Математичний Вісник
Наукового Товариства
ім. Тараса Шевченка
2014. — Т.11

Mathematical Bulletin
of Taras Shevchenko
Scientific Society
2014. — V.11

ПРО ІЗОМОРФІЗМ СКІНЧЕННИХ ПОЛІВ ХАРАКТЕРИСТИКИ ДВА

Роман Попович

Національний університет «Львівська політехніка», Львів, вул.Бандери, 12

Р. Попович. *Про ізоморфізм скінченних полів характеристики два* // Мат. вісн. Наук. тов. ім. Т. Шевченка. — 2014. — Т.11. — С. 12–20.

Явно задано ізоморфізм між першими дванадцятьма полями у вежах за Конвеєм та Відеманом.

R. Popovych, *On isomorphizm of finite fields of characteristic two*, Math. Bull. T. Shevchenko Sci. Soc. **11** (2014), 12–20.

Izomorphism between first twelve fields in towers by Conway and Wiedemann is set explicitely.

1. Вступ

У низці прикладних застосувань із використанням скінченних полів часто потрібні елементи великого мультиплікативного порядку [6]. В ідеалі хотілось би мати можливість отримувати примітивний елемент для будь-якого скінченного 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, так і для спеціальних скінченних полів [1, 2, 4, 6, 8, 9].

Скінченне поле з q елементів позначаємо $\mathbb{F}_q$.

2010 *Mathematics Subject Classification:* 11T30 *УДК:* 512.624
Ключові слова і фрази: скінченне поле, мультиплікативний порядок
E-mail: rombp07@gmail.com

У даній роботі в двійкових рекурсивних розширеннях скінченних полів, які задані Конвеєм [10, 11, 12], описано примітивні елементи для перших дванадцяти полів у відповідній вежі полів. У результаті явно задано ізоморфізм між першими дванадцятьма полями у вежах за Конвеєм та Відеманом. Це можна розглядати як крок у напрямку отримання відповіді на відкрите питання, поставлене Відеманом про явний опис ізоморфізму між полями однакового порядку із двох різних веж скінченних полів (див. [7, problem 30] або [10]. Один варіант вежі запропоновано Конвеєм [11, 12], а інший – Відеманом [10].

Більш точно, розглядаємо скінченні поля за Конвеєм, які будуємо рекурсивно:
$K_0 = \mathbb{F}_2(c_0)$, де c_0 задовольняє рівняння $c_0^2 + c_0 = 1$;
$K_{i+1} = K_i(c_{i+1})$, $i = 0, 1, ...$, де c_{i+1} задовольняє рівняння $c_{i+1}^2 + c_{i+1} = \prod_{j=0}^{i} c_j$.
Тобто, отримуємо таку вежу скінченних полів характеристики 2:

$$\mathbb{F}_2 \subset K_0 = \mathbb{F}_2(c_0) \subset K_1 = K_0(c_1) \subset K_2 = K_1(c_2) \subset \dots$$

Згідно з Відеманом аналогічну вежу скінченних полів характеристики 2 задаємо по-іншому:
$E_0 = \mathbb{F}_2(x_0)$, де x_0 задовольняє рівняння $x_0^2 + x_0 + 1 = 0$;
$E_{i+1} = E_i(x_{i+1})$, $i \geq 0$, де x_{i+1} задовольняє рівняння $x_{i+1}^2 + x_{i+1}x_i + 1 = 0$.
У цьому разі маємо таку вежу скінченних полів:

$$\mathbb{F}_2 \subset E_0 = \mathbb{F}_2(x_0) \subset E_1 = E_0(x_1) \subset E_2 = E_1(x_2) \subset \dots$$

З прикладної точки зору такі побудови дуже привабливі, оскільки операції над елементами скінченного поля можна виконувати рекурсивно, а тому ефективно [5].

Зауважимо, що число елементів мультиплікативної групи K_i^* $(i \geq 0)$ дорівнює $2^{2^{i+1}} - 1$. Позначимо числа Ферма $N_j = 2^{2^j} + 1$ $(j \geq 0)$. Тоді число елементів K_i^* $(i \geq 0)$ дорівнює $\prod_{j=0}^{i} N_j$. Наприклад, отримуємо $|K_0^*| = 2^{2^1} - 1 = 3$, $|K_1^*| = 2^{2^2} - 1 = 15 = 3 \cdot 5$, $|K_2^*| = 2^{2^3} - 1 = 255 = 3 \cdot 5 \cdot 17$.

