УДК 512.44

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

ЕЛЕМЕНТИ ВЕЛИКОГО ПОРЯДКУ В ОДНІЙ ВЕЖІ СКІНЧЕННИХ ПОЛІВ

We construct explicitely elements of high multiplicative order in towers of finite fields of characreristic bigger than two.

Ми явно будуємо елементи великого мультиплікативного порядку у вежах скінченних полів характеристики більшої, ніж два.

Загальновідомо, що мультиплікативна група скінченого поля є циклічною. Твірну цієї групи називають примітивним елементом. Задача ефективної побудови примітивного елемента для заданого скінченого поля є важкою в обчислювальній теорії скінченних полів. Ось чому розглядають менш обмежуюче питання: знайти елемент великого мультиплікативного порядку [1, 2]. У цьому випадку не вимагається обчислити точний порядок елемента: достатньо отримати нижню границю для порядку. Елементи великого порядку потрібні для низки застосувань. Такі застосування, зокрема, включають криптографію, теорію кодування, генератори псевдовипадкових чисел та комбінаторику. Питання розглядають як для загальних [3,4], так і для спеціальних [5–12] скінченних полів. Скінченне поле з q елементів позначаємо F_q. Групу, породжену елементом v, позначаємо $\langle v \rangle$. Кількість сполучень з n елементів по k елементів позначатимемо $\binom{n}{k}$.

Для часткових випадків скінченних полів можна збудувати елементи, що мають набагато більші порядки. Особливий інтерес становить побудова елементів у рекурсивних розширеннях скінченних полів – вежах скінченних полів характеристики два або більшої від двох. З прикладної точки зору такі побудови дуже привабливі, оскільки операції над елементами скінченого поля можна виконувати рекурсивно, а тому ефективно [13]. Такі розширення, зокрема, розглядалися в роботах [7,13,14].

У даній роботі явно будуємо елементи великого порядку в недвійкових двоелементних вежах скінченних полів та даємо явну оцінку знизу на їх мультиплікативний порядок.

Більш точно, розглядаємо скінченні поля, які будуємо рекурсивно:

$E_1 = F_p(x)$, де $p \geq 3$ та x задовольняє рівняння $x^p - x - 1 = 0$;

$E_2 = E_1(y)$, де y задовольняє рівняння $y^p - y - x^{p-1} = 0$.

Тобто, отримуємо таку вежу скінченних полів недвійкової характеристики:

$$F_p \subset E_1 = F_p(x) \subset E_2 = E_1(y).$$

Зауважимо, що число елементів поля E_1 дорівнює p^p, а число елементів поля E_2 дорівнює p^{p^2}. Відомо [1], 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 $E_1 = F_{p^p} = F_p[x]/(x^p - x - 1)$. Зрозуміло, що $x^p = x + 1$.

Також відомо [1], що $F_{p^{p^2}} = F_{p^p}[y]/(y^p - y - x^{p-1}) = E_1(y)$ і тоді $y^p = y + x^{p-1}$.

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 [1,2]. Два елементи α, β з F_q називаємо спряженими (над F_p), якщо

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

для деякого степеня φ^t автоморфізму Фробеніуса.

Далі даємо в лемах 1 та 2 доведення допоміжних для даної роботи результатів.

Лема 1. *У випадку поля $E_1 = F_{p^p} = F_p[x]/(x^p - x - 1)$ спряжені елементи x мають вигляд $x + i$ для $i = 0, ..., p - 1$.*

Доведення. Покажемо, що $x^{p^i} = x + i$, що для будь-якого натурального i. Доведемо це індукцією за i.

Очевидно, що для $i = 0$ рівність виконується. Припустимо, що вона виконується для деякого i. Тоді для $i + 1$ маємо:

$$x^{p^{i+1}} = [x^{p^i}]^p = (x + i)^p = x^p + i = x + i + 1.$$

Отже, рівність справедлива для будь-якого натурального i.

