УДК 512.624

Р. Б. Попович

СКІНЧЕННІ ПОЛЯ ЗА ЗБІГУ ХАРАКТЕРИСТИКИ ОСНОВНОГО ПОЛЯ ТА СТЕПЕНЯ РОЗШИРЕННЯ

Побудовано елементи великого порядку в мультиплікативній групі скінченного поля для випадку, коли характеристика основного поля та степінь розширення рівні.

Відомо, що мультиплікативна група скінченного поля циклічна. Її твірний елемент називають примітивним. Дослідити, як ефективно збудувати примітивний елемент та який вигляд він має важливо і теоретично, і практично. Зокрема, примітивні елементи або принаймні елементи великого порядку потрібні в низці криптографічних побудов [1, 2, 4, 6, 9, 10].

Скінченне поле з q елементів позначаємо F_q. Відомий [5] такий результат: якщо q достатньо велике, то існує такий елемент $a \in F_q$, що в розширенні $F_{q^n} = F_q(\theta)$ елемент $\theta + a$ є примітивним. Детально вивчали розширення степеня 2 та 3 [5]. Зокрема, виявили, що для розширень $F_{q^2} = F_q(\theta)$ за довільного $b \in F_q^*$ існують примітивні елементи вигляду $b(\theta + a)$, $a \in F_q$. Також доведено, що для розширень $F_{q^3} = F_q(\theta)$ існують примітивні елементи вигляду $\theta + a$, $a \in F_q$. Проте, як явно їх знайти (тобто відшукати a за розширень степенів 2 чи 3) невідомо.

У даній роботі розглядаємо явну побудову деяких елементів великого мультиплікативного порядку (зокрема, примітивних) для розширень полів вигляду F_{p^p}, де p – просте число. При цьому позначаємо:

$$O_p = (p^p - 1)/(p-1) = \sum_{i=0}^{p-1} p^i .$$

Для будь-якого простого числа p розширенням Артіна–Шраєра [1, 6] скінченного поля F_p називають поле F_{p^p}. Відомо [3, 8], що $x^p - x - a$ нерозкладний поліном над F_p для будь-якого ненульового елемента a з F_p. Тому можна вважати, що $F_{p^p} = F_p[x]/(x^p - x - a)$. Нехай $\theta \equiv x (\mathrm{mod}\, x^p - x - a)$. Зрозуміло, що $\theta^p = \theta + a$.

Для поля F_q характеристики p автоморфізм Фробеніуса – це відображення $g : F_q \to F_q$, яке кожному елементу α з F_q ставить у відповідність елемент α^p [6, 8]. Два елементи α, β з F_q називаємо спряженими, якщо $\alpha = \beta^{p^t}$. Тобто елементи спряжені, коли $\alpha = g^t(\beta)$ для деякого степеня g^t автоморфізму Фробеніуса.

Лема 1. У полі F_{p^p} спряжені елемента θ мають вигляд $\theta + \alpha$ для $i = 0, \ldots, p-1$.

Д о в е д е н н я. Спряжені елемента θ дорівнюють у цьому випадку θ^{p^i}, $i = 0, \ldots, p-1$. Покажемо, що $\theta^{p^i} = \theta + ia$ для будь-якого невід'ємного цілого i. Доведемо це індукцією по i.

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

$$\theta^{p^{i+1}} = \left(\theta^{p^i}\right)^p = (\theta + ia)^p = \theta^p + ia = \theta + (i+1)a .$$

Отже, рівність справедлива для будь-якого натурального i, що завершує доведення.

Слід зауважити, що елементи $\theta + ia$ є різними для $i = 0,\ldots, p-1$.

Норма [6, 8] елемента $\alpha \in F_{q^n}$ відносно розширення F_{q^n} поля F_q дорівнює $N_{F_{q^n}/F_q}(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i}$. Вона витримує всі степені g^t, $t = 0,\ldots, p-1$ автоморфізму Фробеніуса. Тому норма елемента належить до основного поля. Тобто норма – це відображення з F_{q^n} в F_q. Ядром цього відображення є циклічна підгрупа порядку $(q^n - 1)/(q-1)$. До неї належать елементи з нормою, рівною 1.

