УДК 512.624

Р. Б. Попович

ОБМЕЖЕННЯ НА ПОРЯДОК ЕЛЕМЕНТІВ У ВЕЖАХ КОНВЕЯ СКІНЧЕННИХ ПОЛІВ

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

Вступ. У низці прикладних застосувань із використанням скінченних полів часто потрібні елементи великого мультиплікативного порядку. Відомо, що мультиплікативна група скінченного поля циклічна [12, 13]. Її твірний елемент називають примітивним. В ідеалі хотілось би мати можливість отримувати примітивний елемент для будь-якого скінченного поля. Знайти спосіб ефективно збудувати примітивний елемент та дослідити його вигляд важливо і теоретично, і практично. Проте без розкладу порядку мультиплікативної групи поля на прості множники, не відомо, як досягти мети. Тому розглядають менш претензійне питання: збудувати елемент доказово великого порядку. Тоді досить отримати нижню межу для порядку. Питання розглядають як для загальних [8], так і спеціальних скінченних полів [1, 2, 4, 5, 14, 15]. Зокрема, примітивні елементи або, принаймні, елементи великого порядку потрібні в низці криптографічних побудов.

Інше менш амбітне, але, ймовірно, важливіше питання: знайти примітивні елементи для класу спеціальних скінченних полів. Поліноміальний алгоритм, який знаходить примітивний елемент у скінченному полі малої характеристики, описано раніше [9]. Проте алгоритм спирається на два недоведені припущення та не підкріплений жодним обчислювальним прикладом.

Скінченне поле з q елементів позначаємо F_q. У двійкових рекурсивних розширеннях скінченних полів, які задав Конвей [6], отримуємо певні обмеження на порядок елементів та, як наслідок, нижню межу для порядку. Оцінювання знизу мультиплікативного порядку елементів у вежах Конвея пов'язане з вивченням певних арифметичних співвідношень у них.

Розглядаємо скінченні поля за Конвеєм, які будуємо рекурсивно: $c_{-1}=1$, $K_{-1}=F_2(c_{-1})=F_2$; для $i\ge -1$, $K_{i+1}=K_i(c_{i+1})$, де c_{i+1} задовольняє рівняння

$$c_{i+1}^2+c_{i+1}+\prod_{j=-1}^{i}c_j=0. \qquad (1)$$

Тобто отримуємо таку вежу скінченних полів характеристики два:

$$F_2\subset K_0=F_2(c_0)\subset K_1=K_0(c_1)\subset K_2=K_1(c_2)\subset\dots .$$

Використовуватимемо для $k\ge -1$ позначення $a_k=\prod_{j=-1}^{k}c_j$. Через K_i^* позначатимемо мультиплікативну групу поля K_i.

Легко безпосередньо перевірити такі факти: елемент c_0 є примітивним у K_0, а елемент c_1 – у K_1. Разом з тим Ленстра [11] показав: якщо $i\ge 2$, то елемент c_i не є примітивним у L_i. Деякі примітивні елементи для полів L_2, L_3, L_4 знайдені в праці [3] з використанням комп'ютерних обчислень у середовищі Sage.

Для порівняння, згідно з Відеманом [17] аналогічну вежу скінченних полів характеристики два

$$F_2 \subset E_0 = F_2(x_0) \subset E_1 = E_0(x_1) \subset E_2 = E_1(x_2) \subset \ldots$$

задаємо по-іншому: $x_{-1} = 1, E_{-1} = F_2(x_{-1}) = F_2$; для $i \geq -1$, $E_{i+1} = E_i(x_{i+1})$, де x_{i+1} задовольняє рівняння $x_{i+1}^2 + x_{i+1}x_i + 1 = 0$. Такі побудови веж скінченних полів на практиці дуже привабливі, оскільки операції над елементами скінченного поля можна виконувати рекурсивно, а тому, ефективно [10].

Зауважимо, що кількість елементів мультиплікативної групи K_i^* ($i = 0,1$) дорівнює $2^{2^{j+1}} - 1$. Позначимо числа Ферма $N_j = 2^{2^j} + 1$ ($j = 0,1,\ldots$). Тоді кількість елементів K_i^* ($i = 0,1,\ldots$) дорівнює $\prod_{j=0}^{i} N_j$. Наприклад, для перших п'яти полів у вежі Конвея маємо: $\left|K_0^*\right| = 2^{2^1} - 1 = 3$, $\left|K_1^*\right| = 2^{2^2} - 1 = 15 = 3 \cdot 5$, $\left|K_2^*\right| = 2^{2^3} - 1 = 255 = 3 \cdot 5 \cdot 17$, $\left|K_3^*\right| = 2^{2^4} - 1 = 65535 = 3 \cdot 5 \cdot 17 \cdot 257$, $\left|K_4^*\right| = 2^{2^5} - 1 = 4294967295 = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$.