Лема 2. *Для числа сполучень з повтореннями H_b^a з b елементів по a елементів виконується нерівність: $H_b^a > \left(\frac{b}{a}\right)^a$.*

Доведення. Відомо, що $H_b^a = \begin{pmatrix} b+a-1 \\ a \end{pmatrix}$. Використовуючи відому оцінку для величини біноміальних коефіцієнтів $\begin{pmatrix} n \\ k \end{pmatrix} \geq \left(\frac{n}{k}\right)^k$ при $n = b + a - 1$ та $k = a$, отримуємо

$$H_b^a = \begin{pmatrix} b+a-1 \\ a \end{pmatrix} \geq \left(\frac{b+a-1}{a}\right)^a > \left(\frac{b}{a}\right)^a.$$

Теорема 1. *Спряжені елементи у поля $E_2 = F(p^{p^2})$ над полем $E_1 = F_{p^p}$ мають вигляд*

$$y^{p^i} = y + u\sum_{k=0}^{s}(x+k)^{p-1} + v\sum_{l=s+1}^{p-1}(x+l)^{p-1}, \qquad (1)$$

де $u = v = 0$ або $u \equiv v + 1 (mod p)$, $0 \leq s \leq p - 1$.

Доведення. Виконуємо індукцією за i. При $i = 0$ твердження очевидним чином виконується: $y^{p^0} = y$.

Припустимо, що дане твердження справедливе для $i - 1$. Покажемо, що тоді воно справедливе для i. Розглянемо такі можливі випадки.

1) $u = v = 0$, тобто $y^{p^{i-1}} = y$. Тоді $y^{p^i} = y^p = y + x^{p-1}$. Таким чином, y^{p^i} має вигляд (1).

2) $u = 1$, $v = 0$, $0 \leq s \leq p - 2$, тобто $y^{p^{i-1}} = y + \sum_{k=0}^{s}(x+k)^{p-1}$. Тоді

$$y^{p^i} = y + x^{p-1} + \sum_{k=0}^{s}(x+k+1)^{p-1} = y + \sum_{k=0}^{s+1}(x+k)^{p-1}.$$

Як бачимо, y^{p^i} має вигляд (1), де $1 \le s \le p-1$.

3) $u = 1$, $s = p-1$, тобто $y^{p^{i-1}} = y + \sum_{k=0}^{p-1}(x+k)^{p-1}$. Тоді

$$y^{p^i} = y + x^{p-1} + \sum_{k=0}^{p-1}(x+k+1)^{p-1} = y + x^{p-1} + \sum_{k=1}^{p-1}(x+k)^{p-1} + (x+p)^{p-1} =$$

$$= y + 2x^{p-1} + \sum_{k=1}^{p-1}(x+k)^{p-1}.$$

Таким чином, y^{p^i} має вигляд (1).

4) $u = 0$, $v = p-1$, $0 \le s \le p-1$, тобто $y^{p^{i-1}} = y + (p-1)\sum_{k=s}^{p-1}(x+k)^{p-1}$. У цьому разі

$$y^{p^i} = y + x^{p-1} + (p-1)\sum_{k=s}^{p-1}(x+k+1)^{p-1} =$$

$$= y + (1+p-1)x^{p-1} + (p-1)\sum_{k=s+1}^{p-1}(x+k)^{p-1} = y + (p-1)\sum_{k=s+1}^{p-1}(x+k)^{p-1}.$$

Зрозуміло, що y^{p^i} має вигляд (1).