2. Допоміжні твердження

Далі даємо в лемах 1—3 та наслідку доведення допоміжних для даної роботи результатів.

Лема 1. *Для кожного натурального числа i справедлива рівність*

$$N_i = \prod_{j=0}^{i-1} N_j + 2. \tag{1}$$

Доведення. Індукцією за i. Для $i = 1$ маємо 3+2=5. Припустимо, що рівність (1) виконується для деякого натурального i. Тоді

$\prod_{j=0}^{i} N_j + 2 = (N_i - 2)N_i + 2 = (2^{2^i} - 1)(2^{2^i} + 1) + 2 = 2^{2^{i+1}} + 1 = N_{i+1}$. □

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

Доведення. Припустимо, що існує таке ціле $d > 1$, яке ділить N_m та N_l для деякого $l < m$. Оскільки d ділить N_l, то d ділить $\prod_{i=0}^{m-1} N_i$. Тоді за лемою 1, d ділить $N_m - 2$. Значить, d ділить суму N_m та $N_m - 2$, і маємо $d = 2$. Оскільки всі числа Ферма непарні, то отримали суперечність. □

Як наслідок з леми 2 маємо, що група K_i^* $(i \geq 0)$ є внутрішнім прямим добутком підгруп з N_j $(j \geq 0)$ елементів. Відкрите питання, поставлене Відеманом (див. [7, problem 30] або [10]), полягає в такому: явно задати ізоморфізм між полями однакового порядку $K_i = \mathbb{F}_2(c_0, \ldots, c_i)$ та $E_i = \mathbb{F}_2(x_0, \ldots, x_i)$. Інше відкрите питання, сформульоване Відеманом (див. [7, problem 28] або [10]): чи мультиплікативний порядок $O(x_i)$ елемента x_i дорівнює N_i. Для $0 \leq i \leq 11$ це справедливо, і тоді елемент $\prod_{j=0}^{i} x_j$ є примітивним у полі $E_i = \mathbb{F}_2(x_0, \ldots, x_i)$. Подібне питання можна ставити стосовно оцінки мультиплікативного порядку $O(c_i)$ елемента c_i.

Лема 3. *Нехай маємо вежу полів $L_1 \subset L_2$ та $b \in L_2$. Нехай $b^r = a \in L_1^*$ та r – найменше натуральне число з властивістю $b^r \in L_1^*$. Тоді $O(b) = r \cdot O(a)$.*

Доведення. Оскільки $b^{O(b)} = 1$, то $O(b) \geq r$. Запишемо $O(b) = sr + t$, де $s \in N$ та $0 \leq t < r$. Тоді

$$1 = b^{O(b)} = b^{sr+t} = a^s b^t.$$

Звідси $b^t = a^{-s} \in L_1^*$. За означенням r це можливо лише при $t = 0$. Маємо $a^s = 1$, $s \geq O(a)$ та $O(b) \geq r \cdot O(a)$. З іншого боку $b^{r \cdot O(a)} = a^{O(a)} = 1$, і тому $O(b) = r \cdot O(a)$. □

Наслідок 1. *Нехай $(c_i)^{\alpha_i} = \prod_{j=0}^{i-1} c_j$ та α_i – найменше натуральне число з властивістю $(c_i)^{\alpha_i} \in (K_{i-2}(c_{i-1}))^*$. Тоді*

(a) $O(c_i) = \alpha_i \prod_{j=0}^{i-1} c_j$.

(b) $O(\prod_{j=0}^{i} c_j) = \alpha_i O\Big(\big(\prod_{j=0}^{i-1} c_j\big)^{\alpha_i+1}\Big)$.

Доведення. (a) Отримуємо, поклавши в лемі 3 $b = c_i$, $a = \prod_{j=0}^{i-1} c_j$, $r = \alpha_i$.

