modm)$. У цьому разі отримано нижню межу $\exp(\Omega(m))$. Умову $q \equiv 1(modm)$ для розширень на основі поліномів Кумера знято в [12].

Інше менш амбітне, але, можливо, навіть важливіше питання, — знайти примітивні елементи для класу часткових скінченних полів. Поліноміальний алгоритм, який знаходить примітивний елемент у скінченному полі малої характеристики, описано в [6]. Проте алгоритм спирається на два недоведених припущення і не підкріплений ніяким обчислювальним прикладом. Цю роботу можна розглядати як крок у цьому напрямку. Подамо певні обмеження та, як наслідок, нижню межу для мультиплікативного порядку деяких елементів у двійкових рекурсивних розширеннях скінченних полів, які визначив Відеман [14]. Робота пов'язана з відкритим питанням, що поставив Відеман [10, problem 28]. Волох [13] навів першу нетривіальну оцінку для порядку елементів у цій конструкції, а саме $\exp(2^{2^i\delta})$, де δ – деяка абсолютна константа. Проте значення константи невідоме. Наша межа не залежить ні від якої невідомої константи.

Точніше, розглядаємо такі скінченні поля, які визначив Відеман і які будуються рекурсивно:

$$x_{-1} = 1, E_{-1} = F_2(x_{-1}) = F_2;$$

для $i \geq -1$, $E_{i+1} = E_i(x_{i+1})$, де x_{i+1} задовольняє рівняння $x_{i+1}^2 + x_{i+1}x_i + 1 = 0$. В результаті отримуємо таку вежу скінченних полів характеристики два:

$$F_2 \subset E_0 = F_2(x_0) \subset E_1 = E_0(x_1) \subset ...$$

Щоб порівняти, даємо визначення вежі скінченних полів Конвеєм [14]

$$c_{-1} = 1, L_{-1} = F_2(c_{-1}) = F_2;$$

для $i \geq -1$, $L_{i+1} = L_i(c_{i+1})$, де c_{i+1} задовольняє рівняння $c_{i+1}^2 + c_{i+1} + \prod_{j=-1}^{i} c_j = 0$. У цьому разі виникає така вежа скінченних полів характеристики два:

$$L_{-1} = F_2(c_{-1}) = F_2 \subset L_0 = L_{-1}(c_0) \subset L_1 = L_0(c_1) \subset ...$$

З погляду застосувань такі побудови дуже привабливі, бо можемо виконувати операції над елементами скінченного поля рекурсивно, а, значить, ефективно [7].

Зауважимо, що кількість елементів мультиплікативної групи E_i^* $(i \geq 0)$, тобто множини ненульових елементів поля E_i, дорівнює $2^{2^{i+1}} - 1$. Якщо позначити числа Ферма $N_j = 2^{2^j} + 1$ $(j \geq 0)$, то потужність множини E_i^* $(i \geq 0)$ дорівнює $2^{2^{i+1}} - 1 = \prod_{j=0}^{i} N_j$. Наприклад, $|E_0^*| = 2^{2^1} - 1 = 3$, $|E_1^*| = 2^{2^2} - 1 = 15 = 3 \cdot 5$, $|E_2^*| = 2^{2^3} - 1 = 255 = 3 \cdot 5 \cdot 17$.

I. Допоміжні результати

Далі подамо в лемах 1–8 допоміжні для цієї роботи результати.

Лема 1. [5, section 1.3] *Для $j \geq 1$ справедлива така рівність*

$$N_j = \prod_{k=0}^{j-1} N_k + 2.$$

Як наслідок леми 1, маємо таку лему.

Лема 2. *Числа N_j ($j \geq 0$) є попарно взаємно простими.*

Лема 3. [14] *Для $i \geq 0$, виконується рівність* $(x_i)^{N_i} = 1$.

Мультиплікативний порядок елемента x_i поля визначають як найменше невід'ємне ціле число N_i таке, що $(x_i)^{N_i} = 1$. Згідно з теоремою Лагранжа для скінченних груп, з леми 3 випливає, що порядок елемента x_i ділить N_i. У випадку, коли N_i просте, x_i має порядок, що точно дорівнює N_i. Відкрите питання, що поставив Відеман [10, problem 28], полягає у такому: чи завжди мультиплікативний порядок $O(x_i)$ елемента x_i дорівнює N_i. У будь-якому випадку, порядок елемента x_i ділить N_i.