Лема 2. Елемент θ має в F_{p^p} мультиплікативний порядок, який є дільником числа O_p.

Д о в е д е н н я. Зрозуміло, що $\beta=\theta^{O_p} = \prod_{i=0}^{p-1} \theta^{p^i}$ – це норма елемента $N_{F_{p^p}/F_p}(\theta)$, яка належить до F_p. Оскільки $\beta=\theta^p + \sum_{i=2}^{p-1} a_i\theta^i + (p-1)!\,\theta$ та $(p-1)! \equiv -1 (\mathrm{mod}\, p)$ (за теоремою Вільсона), то, враховуючи $\theta^p - \theta = 1$ та $\sum_{i=2}^{p-1} a_i\theta^i = 0$, маємо $\beta=1$.

Лема 3. Всі елементи вигляду $\theta + ia$, $i = 0,\ldots, p-1$, мають однаковий мультиплікативний порядок.

Д о в е д е н н я. Візьмемо довільні два елементи α, β такого вигляду, який наведено в формулюванні цієї леми. Згідно з лемою 1 ці елементи є спряженими. Тобто існує такий степінь g^t автоморфізму Фробеніуса, що $\alpha = g^t(\beta)$. Зрозуміло, що g^t також є автоморфізмом. Якщо g^t – автоморфізм і $\beta^k = 1$, то тоді $g^t(\beta^k) = \alpha^k = 1$. Доведення завершене.

Числа Белла $B(n)$, $n = 0,1,\ldots$ [3, 7, 11] виникають у низці комбінаторних задач. Наприклад, $B(n)$ дає кількість розбиттів множини з n елементів. Доведено, що послідовність цих чисел за модулем довільного простого числа p є періодичною, і мінімальний період b_p ділить O_p. Висловлено гіпотезу [11], що для будь-якого простого p виконується $b_p = O_p$, та зроблено певні обчислення з перевірки гіпотези.

Позначимо мультиплікативний порядок елемента θ у полі F_{p^p} через c_p. У [3, proposition 1.2a] без доведення сформульовано таке твердження: для будь-якого простого p виконується $c_p = b_p$. Виходячи з леми 2 та відомих формулювань [3, 11], маємо таку гіпотезу про мультиплікативний порядок елемента θ.

Гіпотеза. Елемент θ має в полі F_{p^p} мультиплікативний порядок, рівний O_p.

Гіпотезу перевірили для певних значень p у середовищі комп'ютерної алгебри Maple (пакети Galois Field та NumTheory) Для цього числа O_p розклали на прості множники і потім обчислили відповідні степені елемента θ. Для піднесення до степеня використовували відомий швидкий (''індійський'') алгоритм послідовних піднесень до квадрата та множень. Для $p > 53$ розкласти O_p на прості множники не вдалося. Тут брали відомі розклади числа O_p на прості множники, отримані в межах т. зв. Cunnigham проекту [7, 11, 12].

Користуючись цими розкладами, обчислювали θ в степені O_p / q для будь-якого простого дільника q числа O_p. Дійсно, якщо елемент не дорівнює одиниці в степені O_p / q, то цей же елемент не дорівнює одиниці також у степені будь-якого дільника O_p / q.

Отримані чи взяті з літературних джерел прості множники для O_p / q наведені далі. Записи $A(p,l)$ або $B(p,l)$ позначають прості дільники O_p з l десятковими розрядами. Якщо розряди дільника не поміщаються в одному рядку, то запис переносимо в наступні рядки.

p=2, A(2,1)=3

p=3, A(3,2)=13

p=5, A(5,2)=11, B(5,2)=71

Тоді маємо розклад на прості множники $O_p = 11 \cdot 71 = 781$. Виходячи з цього розкладу, знаходимо степені елемента θ та як результат – його мультиплікативний порядок:

$\theta^{11} = \theta^3 + 2\theta^2 + \theta \neq 1$,

$\theta^{71} = 4\theta^4 + 2\theta^3 + 4\theta^2 + 3\theta + 1 \neq 1$.