5) $u, v \ne 0$, $u, v \ne p-1$, $u = v+1$, $0 \le s \le p-2$, тобто

$$y^{p^i} = y + u\sum_{k=0}^{s}(x+k)^{p-1} + v\sum_{l=s+1}^{p-1}(x+l)^{p-1}.$$

У цьому випадку

$$y^{p^i} = y + x^{p-1} + u\sum_{k=0}^{s}(x+k+1)^{p-1} + v\sum_{l=s+1}^{p-1}(x+l+1)^{p-1} =$$

$$= y + u\sum_{k=0}^{s+1}(x+k)^{p-1} + v\sum_{l=s+2}^{p-1}(x+l)^{p-1}.$$

Очевидно, що y^{p^i} має вигляд (1). Доведення теореми 1 завершене.

Спряжені елемента $y \in F_{p^{p^2}}$ відносно F_p отримуємо застосовуючи всі автоморфізми поля $F_{p^{p^2}}$ над F_p до елемента y [1]. Згадані автоморфізми утворюють групу з операцією, яка є звичайною композицією відображень. Згідно з [1, theorem 2.21] ця група циклічна порядку p^2.

Основний результат даної роботи дається в теоремі 2.

Теорема 2. *Елемент y поля $F_{p^{p^2}}$ має мультиплікативний порядок більший від $\frac{p^p-1}{p-1}$.*

Доведення. До підгрупи $\langle y\rangle$ належать спряжені елемента y (за рахунок p^2 автоморфізмів над F_p), які мають за лемою 1 вигляд (1). У результаті маємо p^2 різних лінійних двочленів від y з коефіцієнтами з поля F_{p^p}. З них утворюємо добутки, вибираючи щонайбільше $p-1$ двочлен (двочлени можна повторювати). У результаті отримуємо різні добутки за модулем полінома y^p-y-x^{p-1}. Оцінимо загальне можливе число таких добутків.

Зрозуміло, що маємо сполучення з повтореннями з p^2 елементів по r елементів $(0 \le r \le p-1)$. Тобто загалом маємо $\sum_{r=0}^{p-1} H_{p^2}^r$ варіантів. Тепер даємо оцінку знизу для цієї суми. Згідно лемою 2 маємо нерівпості

$\sum_{r=0}^{p-1} H_{p^2}^r > \sum_{r=0}^{p-1} \left(\frac{p^2}{r}\right)^r > \sum_{r=0}^{p-1} p^r = \frac{p^p-1}{p-1}$,

і отримали потрібний результат.

Розглянемо для прикладу випадок $p=5$, Маємо

$$E_1 = F_{p^p} = F_p[x]/(x^p - x - 1) = F_{5^5} = F_5[x]/(x^5 - x - 1).$$

Тоді $x^5 = x+1$, $x^{5^2} = x+2$, $x^{5^3} = x+3$, $x^{5^4} = x+4$. Тобто елемент x має 5 спряжених елементів (враховуючи сам елемент).

Також маємо

$$E_2 = F_{p^{p^2}} = F_{p^p}[y]/(y^p - y - x^{p-1}) = F_{5^{5^2}} = F_{5^5}[y]/(y^5 - y - x^4) = F_{5^5}(y).$$

Елемент y має 25 спряжених елементів. Вони виписані далі.