(b) Оскільки $\prod_{j=0}^{i-1} c_j \in K_{i-2}(c_{i-1})$, то $\big(\prod_{j=0}^{i} c_j\big)^{\alpha_i} \in K_{i-2}(c_{i-1})$ тоді і тільки тоді, коли $(c_i)^{\alpha_i} \in K_{i-2}(c_{i-1})$. Значить, α_i – найменше натуральне число з властивістю $\left(\prod_{j=0}^{i} c_j\right)^{\alpha_i} \in K_{i-2}(c_{i-1})$. Візьмемо в лемі 3 $a = \left(\prod_{j=0}^{i-1} c_j\right)^{\alpha_i+1}$, $b = \prod_{j=0}^{i} c_j$ та $r = \alpha_i$. Оскільки

$$b^r = \Big(\prod_{j=0}^{i} c_j\Big)^{\alpha_i} = (c_i)^{\alpha_i}\Big(\prod_{j=0}^{i-1} c_j\Big)^{\alpha_i} = \Big(\prod_{j=0}^{i-1} c_j\Big)^{\alpha_i+1} = a,$$

то

$$O\Big(\prod_{j=0}^{i} c_j\Big) = \alpha_i O\Big(\Big(\prod_{j=0}^{i-1} c_j\Big)^{\alpha_i+1}\Big).$$

□

3. Основні результати

Основні результати даної роботи наведено в теоремах 1–3.

Теорема 1. *$c_0^3 = 1$ та $\alpha_0 = 3$ – найменше натуральне число з властивістю $(c_0)^{\alpha_0} \in \mathbb{F}_2$;*
$c_1^5 = c_0$ та $\alpha_1 = 5$ – найменше натуральне число з властивістю $(c_1)^{\alpha_1} \in K_0$;
для $2 \le i \le 11$: $(c_i)^{N_i} = \prod_{j=0}^{i-1} c_j$ та $\alpha_i = N_i$ – найменше натуральне число з властивістю $(c_i)^{\alpha_i} \in K_{i-2}(c_{i-1})$.

Доведення. Рівність $c_0^3 = 1$ можна легко перевірити безпосередньо. Оскільки $c_1^2 = c_1 + c_0$, $c_1^4 = (c_1 + c_0)^2 = c_1 + 1$, то $c_1^5 = c_0$.

Послідовно обчислюючи степені елемента c_2, отримуємо:

$$c_2^2 = c_2 + c_1c_0,$$

$$c_2^4 = (c_2 + c_1c_0)^2 = c_2 + c_1 + 1,$$

$$c_2^8 = (c_2 + c_1 + 1)^2 = c_2 + c_1 + c_0 + c_1c_0 + 1,$$

$$c_2^8 = (c_2 + c_1 + 1)^2 = c_2 + c_1 + c_0 + c_1c_0 + 1,$$

$$c_2^{16} = (c_2 + c_1 + c_0 + c_1c_0 + 1)^2 = c_2 + 1.$$

Тоді $c_2^{17} = (c_2 + 1)c_2 = c_1c_0$.

Для доведення рівностей при $3 \le i \le 11$ використано комп'ютерні обчислення. При знаходженні степенів елементів застосовано широко відомий швидкий («індійський») алгоритм послідовних піднесень до квадрату та множень.

Відомо, що для $0 \le i \le 4$ числа Ферма є простими [3]: $N_0 = 3$, $N_1 = 5$, $N_2 = 17$, $N_3 = 257$, $N_4 = 65537$. Нами перевірено, що $(c_3)^{257} = c_2c_1c_0$ та $(c_4)^{65537} = c_3c_2c_1c_0$.

Для $5 \le i \le 11$ числа Ферма повністю розкладені на прості множники [3]. Відповідні розклади й пов'язані з ними результати перевірки наведено далі.

Виходячи з розкладу $N_5 = 641 \cdot 6700417$, перевірено, що

$$(c_5)^{641 \cdot 6700417} = c_4 c_3 c_2 c_1 c_0.$$

Користуючись розкладом $N_6 = 274177 \cdot\ 67280421310721$, отримано

$$(c_6)^{274177 \cdot\ 67280421310721} = c_5 c_4 c_3 c_2 c_1 c_0.$$

Маючи розклад $N_7 = 59649589127497217 \cdot 5704689200685129054721$, перевірено, що

$$(c_7)^{59649589127497217 \cdot 5704689200685129054721} = c_6 c_5 c_4 c_3 c_2 c_1 c_0.$$

Для розкладу $N_8 = 1238926361552897 \cdot P_{62}$, де P_{62} – просте число з 62 десятковими розрядами,
$P_{62} = 93461639715357977769163558199606896584051237541638188580280321$,
перевірено, що

$$(c_8)^{1238926361552897 \cdot P_{62}} = c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0.$$