Таким чином, мультиплікативнй порядок елемента θ дорівнює 781. Тоді згідно з лемою 3 мультиплікативний порядок всіх елементів вигляду $\theta + ia$ дорівнює 781.

p=7, A(7,2)=29, A(7,4)=4733

У цьому випадку $O_p = 29 \cdot 4733 = 137257$. Обчислення дали, що

$\theta^{29} = \theta^5 + 4\theta^4 + 6\theta^3 + 4\theta^2 + \theta \neq 1$,

$\theta^{4733} = \theta^6 + 5\theta^5 + 2\theta^4 + 5\theta^3 + 4\theta^2 + 2\theta + 5 \neq 1$.

Отже, мультиплікативнй порядок елемента θ дорівнює 137257. Тоді згідно з лемою 3 мультиплікативний порядок всіх елементів вигляду $\theta + ia$ також дорівнює 137257.

p=11, A(11,5)=15797, A(11,7)=1806113

Маємо: $O_p = 15797 \cdot 1806113 = 28531167061$. Обчислюючи степені θ, отримали:

$\theta^{15797} = 2\theta^{10} + 3\theta^9 + 2\theta^8 + 3\theta^7 + 4\theta^6 + 8\theta^5 + 6\theta^4 + 4\theta^3 + 3\theta^2 + 8\theta \neq 1$,

$\theta^{18061137} = 3\theta^{10} + 4\theta^9 + 8\theta^8 + 6\theta^6 + 7\theta^5 + \theta^4 + 5\theta^3 + 4\theta^2 + 6 \neq 1$.

Отже, порядок елемента θ та всіх елементів вигляду $\theta + ia$ дорівнює 28531167061.

p=13, A(13,2)=53, A(13,6)=264031, A(13,7)=1803647

p=17, A(17,5)=10949, A(17,7)=1749233, A(17,10)=2699538733

p=19, A(19,24)= 109912203092239643840221
Як бачимо, якщо p=19, то число O_p є простим, і тому без обчислень зрозуміло, що мультиплікативний порядок елемента θ дорівнює O_p.

p=23, A(23,3)=461, A(23,4)=1289, A(23,12)=831603031789,
A(23,13)= 1920647391913

p=29, A(29,2)=59, A(29,5)=16763, B(29,5)=84449, A(29,7)=2428577,
A(29,8)= 14111459, B(29,8)=58320973, A(29,9)=549334763
Оскільки згідно з [7] кожен дільник O_p (зокрема, простий дільник) має вигляд $2kp+1$ ($k \geq 1$), то цей дільник не менший від $2p+1$. У цьому випадку дільник A(29,2)=59 точно дорівнює $2p+1$.

p=31, A(31,45)=5689724710241078652870214343019771585348244 81
Якщо p=31, то число O_p є простим, і тому мультиплікативний порядок елемента θ дорівнює O_p.

p=37, A(37,3)=149, A(37,4)=1999, B(37,4)=7993, A(37,5)=16651, B(37,5)=17317,
A(37,14)=10192715656759, A(37,26)=41903425553544839998158239

p=41, A(41,2)=83, A(41,7)=1752341, A(41,8)=20567159,
A(41,19)=1876859311090803007, A(41,31)=592618758969149753779349775 6719
Дільник A(41,2)=83 точно дорівнює $2p+1$.

p=43, A(43,3)=173, A(43,6)=120401,
A(43,62)=19825223972382274003506149120708429799166030881820328923772 41

p=47, A(47,4)=1693, A(47,36)=25574249289676351147463853018887601 7,
A(47,39)=19470703301609922826706829918024401163 7

p=53, A(53,3)=107, A(53,6)=141829, A(53,17)=16505521259654533,
A(53,17)=14347072047858931328831 3473,
A(53,41)=13033960579631324880455449881408994392143
Дільник A(53,3)=107 точно дорівнює $2p+1$.