Лема 4. *Нехай $u_r = \prod_{i=0}^{r} x_i$ для $r = 0, 1....$ Мультиплікативний порядок елемента u_r дорівнює $O(u_r) = \prod_{i=0}^{r} O(x_i)$.*

□ *Доведення.* Оскільки числа Ферма попарно взаємно прості (див. лему 2), порядок елемента $u_r = \prod_{i=0}^{r} x_i$ є добутком порядків елементів x_i, $0 \leq i \leq r$. Кількість елементів мультиплікативної групи E_i^* ($i = 0, 1, ...$) дорівнює $\prod_{j=0}^{i} N_j$. Як наслідок леми 3 маємо, що група E_i^* ($i = 0, 1, ...$) є внутрішнім прямим добутком підгруп з $N_j (j = 0, ..., i)$ елементів. Елемент x_i належить до підгрупи порядку N_i. ■

Кажемо, що елемент скінченного поля є примітивним, якщо його порядок дорівнює кількості ненульових елементів скінченного поля. Якщо порядок елемента x_i справді N_i для $0 \leq i \leq r$, то $u_r = \prod_{i=0}^{r} x_i$ є примітивним елементом у E_r, бо $2^{2^{i+1}} - 1 = \prod_{j=0}^{i} N_j$. Отже, наведене раніше питання Відемана можна переформулювати й так: чи елемент $u_r = \prod_{i=0}^{r} x_i$ примітивний.

Лема 5. *Для $j \geq 2$, дільник $\alpha > 1$ числа N_j має вигляд $\alpha = l \cdot 2^{j+2} + 1$, де l – додатне ціле.*

□ *Доведення.* Результат, що отримали Ейлер і Лукас (див. [4, theorem 1.3.5]), стверджує: для $j \geq 2$, простий дільник числа N_j має вигляд $l \cdot 2^{j+2} + 1$, де l є додатним цілим. Неважко показати, що добуток двох чисел вказаного вигляду є числом такого ж вигляду. Отже, отримуємо потрібний результат. ■

Лема 6. *Нехай K – скінченне поле характеристики два та $x, y \in K$. Якщо*

$$y^2 = yx + 1, \tag{1}$$

то

$$y^{2^k} = yx^{2^k - 1} + \sum_{j=1}^{k} x^{2^k - 2^j}. \tag{2}$$

для будь-якого додатного цілого числа k.

□ *Доведення.* Індукцією за k. Для $k = 1$ отримуємо рівність (1).

Припустимо, що рівність (2) виконується для деякого додатного цілого числа k. Тоді

$$y^{2^{k+1}} = \left(y^{2^k}\right)^2 = \left(yx^{2^k-1} + \sum_{j=1}^{k} x^{2^k-2^j}\right)^2 =$$

$$= y^2 x^{2^{k+1}-2} + \sum_{j=1}^{k} x^{2^{k+1}-2^{j+1}}.$$

Враховуючи (1), маємо

$$y^{2^{k+1}} = yx^{2^{k+1}-1} + \sum_{j=1}^{k+1} x^{2^{k+1}-2^j},$$

тобто рівність (2) виконується і для $k + 1$. ■

Лема 7. $O(x_i) = N_i$ *для* $0 \leq i \leq 11$.

□ *Доведення.* Для $0 \leq i \leq 4$ числа Ферма є простими [4]: $N_0 = 3$, $N_1 = 5$, $N_2 = 17$, $N_3 = 257$, $N_4 = 65537$. Тому очевидно, що для цих чисел, як наслідок леми 3, порядок елемента x_i збігається з відповідним числом Ферма, тобто $O(x_i) = N_i$.

Далі для доведення використовуємо комп'ютерні обчислення. Ми виконуємо обчислення порядку елемента x_i для $5 \leq i \leq 11$. У цьому випадку числа Ферма повністю розкладені на прості множники [4]. Відповідні розклади наведено далі. Якщо розряди множника не поміщаються в одному рядку, то запис переносимо в наступні рядки.