Виходячи з розкладу
$N_9 = 2424833 \cdot 7455602825647884208337395736200454918783366342657 \cdot P_{99}$, де P_{99} – просте число з 99 десятковими розрядами,
$P_{99} = 741640062627530801524787141901937474059940781097519023905821316144415759504705008092818711693940737$,
перевірено, що

$$(c_9)^{2424833 \cdot 7455602825647884208337395736200454918783366342657 \cdot P_{99}} = c_8 c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0.$$

Користуючись таким розкладом для числа N_{10}:
$45592577 \cdot 6487031809 \cdot 4659775785220018543264560743076778192897 \cdot P_{252}$,
де P_{252} – просте число з 252 десятковими розрядами,
$P_{252} = 130439874405488189727484768796509903946608530841611892186895295776832416251471863574140227977573104895898783928842923844831149032913798729088601617946094119449010595906710130531906171018354491609619193912488538116080712299672322806217820753127014424577$,
перевірено, що

$$(c_{10})^{45592577 \cdot 6487031809 \cdot 4659775785220018543264560743076778192897 \cdot P_{252}} = \prod_{j=0}^{9} c_j.$$

Для розкладу
$N_{11} = 319489 \cdot 974849 \cdot 167988556341760475137 \cdot 3560841906445833920513 \cdot P_{564}$,
де P_{564} – просте число з 564 десятковими розрядами,

$P_{564} = 17346244717914755543025897086430977837742184472366408464934701906136357919287910885759103833040883717798381086845154642194071297830613418986428082601454275870858924387368556397311894886939915854550661114742021613425570172605641393943669457932209686651089596854827053880726458285541519364019124649311825460928798157330577955733585049822792800909428725675915189121186227517143192297881009792510360354969172799126635273587832366471931547770914277453770382945849189175903251109439381322486044298573971650711059244462177542540706913047034 6$

перевірено, що

$$(c_{11})^{319489 \cdot 974849 \cdot 167988556341760475137 \cdot 3560841906445833920513 \cdot P_{564}} = \prod_{j=0}^{10} c_j.$$

Для доведення факту: N_i – найменше натуральне число з властивістю $c_i^{N_i} \in (K_{i-2}(c_{i-1}))^*$, досить перевірити, що $c_i^{N_i/p} \notin (K_{i-2}(c_{i-1}))^*$ для будь-якого простого дільника p числа N_i. Дійсно, якщо елемент c_i в степені N_i/p не належить до $(K_{i-2}(c_{i-1}))^*$, то цей же ж елемент в степені будь-якого дільника N_i/p також не належить до $(K_{i-2}(c_{i-1}))^*$. Оскільки для $0 \leq i \leq 4$ числа Ферма є простими, то для них вказаний факт очевидним чином виконується. Для $5 \leq i \leq 11$ виконано відповідні перевірки. $\square$

Теорема 2. *Мультиплікативні порядки елементів є такими:*
$O(c_0) = N_0, O(c_1) = N_0N_1, O(c_0c_1) = N_1$;
для $2 \leq i \leq 11$: $O(c_i) = O(\prod_{j=0}^{i} c_j) = \prod_{j=1}^{i} N_j$.

Доведення. Безпосередньо можна перевірити, що $O(c_0) = N_0 = 3$. Оскільки $O(c_0) = 3$ і згідно з теоремою 1, $(c_1)^5 = c_0$ та $\alpha_1 = 5$ є найменшим натуральним числом з властивістю $(c_1)^{\alpha_1} \in K_0$, то за наслідком 1(a), $O(c_1) = 5 \cdot 3$. За наслідком (b) $O(c_1c_0) = 5 \cdot O((c_0)^6) = 5$.

Оскільки $O(c_1c_0) = 5$ і згідно з теоремою 1, $(c_2)^{17} = c_1c_0$ та $\alpha_2 = 17$ є найменшим натуральним числом з властивістю $(c_2)^{\alpha_2} \in K_0(c_1)$, то за наслідком 1(a), $O(c_2) = 17 \cdot 5$. За наслідком 1(b), $O(c_2c_1c_0) = 17 \cdot O((c_1c_0)^{18}) = 17 \cdot 5$. Так як (18,5)=1, то $O((c_1c_0)^{18}) = O(c_1c_0) = 5$ і маємо $O(c_2c_1c_0) = 17 \cdot 5$.