p=59, A(59,3)=709, A(59,9)=141579233,
A(59,92)=51903291854581173295562858632977054883460514085070452 51
54528413772606533396805577108032429 13

p=61, A(61,3)=977, A(61,21)=343625872243632312073,
A(61,30)=39885328645607179260991799 5907,
A(61,55)=10004032441835355657203947231405280282357118744913228 63

p=67, A(67,3)=269, A(67,4)=4021, A(67,6)=730837, A(67,8)=10960933,
A(67,34)=15149548850966040235622879157300 49,
A(67,69)=25663373411515286834250498396501067787388492016586691622470 12
15378677

p=71, A(71,6)=105649, A(71,16)=3388409395214741,
A(71,17)=17882954877203881,
A(71,93)=613683109618829730126963701125307210322365580597593081378705115087489446138913203546134827149

p=73, A(73,3)=293, B(73,3)=439, A(73,7)=1414741, A(73,8)=25239167,
B(73,8)=56377463, A(73,13)=1295720382587, A(73,16)=3611379501352361,
A(73,19)=1192167517020392933, A(73,31)=2026896285132395253381459595427,
A(73,32)=499681690027565019871194692395 79

p=79, A(79,3)=317, A(79,10)=1558537597, A(79,21)=171355071830508389477,
A(79,26)=54493132908043378263202913,
A(79,91)=22721150760046430236542239283038495399004182773576902092080250519046301344744302355875324 69

p=83, A(83,4)=2657, A(83,8)=11155201,
A(83,28)=1008505707601323349156769489,
A(83,120)=7836470444281502295741301492530485608458896884973672654179464830453763633187875989865272866159794567160521003597813795 01

p=89, A(89,3)=179, A(89,16)=8009862103557709,
A(89,25)=5964844210432006407836201,
A(89,29)=37307598912253490893302199133,
A(89,43)=257547889129853898600286691187110957470527 1,
A(89,58)=433007530959965732263437104296742837353379953456676552251 7

p=97, A(97,3)=389, A(97,6)=363751, A(97,9)=684640163,
A(97,29)=119437287337412947643906021 53,
A(97,51)=549180361199324724418373466271912931710271534073773,
A(97,95)=8541141001659286493853574226216428866075481869951936405124192796107787202862078758958760835787 7

p=101, A(101,3)=607, A(101,4)=1213, B(101,4)=5657, A(101,6)=157561,
A(101,13)=9931988588681, A(101,15)=102208068907493,
A(101,18)=393101595766008847,
A(101,53)=126029656265361098723842162970857603088232945227460 17,
A(101,89)=827704658429408347048873899828426397792600825329983113733423219236746351966679507065254 29

p=103, A(103,4)=1237, A(103,23)=16706917226363953216841,
A(103,29)=66372424944116825940401913193,
A(103,54)=167321256949237716863040684441514323749790592645938001,
A(103,98)=897075816032208374954237465384234946518940476347410879882394089886650087504711936667719658858415 73

p=107, A(107,9)=137122213, A(107,11)=10508824813,
A(107,33)=847261197784821583381604854855693,
A(107,165)=10766612031801322134832621304679109736373060932198056581051145604641198117773763593541448030606366150345328023553083957066087322041965629823766202433001015490024372 1

p=109, A(109,4)=2617, A(109,25)=619609874313908289143863 1,
A(109,49)=708022605183994255434421517741836511379166407220 3,
A(109,58)=208713939295518862111380319002407112397476975917955337364 9
A(109,86)=464027680737994183678386213462383636318527230770013415699738962634317307438534121839 69

p=113, A(113,3)=227, A(113,4)=3391, B(113,4)=8363,
A(113,14)=34314816732569,
A(113,33)=7851928002561978986444431714786031,
A(113,47)=70739255769077616674066085318030811655932920203,
A(113,53)=463619438165353893856898038800353703519601461561358 49,
A(113,75)=1561889236249215987064296398692807838315177531265990839213472258388741375 07