Допоміжні результати. Далі даємо в лемах 1–8 доведення допоміжних для даного дослідження результатів.

Лема 1. Для $j \geq 2$, дільник $m > 1$ числа N_j має вигляд $m = l \cdot 2^{j+2} + 1$, де l – натуральне число.

Д о в е д е н н я. Результат, отриманий Ейлером і Лукасом (див. [7]), стверджує: для $j \geq 2$ простий дільник числа N_j має вигляд $l \cdot 2^{j+2} + 1$, де l – натуральне число. Очевидно, що добуток двох чисел вказаного вигляду є числом такого ж вигляду. Лему доведено.

Лема 2. Якщо m_i – найменше натуральне число з властивістю $(c_i)^{m_i} \in K_{i-1}$, то $m_i = l \cdot 2^{i+2} + 1$, де l – натуральне число.

Д о в е д е н н я. Розглянемо фактор-групу K_i^* / K_{i-1}^* з операцією, індукованою множенням на K_{i-1}. Оскільки ця група має N_i елементів, а порядок суміжного класу елемента c_i в ній дорівнює m_i, то за теоремою Лагранжа для скінченних груп число m_i ділить N_i. Тоді за лемою 1 отримуємо потрібний результат.

Лема 3. Якщо m_i – найменше натуральне число з властивістю $(c_i)^{m_i} \in K_{i-1}$, то $(c_i)^{m_i - 1} = u(c_i + 1)$, де $u \in K_{i-1}$.

Д о в е д е н н я. Виходячи з властивості числа m_i, маємо $(c_i)^{m_i - 1} \in uc_{i-1} + v$, де $u, v \in F_2(c_{i-1})$, $u \neq 0$. Тоді $(c_i)^{\alpha_i} = (uc_i + v)c_i = (u + v)c_i + ua_{i-1}$. Оскільки $(c_i)^{m_i} \in K_{i-1}$, то $u + v = 0$, тобто $u = v$, і доведення завершене.

Лема 4. Для $i \geq 0$ справедлива рівність $(c_i)^{2^{2^i}} = c_i + 1$.

Д о в е д е н н я. Безпосередньо можна перевірити, що елемент $c_i + 1$, як і c_i, є коренем рівняння (1). Тоді елементи c_i та $c_i + 1$ спряжені над полем F_2. Відповідна група Галуа складається лише з двох автоморфізмів: одиничного (тотожного) та автоморфізму, який полягає у піднесенні елементів до степеня 2^{2^i}, тобто $(c_i)^{2^{2^i}} = c_i + 1$.

Лема 5. Для $i \geq 0$ виконується співвідношення $(c_i)^{N_i} = a_{i-1}$.

Д о в е д е н н я. Домножуючи ліву та праву частини рівності з формулювання леми 4 на c_i та враховуючи рівність (1), отримуємо: $(c_i)^{2^{2^i}+1} = (c_i+1)c_i = a_{i-1}$.

Лема 6. Припустимо, що $i \geq 0$. Для $k \geq 1$ виконується співвідношення

$$(c_i)^{2^k} = c_i + a_{i-1} + \ldots + (a_{i-1})^{2^{k-1}}.$$

Д о в е д е н н я. Індукцією за k. При $k=1$ маємо правильну рівність (1). Якщо $(c_i)^{2^{k-1}} = c_i + a_{i-1} + \ldots + (a_{i-1})^{2^{k-2}}$,
то

$$(c_i)^{2^k} = (c_i + a_{i-1} + \ldots + (a_{i-1})^{2^{k-2}})^2 = c_i^2 + a_{i-1}^2 + \ldots + (a_{i-1})^{2^{k-1}}.$$

Враховуючи вираз (1), отримуємо потрібний результат.

Лема 7. Для $i \geq 1$ виконується співвідношення $a_{i-1} + \ldots + (a_{i-1})^{2^{2^{i-1}-1}} = 1$.