$O(c_2c_1c_0) = 17 \cdot 5$ і згідно з теоремою 1, $(c_3)^{257} = c_2c_1c_0$ та $\alpha_3 = 257$ є найменшим натуральним числом з властивістю $(c_3)^{\alpha_3} \in K_1(c_2)$. Тоді за наслідком 1(a), $O(c_3) = 257 \cdot 17 \cdot 5$. За наслідком 1(b) виконується

$$O(c_3c_2c_1c_0) = 257 \cdot O((c_2c_1c_0)^{258}) = 257 \cdot 17 \cdot 5.$$

При отриманні останнього порядку враховано, що (258,17·5)=1.

Так як $O(c_3c_2c_1c_0) = 257 \cdot 17 \cdot 5$ і згідно з теоремою 1, $(c_4)^{65537} = c_3c_2c_1c_0$ та $\alpha_4 = 65537$ є найменшим натуральним числом з властивістю $(c_4)^{\alpha_4} \in$

$K_2(c_3)$, то за наслідком 1(a) $O(c_4) = 65537 \cdot 257 \cdot 17 \cdot 5$. За наслідком 1(b), $O(c_4c_3c_2c_1c_0) = 65537 \cdot O\big((c_3c_2c_1c_0)^{65538}\big) = 65537 \cdot 257 \cdot 17 \cdot 5$. При цьому враховано, що (65538,257·17·5)=1.

Маємо $O(c_4c_3c_2c_1c_0) = 65537{\cdot}257{\cdot}17{\cdot}5$ і згідно з теоремою 1, $(c_5)^{641\cdot 6700417} = c_4c_3c_2c_1c_0$ та $\alpha_5 = 641 \cdot 6700417$ є найменшим натуральним числом з властивістю $(c_5)^{\alpha_5} \in K_3(c_4)$. За наслідком 1(a) виконується

$$O(c_5) = 641 \cdot 6700417 \cdot 65537 \cdot 257 \cdot 17 \cdot 5.$$

За наслідком 1(b) справедливі рівності

$$O(\prod_{j=0}^{5} c_j) = 641{\cdot}6700417{\cdot}O((\prod_{j=0}^{4} c_j)^{641\cdot 6700417+1}) = 641{\cdot}6700417{\cdot}65537{\cdot}257{\cdot}17{\cdot}5.$$

При цьому враховано, що (641·6700417+1,65537·257·17·5)=1.

Виконується $O(\prod_{j=0}^{5} c_j) = 641 \cdot 6700417 \cdot 65537 \cdot 257 \cdot 17 \cdot 5$ і згідно з теоремою 1 $(c_6)^{274177\cdot 67280421310721} = c_5c_4c_3c_2c_1c_0$ та $\alpha_6 = 274177 \cdot 67280421310721$ є найменшим натуральним числом з властивістю $(c_6)^{\alpha_6} \in K_4(c_5)$. Наслідок 1(a) дає $O(c_6) = 274177 \cdot 67280421310721 \cdot 641 \cdot 6700417 \cdot 65537 \cdot 257 \cdot 17 \cdot 5$. За наслідком 1(b) маємо

$$O\big(\prod_{j=0}^{6} c_j\big) = 274177{\cdot}67280421310721{\cdot}O\big(\big(\prod_{j=0}^{5} c_j\big)^{274177\cdot 67280421310721+1}\big) = \prod_{j=1}^{6} N_j.$$

Враховано, що (274177·67280421310721+1, 641·6700417·65537·257·17·5)=1.

Оскільки $O(c_6c_5c_4c_3c_2c_1c_0) = N_6N_5N_4N_3N_2N_1$ і за теоремою 1 $(c_7)^{N_7} = c_6c_5c_4c_3c_2c_1c_0$ та $\alpha_7 = N_7$ є найменшим натуральним числом з властивістю $(c_7)^{N_7} \in K_5(c_6)$, то за наслідком 1(a) $O(c_7) = N_7N_6N_5N_4N_3N_2N_1$. За наслідком 1(b) отримуємо

$$O(c_7c_6c_5c_4c_3c_2c_1c_0) = N_7O((c_6c_5c_4c_3c_2c_1c_0)^{N_7+1}) = N_7N_6N_5N_4N_3N_2N_1.$$

Враховано, що $(N_7 + 1, N_6N_5N_4N_3N_2N_1) = 1$.