$$y^{5^0} = y$$

$$y^{5^1} = y + x^4$$

$$y^{5^2} = y + x^4 + (x+1)^4$$

$$y^{5^3} = y + x^4 + (x+1)^4 + (x+2)^4$$

$$y^{5^4} = y + x^4 + (x+1)^4 + (x+2)^4 + (x+3)^4$$

$$y^{5^5} = y + x^4 + (x+1)^4 + (x+2)^4 + (x+3)^4 + (x+4)^4$$

$$y^{5^6} = y + 2x^4 + (x+1)^4 + (x+2)^4 + (x+3)^4 + (x+4)^4$$

$$y^{5^7} = y + 2x^4 + 2(x+1)^4 + (x+2)^4 + (x+3)^4 + (x+4)^4$$

$$y^{5^8} = y + 2x^4 + 2(x+1)^4 + 2(x+2)^4 + (x+3)^4 + (x+4)^4$$

$$y^{5^9} = y + 2x^4 + 2(x+1)^4 + 2(x+2)^4 + 2(x+3)^4 + (x+4)^4$$

$$y^{5^{10}} = y + 2x^4 + 2(x+1)^4 + 2(x+2)^4 + 2(x+3)^4 + 2(x+4)^4$$

$$y^{5^{11}} = y + 3x^4 + 2(x+1)^4 + 2(x+2)^4 + 2(x+3)^4 + 2(x+4)^4$$

$$y^{5^{12}} = y + 3x^4 + 3(x+1)^4 + 2(x+2)^4 + 2(x+3)^4 + 2(x+4)^4$$

$$y^{5^{13}} = y + 3x^4 + 3(x+1)^4 + 3(x+2)^4 + 2(x+3)^4 + 2(x+4)^4$$

$$y^{5^{14}} = y + 3x^4 + 3(x+1)^4 + 3(x+2)^4 + 3(x+3)^4 + 2(x+4)^4$$

$$y^{5^{15}} = y + 3x^4 + 3(x+1)^4 + 3(x+2)^4 + 3(x+3)^4 + 3(x+4)^4$$

$$y^{5^{16}} = y + 4x^4 + 3(x+1)^4 + 3(x+2)^4 + 3(x+3)^4 + 3(x+4)^4$$

$$y^{5^{17}} = y + 4x^4 + 4(x+1)^4 + 3(x+2)^4 + 3(x+3)^4 + 3(x+4)^4$$

$$y^{5^{18}} = y + 4x^4 + 4(x+1)^4 + 4(x+2)^4 + 3(x+3)^4 + 3(x+4)^4$$

$$y^{5^{19}} = y + 4x^4 + 4(x+1)^4 + 4(x+2)^4 + 4(x+3)^4 + 3(x+4)^4$$

$$y^{5^{20}} = y + 4x^4 + 4(x+1)^4 + 4(x+2)^4 + 4(x+3)^4 + 4(x+4)^4$$

$$y^{5^{21}} = y + 4(x+1)^4 + 4(x+2)^4 + 4(x+3)^4 + 4(x+4)^4$$

$$y^{5^{22}} = y + 4(x+2)^4 + 4(x+3)^4 + 4(x+4)^4$$

$$y^{5^{23}} = y + 4(x+3)^4 + 4(x+4)^4$$

$$y^{5^{24}} = y + 4(x+4)^4$$

Отримали $p^2 = 25$ різних лінійних двочленів від y з коефіцієнтами з поля F_{p^p}. З них утворюємо добутки по $p - 1 = 4$ співмножники.

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. *Попович Р.* Елементи великого порядку в розширеннях Артіна-Шраєра скінченних полів // Мат. студії – 2013. – **39**, №2. – С. 115–118.
6. *Попович Р.* Про елементи великого порядку в розширеннях скінченних полів на основі поліномів Куммера // Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ. – 2013. – **24**, №1. – С. 139–145.
7. *Попович Р.* Нижня межа для мультиплікативного порядку елементів у вежах скінченних полів характеристики $p \geq 3$ // Наук. вісник Ужгород. ун-ту. Сер. матем. і інформ. – 2014. – **25**, №1. – С. 120–123.
8. *Ahmadi O., Shparlinski I. E., Voloch J. F.* Multiplicative order of Gauss periods // Intern. J. Number Theory – 2010. – **6**, №4. – P. 877–882.
9. *Burkhart J. F. et al.* Finite field elements of high order arising from modular curves // Des. Codes Cryptogr. – 2009. – **51**, №3. – P. 301–314.
10. *Cheng Q.* On the construction of finite field elements of large order // Finite Fields Appl. – 2005. – **11**, №3. – P. 358–366.
11. *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.
12. *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.
13. *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.
14. *Wiedemann D.* An iterated quadratic extension of GF(2) // Fibonacci Quart. – 1988. – **26**, №4. – P. 290–295.

Одержано 4.11.2014