Д о в е д е н н я. За лемою 6 маємо:

$$(c_i)^{2^{2^i}} = c_i + a_{i-1} + \ldots + (a_{i-1})^{2^{2^i}-1}.$$

З іншого боку, лема 4 дає $(c_i)^{2^{2^i}} = c_i + 1$. Порівнюючи вільні члени у правих частинах вказаних виразів, отримуємо потрібний результат. Лему доведено.

Для невід'ємного числа r та елемента $x \in K_{i-1}$ введемо позначення $S_r(x) = \sum_{j=0}^{r-1} x^{2^j}$.

Лема 8. Для елементів x,t,u поля K_{i-1} справедливі твердження:

(a) якщо $r = gw + h$, то $S_r(x) = \sum_{l=0}^{g-1} [S_w(x)]^{2^{wl}} + S_h(x^{2^{gw}})$;

(b) якщо елементи t і u спряжені над якимось підполем поля K_{i-1} та $S_r(t) = d \in F_2$, то $S_r(u) = d$.

Д о в е д е н н я. (a) Очевидна рівність.

(b) Якщо t задовольняє рівність $S_r(t) = d$ для $d \in F_2$, то, подіявши відповідним автоморфізмом G, отримаємо: $G(S_r(t)) = S_r(G(t)) = S_r(u) = G(d) = d$.

Основні результати. Далі даємо в теоремах 1, 2 та наслідку доведення основних результатів.

Теорема 1. Припустимо, що $i \geq 1$. Якщо m_i – найменше натуральне число з властивістю $(c_i)^{m_i} \in K_{i-1}$ та $m_i = 2^k + 1$, то $k = 2^i$.

Д о в е д е н н я. Методом від протилежного. Припустимо, що m_i – найменше натуральне число з властивістю $(c_i)^{m_i} \in K_{i-1}$, $m_i = 2^k + 1$ і $k < 2^i$. Тоді $(c_i)^{2^k+1} \in K_{i-1}$, і за лемою 3 $(c_i)^{2^k+1} = u(c_i+1)$, де $u \in K_{i-1}$. Оскільки за лемою 6

$$(c_i)^{2^k} = c_i + a_{i-1} + \ldots + (a_{i-1})^{2^{k-1}},$$

то

$$S_k(a_{i-1}) = a_{i-1} + \ldots + (a_{i-1})^{2^{k-1}} = 1. \qquad (2)$$

Разом з тим за лемою 7

$$S_{2^i}(a_{i-1}) = a_{i-1} + \ldots + (a_{i-1})^{2^{2^i-1}} = 1. \qquad (3)$$

Далі рекурсивно будуємо для $j \geq 1$ елементи $S_{k_j}(a_{i-1}) \in F_2$. При $j = 1$ беремо $k_1 = k$, тобто $S_{k_1}(a_{i-1}) = S_k(a_{i-1}) = 1 \in F_2$.

Якщо $S_{k_j}(a_{i-1})$ відоме, то виконуємо таке. Зауважимо, що $S_k(a_{i-1})$ з рівності (2) має k доданків, а $S_{2^i}(a_{i-1})$ з рівності (3) – 2^i доданків. Виконуємо ділення $2^i = g_j k_j + h_j$, де $0 \leq h_j < k_j$. Якщо $h_j = 0$, то g_j парне, і за лемою 8(a)

$$1 = S_{2^i}(a_{i-1}) = \sum_{m=0}^{g_j - 1} [S_{k_j}(a_{i-1})]^{2^m} = g_j S_{k_j}(a_{i-1}) = 0.$$

Отримали суперечність. Під час перетворення останньої рівності скористалися таким фактом: оскільки $S_{k_j}(a_{i-1}) \in F_2$, то $[S_{k_j}(a_{i-1})]^{2^m} = S_{k_j}(a_{i-1})$ для $m = 0, \ldots, g_j - 1$. Отже, $h_j > 0$ і за лемою 8(a)

$$S_{2^i}(a_{i-1}) = g_j S_{k_j}(a_{i-1}) + S_{h_j}((a_{i-1})^{2^{g_j k_j}}).$$

Тоді

$$S_{h_j}((a_{i-1})^{2^{g_j k_j}}) = 1 + g_j S_{k_j}(a_{i-1}) \in F_2.$$

Покладаємо $k_{j+1} = h_j$. Зрозуміло, що $k_j > k_{j+1}$. Оскільки елементи a_{i-1} та $(a_{i-1})^{2^{g_j k_j}}$ спряжені над підполем поля K_{i-1}, то за лемою 8(b)

$$S_{h_j}(a_{i-1}) = S_{h_j}((a_{i-1})^{2^{g_j k_j}}) \in F_2.$$

Так як послідовність чисел $k_1 > k_2 > \ldots$ строго спадальна, то за скінченну кількість кроків отримаємо $k_r = 0$ та $S_{k_r}(a_{i-1}) = S_0(a_{i-1}) = a_{i-1} \in F_2$ – суперечність. Теорема доведена.