$N_5 = 641 \cdot 6700417$

$N_6 = 274177 \cdot 67280421310721$

$N_7 = 59649589127497217 \cdot 5704689200685129054721$

$N_8 = 1238926361552897 \cdot P_{62}$,

де P_{62} – просте число з 62 десятковими розрядами,

$P_{62} = 93461639715357977769163558199606896584051237541638188580280321$

$N_9 = 2424833 \cdot 7455602825647884208337395736200454918783366342657 \cdot P_{99}$,

де P_{99} – просте число з 99 десятковими розрядами,

$P_{99} = 741640062627530801524787141901937474059940781097519023905821316144415759504705008092818711693940737$

$N_{10} = 45592577 \cdot 6487031809 \cdot 4659775785220018543264560743076778192897 \cdot P_{252}$,

де P_{252} – просте число з 252 десятковими розрядами,

$P_{252} = 13043987440548818972748476879650990394660853084161189218689529577683241625147186357414022797757310489589878392884292384483114903291379872$

90886016179460941194490105959067101305319061710183544916096191939124885381160807122996723228062178207531270144245774
$N_{11} = 319489 \cdot 974849 \cdot 167988556341760475137 \cdot 356084190644583392051 3 \cdot P_{564}$,
де P_{564} – просте число з 564 десятковими розрядами,
$P_{564} = 17346244717914755543025897086430977837742184472366408464934701906136357919287910885759103833040883717798381086845154642194071297830613418986428082601454275870858924387368556397311894886939915854550661114742021613255701726056413939436694579322096866510895968548270538807264582855415193640191246493118254609287981573305779557335850498227928009094287256759151891211862275171431922978810097925103603549691727991266352735878323664719315477709142774537703829458491891759032511093938132248604429857397165071105924446217754254070$
$69130470346.$

Використовуючи наведені розклади, обчислюємо x_i в степені N_i/q для будь-якого простого дільника q числа N_i. Справді, якщо елемент у степені N_i/q не дорівнює одиниці, то цей самий елемент у степені будь-якого дільника N_i/q також не дорівнює одиниці. Як результат, отримуємо, що для $5 \le i \le 11$ порядок елемента x_i не менший, ніж число N_i, тобто точно дорівнює N_i. ■

Лема 8. $(x_i)^{-1} = x_i + x_{i-1}$.

□ *Доведення.* На підставі наведеного у вступі рекурсивного рівняння, що задає вежу Відемана, маємо

$$x_i(x_i + x_{i-1}) = (x_i)^2 + x_i x_{i-1} = 1.$$

Отже, елемент x_i є оберненим до елемента $x_i + x_{i-1}$. ■

II. Основні результати

У цьому розділі даємо в теоремі 1, теоремі 2 та наслідку 1 основні результати цієї роботи.

Теорема 1. *Порядок $O(x_i)$, де $i \ge 0$, не може бути дільником числа вигляду $2^k + 1$, де k – натуральне число, яке задовольняє умову $k < 2^i$.*

□ *Доведення.* Індукцією за i. Якщо $0 \le i \le 11$, виконується за лемою 7. Нехай твердження справедливе для всіх чисел до $i - 1$ включно.

Покажемо методом від протилежного, що це твердження виконується й для i. Для цього припустимо, що $O(x_i)$ ділить $2^k + 1$, де $k < 2^i$. Тоді $(x_i)^{2^k+1} = 1$. Звідси отримуємо за лемою 8

$$(x_i)^{2^k} = (x_i)^{-1} = x_i + x_{i-1}. \qquad (3)$$

Разом з тим, приймаючи в (2) $y = x_i$, $x = x_{i-1}$, маємо

$$(x_i)^{2^k} = x_i (x_{i-1})^{2^k-1} + \sum_{j=1}^{k} (x_{i-1})^{2^k-2^j}. \qquad (4)$$

Порівнюючи коефіцієнти біля x_i в (3) та (4), отримуємо $(x_{i-1})^{2^k-1} = 1$. Отже, $O(x_{i-1})$ ділить $2^k - 1$. Тоді $O(x_{i-1})$ ділить суму чисел $2^{2^{i-1}} + 1$ (див. лему 3) та $2^k - 1$, яка дорівнює $2^{2^{i-1}} + 2^k$. Якщо числа k та 2^{i-1} збігаються, то вказана сума дорівнює степеню двійки, і отримуємо суперечність. Коли ж числа k та 2^{i-1} різні, то цю суму можна записати у вигляді $2^l(2^d + 1)$, де l – більше з чисел k та 2^{i-1}, а d – абсолютна величина їх різниці. Оскільки 2^l взаємно просте з $2^{2^{i-1}} + 1$, то $O(x_{i-1})$ ділить $2^d + 1$. А оскільки $1 \le k < 2^{i-1}$, то $d = |2^{i-1} - k| < 2^{i-1}$. Отримали суперечність з припущенням індукції.