p=137, A(137,4)=1097, A(137,6)=124123, A(137,10)=1918644449,
A(137,11)=12779722229, A(137,12)=574894288613, A(137,15)=271329112787027,
A(137,26)=54142883557383383180139791,
A(137,34)=17594294674609358799167756101806 59,
A(137,35)=14502230930480689611402075474137987,
A(137,59)=588561079227779241809167742182641919130595839705607470527 99,
A(137,85)=9340712325594008400934073398698792409828571275985973473156933906783567493646870672273

p=163, A(163,3)=653, A(163,4)=2609, A(163,5)=41729, A(163,8)=31943437,
A(163,13)=3727539197017, A(163,15)=391683908074297,
A(163,19)=8224734227858383253,
A(163,294)=8737311135691969908908359861921291734095248866944470440653588068701193660798779198131419445276000644071895299435327655357981750502071264503065600754938066701030793023660875799632154458829571951323912188569789946641082872903093045449356906102825252638400510363461187067126334012720104708691122 09

p=167, A(167,5)=16033, A(167,13)=1001953110409,
A(167,27)=669806250678629514045626189,
A(167,326)=8744423991851334720041720676388526687848659201769747545227549280252410764892276440966976400544033999957633617421527720575301075514494476301446175118650888938294837811574570530306804238215680798973780373369560733466176225637697189917673613153190594814658944874220613663405070214647381181379826577241190480565776657236747588854 9

У результаті виконаних обчислень з'ясовано, що наведена раніше гіпотеза справедлива для p<126 та для p=137,163,167,173. Тобто з урахуванням леми 3 маємо такий результат.

Теорема 1. Елемент $\theta + ia$, $i = 0,...,p-1$, має в F_{p^p} мультиплікативний порядок, рівний O_p для p<126 та для p=137,163,167,173.

Для наведених далі простих чисел p повні розклади O_p на прості множники знайдені [7, 11], але в літературі наведені не всі множники.

p=149, A(149,4)=1193, A(149,8)=51784951, A(149,9)=450090559,
B(149,9)=465814231,
A(149,44)=14897084928588789671974072568141537826492971,
A(149,53)=24356237167368011037018270166971738740925336580189261,
A(149,84), A(149,115) - не наведені в літературі прості множники.

p=157, A(157,3)=347, A(157,5)=86351, A(157,6)=685081,
A(157,13)=1356984109417,
A(157,61)=269246276242763276898122337166239758557650345281852679342077 3,
A(157,99), A(157,167)

p=173, A(173,18)=161297590410850151,
A(173,176), A(173,184)

Далі подано прості числа p, для яких повні розклади O_p на прості множники на сьогодні невідомі. Позначення $C(p,l)$ означає складений дільник O_p з l десятковими розрядами, розклад якого невідомий.

p=127, A(127,3)=509, A(127,5)=22861,A(127,25)=1320675600886906675359917,
C(127,234) - складений дільник з невідомим розкладом.

p=131, A(131,4)=1049, A(131,18)=1742643541410742623061,
C(131,251)

p=139, A(139,3)=557, A(139,12)=119833345601,
C(139,282)

p=151, A(151,4)=2417, A(151,5)=15101, A(151,7)=1234577,
A(151,37)=760658609581520401030226740176590735 3,
C(151,277)

p=179, A(179,33)=6183119082113155839913145480811 49,
C(179,369)

Використовуючи наведені часткові розклади (розклади з невідомими простими або зі складеними множниками), перевірили для всіх можливих випадків, що порядок елемента θ не є власним дільником O_p.

Таким чином, виконані обчислення показують, що наведена на початку гіпотеза, ймовірно, виконується для більшості простих чисел. Тоді елемент θ та спряжені з ним мають великий мультиплікативний порядок, рівний O_p. Виходячи з цього, можна явно збудувати деякі примітивні елементи в розширеннях Артіна–Шраєра.