Теорема 2. Число m_i дорівнює N_i для $0 \leq i \leq 11$ та має значення принаймні $3 \cdot 2^{i+2} + 1$ для $j \geq 12$.

Д о в е д е н н я. Згідно з [16], для $0 \leq i \leq 11$ виконується рівність $m_i = N_i$. Покажемо тепер, що для $j \geq 12$ справедлива нерівність $m_i \geq 3 \cdot 2^{i+2} + 1$. Згідно з лемою 2, m_i ділить N_i. Виходячи з леми 1, $m_i = s \cdot 2^{i+2} + 1$, де s – натуральне число. За теоремою 1, число s не може дорівнювати 1 або 2, тобто $s \geq 3$. Доведення завершене.

Виходячи з праці [16] та теореми 2, отримуємо такий наслідок.

Наслідок. Мультиплікативний порядок елементів c_i та a_i дорівнює $\prod_{j=1}^{i} N_j$ для $1 \leq i \leq 11$ та має значення принаймні $\prod_{j=1}^{11} N_j \cdot \prod_{j=12}^{i} (3 \cdot 2^{j+2} + 1)$ для $i \geq 12$.

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 // Intern. J. Number Theory. – 2010. – **6**, № 4. – P. 877–882.

3. *le Bruyn L.* The odd knights of the round table. – 2010. – http://www.neverendingbooks.org/the-odd-knights-of-the-round-table http://www.neverendingbooks.org/seating-the-first-few-thousand-knights http://www.neverendingbooks.org/seating-the-first-few-billion-knights
4. *Burkhart J. F. et al.* Finite field elements of high order arising from modular curves // Des. Codes Cryptogr. – 2009. – **51**, № 3. – P. 301–314.
5. *Cheng Q.* On the construction of finite field elements of large order // Finite Fields Appl. – 2005. – **11**, № 3. – P. 358–366.
6. *Conway J. H.* On Numbers and Games. – Academic Press, New York, 1976. – 247 p.
7. *Crandall R., Pomerance C.* Prime Numbers: A Computational Perspective. – Springer-Verlag, New York, 2005. – 598 p.
8. *Gao S.* Elements of provable high orders in finite fields // Proc. Amer. Math. Soc. – 1999. – **107**, № 6. – P. 1615–1623.
9. *Huang M.-D., Narayanan A. K.* Finding primitive elements in finite fields of small characteristic. – 2013. – arXiv 1304.1206.
10. *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.
11. *Lenstra H. W.* Nim multiplication. – 1978. – https://openaccess.leidenuniv.nl/handle/1887/2125.
12. *Lidl R., Niederreiter H.* Finite Fields. – Cambridge University Press, Cambridge, 1997. – 756 p.
13. *Mullen L., Panario D.* Handbook of finite fields. – CRC Press, Boca Raton, 2013. – 1068 p.
14. *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.
15. *Popovych R.* Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$ // Ibid. – 2013. – **18**, № 1. – P. 86–92.
16. *Popovych R.* Multiplicative orders of elements in Conway's towers of finite fields – 2015. – arXiv 1509.01958.
17. *Wiedemann D.* An iterated quadratic extension of GF(2) // Fibonacci Quart. – **26**. – 1988. – P. 290–295.

ОГРАНИЧЕНИЯ НА ПОРЯДОК ЭЛЕМЕНТОВ В БАШНЯХ КОНВЕЯ КОНЕЧНЫХ ПОЛЕЙ

В определенных Конвеем башнях конечных полей характеристики два получаем некоторые ограничения на мультипликативный порядок элементов и, как следствие, нижнюю границу для порядка.

RESTRICTIONS ON THE ORDER OF ELEMENTS IN CONWAY TOWERS OF FINITE FIELDS

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

Нац. ун-т "Львівська політехніка", Львів

Одержано 09.09.15