Отже, твердження теореми виконується й для i. ■

Теорема 2. *Порядок елемента x_i дорівнює N_i для $0 \le r \le 11$ та є принаймні $3 \cdot 2^{i+2} + 1$ для $i \ge 12$.*

□ *Доведення.* За лемою 7, $O(x_i) = N_i$ виконується, якщо $0 \le i \le 11$. Покажемо тепер, що $O(x_i) \ge 3 \cdot 2^{i+2} + 1$ для $i \ge 12$. Якщо $(x_i)^{n_i} = 1$, то згідно з теоремою Лагранжа для скінченних груп n_i ділить N_i. Згідно з лемою 3, $n_i = s \cdot 2^{i+2} + 1$, де s є додатним цілим числом. За теоремою 1 s не може дорівнювати 1 або 2, тобто $s \ge 3$. Отже, отримуємо потрібний результат. ■

Наслідок 1. Порядок елемента $u = \prod_{i=0}^{r} x_i$ дорівнює $\prod_{i=0}^{11} N_i$ для $0 \le r \le 11$ та є принаймні

$$\prod_{i=0}^{11} N_i \cdot \prod_{i=12}^{r} (3 \cdot 2^{i+2} + 1)$$

для $r \ge 12$.

□ *Доведення.* Згідно з лемою 4, маємо рівність $O(u) = \prod_{i=0}^{r} O(x_i)$. Застосовуючи теорему 2, отримуємо наведені в формулюванні наслідку оцінки для порядку. ■

Література

[1] *Ahmadi O., Shparlinski I. E., Voloch J. F.* Multiplicative order of Gauss periods // Intern. J. Number Theory, **6** (4), 2010, P. 877–882.

[2] *Burkhart J. F. et al.* Finite field elements of high order arising from modular curves // Math. Comp., **51** (3), 2009, P. 301–314.

[3] *Cheng Q.* On the construction of finite field elements of large order // Finite Fields Appl., **11** (3), 2005, P. 358–366.

[4] *Crandall R., Pomerance C.* Prime numbers: a computational perspective. – Second Edition, Springer, New York, 2005, 596 p.

[5] *Gao S.* Elements of provable high orders in finite fields // Proc. Amer. Math. Soc., **107** (6), 1999, P. 1615–1623.

[6] *Huang M.-D., Narayanan A. K.* Finding primitive elements in finite fields of small characteristic // arXiv 1304.1206, 2013.

[7] *Ito H., Kajiwara T., Song H.* A Tower of Artin-Schreier extensions of finite fields and its applications // JP J. Algebra, Number Theory Appl., **2** (2), 2011, P. 111–125.

[8] *Lidl R., Niederreiter H.* Finite fields. – Cambridge University Press, Cambridge, 1997, 755 p.

[9] *Mullen L., Panario D.* Handbook of finite fields. – CRC Press, London – New York, 2013, 1068 p.

[10] *Mullen G. L., Shparlinski I. E.* Open problems and conjectures in finite fields, In: Finite Fields and Applications, volume 233 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 1996, P. 243–268.

[11] *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$ // Finite Fields Appl., **18** (4), 2012, P. 700–710.

[12] *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$ // Finite Fields Appl., **19** (1), 2013, P. 86–92.

[13] *Voloch J. F.* Elements of high order on finite fields from elliptic curves // Bull. Austral. Math. Soc. **81** (3), 2010, P. 425–429.

[14] *Wiedemann D.* An iterated quadratic extension of GF(2) // Fibonacci Quart. **26** (4), 1988, P. 290–295.

RESTRICTIONS ON THE ORDER OF ELEMENTS IN WIEDEMANN'S TOWERS OF FINITE FIELDS

R. B. Popovych

Lviv Polytechnic National University
12, S. Bandera Str., Lviv, 79013, Ukraine

We obtain some restrictions on multiplicative order of elements in defined by Wiedemann towers of finite fields of characteristic two and as a consequence a lower bound on the order.

Key words: finite field, multiplicative order, Wiedemann's tower.

2000 MSC: 11T30

UDK: 512.624