Так як $O(c_7c_6c_5c_4c_3c_2c_1c_0) = N_7N_6N_5N_4N_3N_2N_1$ і згідно з теоремою 1 $(c_8)^{N_8} = c_7c_6c_5c_4c_3c_2c_1c_0$ та $\alpha_8 = N_8$ є найменшим натуральним числом з властивістю $(c_8)^{N_8} \in K_6(c_7)$, то за наслідком 1(a) $O(c_8) = N_8N_7N_6N_5N_4N_3N_2N_1$. За наслідком 1(b) виконується

$$O(c_8c_7c_6c_5c_4c_3c_2c_1c_0) = N_8O((c_7c_6c_5c_4c_3c_2c_1c_0)^{N_8+1}) = N_8N_7N_6N_5N_4N_3N_2N_1.$$

Враховано, що $(N_8 + 1, N_7N_6N_5N_4N_3N_2N_1) = 1$.

Оскільки $O(c_8c_7c_6c_5c_4c_3c_2c_1c_0) = N_8N_7N_6N_5N_4N_3N_2N_1$ і згідно з теоремою 1 $(c_9)^{N_9} = c_8c_7c_6c_5c_4c_3c_2c_1c_0$ та $\alpha_9 = N_9$ є найменшим натуральним числом з властивістю $(c_9)^{N_9} \in K_7(c_8)$. Тоді за наслідком 1(a) виконується $O(c_9) = N_9N_8N_7N_6N_5N_4N_3N_2N_1$. За наслідком 1(b) виконується

$$O(c_9c_8c_7c_6c_5c_4c_3c_2c_1c_0) = N_9O((c_8c_7c_6c_5c_4c_3c_2c_1c_0)^{N_9+1}) = \prod_{j=1}^{9} N_j.$$

Враховано, що $(N_9+1, N_8N_7N_6N_5N_4N_3N_2N_1) = 1$.

Виконується $O(c_9c_8c_7c_6c_5c_4c_3c_2c_1c_0) = N_9N_8N_7N_6N_5N_4N_3N_2N_1$ і згідно з теоремою 1, $(c_{10})^{N_{10}} = c_9c_8c_7c_6c_5c_4c_3c_2c_1c_0$ та $\alpha_{10} = N_{10}$ є найменшим натуральним числом з властивістю $(c_{10})^{N_{10}} \in K_8(c_9)$. Тоді наслідок 1(a) дає $O(c_{10}) = N_{10}N_9N_8N_7N_6N_5N_4N_3N_2N_1$. За наслідком 1(b) отримуємо

$$O(c_{10}c_9c_8c_7c_6c_5c_4c_3c_2c_1c_0) = N_{10}O((c_9c_8c_7c_6c_5c_4c_3c_2c_1c_0)^{N_{10}+1}) = \prod_{j=1}^{10} N_j.$$

Враховано, що $(N_{10}+1, N_9N_8N_7N_6N_5N_4N_3N_2N_1) = 1$.

Оскільки $O(c_{10}c_9c_8c_7c_6c_5c_4c_3c_2c_1c_0) = N_{10}N_9N_8N_7N_6N_5N_4N_3N_2N_1$ і згідно з теоремою 1, $(c_{11})^{N_{11}} = c_{10}c_9c_8c_7c_6c_5c_4c_3c_2c_1c_0$ та $\alpha_{11} = N_{11}$ є найменшим натуральним числом з властивістю $(c_{11})^{N_{11}} \in K_9(c_{10})$, то за наслідком (a) $O(c_{11}) = N_{11}N_{10}N_9N_8N_7N_6N_5N_4N_3N_2N_1$. За наслідком (b) маємо

$$O(c_{11}c_{10}c_9c_8c_7c_6c_5c_4c_3c_2c_1c_0) = N_{11}O((c_{10}c_9c_8c_7c_6c_5c_4c_3c_2c_1c_0)^{N_{11}+1}) = \prod_{j=1}^{11} N_j.$$

Враховано, що $(N_{11}+1, N_{10}N_9N_8N_7N_6N_5N_4N_3N_2N_1) = 1$. $\square$

Теорема 3. *Ізоморфізми полів однакового порядку у вежах за Конвеєм та Відеманом можна задати так (кожен черговий ізоморфізм є продовженням попереднього):*

$\begin{array}{l} \mathbb{F}_2(c_0) \to \mathbb{F}_2(x_0) \\ c_0 \mapsto x_0 \end{array}$,

$\begin{array}{l} \mathbb{F}_2(c_0, c_1) \to \mathbb{F}_2(x_0, x_1) \\ c_1 \mapsto x_1x_0 \end{array}$ *та*

$\begin{array}{l} \mathbb{F}_2(c_0, \ldots, c_i) \to \mathbb{F}_2(x_0, \ldots, x_i) \\ c_i \mapsto \prod_{j=1}^{i} x_j \end{array}$ *для* $2 \le i \le 11$.

Доведення. Зауважимо, що згідно з теоремою 2, $O(c_0) = 3$, $O(c_1) = 3 \cdot 5$ та $O(c_i) = \prod_{j=1}^{i-1} N_j$ для $2 \le i \le 11$. Згідно з лемою 2, $(3, \prod_{j=1}^{i-1} N_j) = 1$. Тоді $O(c_ic_0) = \prod_{j=0}^{i-1} N_j$ для $2 \le i \le 11$.

Таким чином, елементи c_0 та x_0, c_1 та x_1x_0,c_ic_0 та $\prod_{j=0}^{i} x_j$ є примітивними елементами для відповідних полів. Співставляючи елементу c_0 елемент

x_0, елементу c_1 елемент x_1x_0, а для $2 \le i \le 11$ елементам c_i відповідно елементи $\prod_{j=0}^{i} x_j \cdot (x_0)^{-1} = \prod_{j=1}^{i} x_j$, отримуємо ізоморфізми з $\mathbb{F}_2(c_0, \ldots, c_i)$ в $\mathbb{F}_2(x_0, \ldots, x_i)$, які задано явно. $\square$

Виходячи з теореми 3, можемо буквально виписати в який елемент поля $\mathbb{F}_2(x_0, \ldots, x_i)$ переходить будь-який елемент поля $\mathbb{F}_2(c_0, \ldots, c_i)$. Враховуємо, що базовими елементами поля $\mathbb{F}_2(c_0, \ldots, c_i)$ є

$$1, c_0, \ldots, c_i, c_0c_1, \ldots, c_0c_i, \ldots, c_0 \cdots c_i.$$

Слід записати елемент поля $\mathbb{F}_2(c_0, \ldots, c_i)$ як лінійну комбінацію базових елементів із коефіцієнтами з $\mathbb{F}_2$, а тоді замінити $c_0, \ldots, c_i$ згідно з теоремою 3.

Завдання подальших досліджень: з'ясувати чи формулювання, аналогічні формулюванням теорем 1—3 справедливі для довільного $i \ge 12$.

ЛІТЕРАТУРА

1. O. Ahmadi, I.E. Shparlinski, J.F. Voloch, *Multiplicative order of Gauss periods*, Int. J. Number Theory **6**:4 (2010), 877–882.
2. Q. Cheng, *On the construction of finite field elements of large order*, Finite Fields Appl. **11**:3 (2005), 358–366.
3. R. Crandall, C. Pomerance, *Prime Numbers, A Computational Perspective*, Springer-Verlag (2005), 596 p.
4. S. Gao, *Elements of provable high orders in finite fields*, Proc. Amer. Math. Soc. **127**:6 (1999), 1615–1623.
5. H. Ito, T. Kajiwara, H. Song, *A Tower of Artin-Schreier extensions of finite fields and its applications*, JP J. Algebra, Number Theory Appl. **22**:2 (2011), 111–125.
6. G.L. Mullen, D. Panario, *Handbook of finite fields*, CRC Press (2013), 1068 p.
7. G.L. Mullen, I.E. Shparlinski, *Open problems and conjectures in finite fields*, in: Finite Fields and Applications, London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, **233** (1996), 243–268.
8. R. Popovych, *Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$*, Finite Fields Appl. **18**:4 (2012), 700–710.
9. R. Popovych, *Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$*, Finite Fields Appl. **19**:1 (2013), 86–92.
10. D. Wiedemann, *An iterated quadratic extension of GF(2)*, Fibonacci Quart., **26**:4 (1988), 290–295.
11. J.H. Conway, *On Numbers and Games*, New York: Academic Press (1976), 238 p.
12. J.H. Conway, N.J. A. Sloane. *Lexicographic Codes: Error-Correcting Codes from Game Theory*, IEEE Trans. Inf. Theory **32**:3 (1986), 337–348.

Надійшло 23.04.2014