Теорема 2. Якщо α – примітивний елемент в F_p і елемент θ має в F_{p^p} мультиплікативний порядок O_p, то елемент $\alpha(\theta+ia)^j$ ($i=0,\dots,p-1$; $j=1,\dots,p-1$) – примітивний в F_{p^p}.

Д о в е д е н н я. Покажемо спочатку, що числа $p-1$ та $O_p = p^{p-1}+\dots+1$ взаємно прості. Дійсно, нехай t є дільником $p-1$. Тоді $p \equiv 1 \bmod t$ і $p^{p-1}+\dots+1 \equiv 1+\dots+ = p \equiv 1 \bmod t$, тобто $p^{p-1}+\dots+1$ не ділиться на t.

Таким чином, мультиплікативна група поля F_{p^p} є внутрішнім прямим добутком двох підгруп: з $p-1$ та з O_p елементів. Елемент α породжує підгрупу з $p-1$ елементів, а елемент $\theta+ia$ – підгрупу з O_p елементів. Значить, елемент $\alpha(\theta+ia)$ примітивний в F_{p^p}.

Як зауважено раніше, кожен дільник O_p не менший від $2p+1$. Тоді найбільший спільний дільник числа від 2 до $p-1$ й O_p дорівнює 1. Отже, порядок елемента $(\theta+ia)^j$ $(j=2,\dots,p-1)$ збігається з порядком $\theta+ia$ і дорівнює O_p. Елемент α породжує підгрупу з $p-1$ елементів, а $(\theta+ia)^j$ –

підгрупу з O_p елементів. Таким чином, елемент $\alpha(\theta + ia)^j$ примітивний в F_{p^p}. Доведення завершене.

Як видно з наведених раніше розкладів, O_p може бути простим числом.

Теорема 3. Якщо O_p просте число, то всі примітивні елементи поля F_{p^p} мають вигляд $\alpha \cdot u$, де α – примітивний елемент в F_p, а u – неодиничний елемент поля F_{p^p} з нормою 1.

Д о в е д е н н я. Мультиплікативна група $F^*_{p^p}$ розширення Артіна–Шраєра є внутрішнім прямим добутком підгрупи F^*_p та підгрупи з O_p елементів.

Елемент ц породжує підгрупу F^*_p. Оскільки O_p – просте число, то в підгрупі A з O_p елементів кожен неодиничний елемент є твірним. Всі елементи з A (і тільки вони) мають норму 1. У результаті отримуємо твердження теореми.

Зауважимо, що крім примітивних елементів вигляду $\alpha(\theta + ia)^j$ (кількість яких дорівнює $(p-1)\cdot p \cdot \lambda(p-1)$, де λ позначає функцію Ейлера), в полі F_{p^p} є також інші примітивні елементи, оскільки їх загальна кількість $\lambda(p^p - 1) = \lambda(p-1)\cdot\lambda(O_p)$.

Теорема 4. Множина примітивних елементів поля F_{p^p} розбивається на підмножини по p спряжених елементів у кожній.

Д о в е д е н н я. Спочатку покажемо, що загальна кількість примітивних елементів $\lambda(p-1)\cdot\lambda(O_p)$ ділиться на p. Для цього досить показати, що на p ділиться співмножник $\lambda(O_p)$. Дійсно, функція Ейлера λ володіє властивістю мультиплікативності. Число O_p має хоча б один простий дільник і його записують як $2kp+1$ для деякого натурального k. Тоді $\lambda(O_p)$ ділиться на $\lambda(2kp+1) = 2kp$.

Будь-який примітивний елемент поля F_{p^p} має p спряжених елементів [6]. Неважко перевірити, що спряженість елементів є відношенням еквівалентності. Тоді дві підмножини попарно спряжених елементів або не перетинаються або збігаються. Доведення завершене.

Випишемо всі примітивні елементи, якщо $p = 3$, тобто для поля F_{3^3}. Кількість елементів мультиплікативної групи поля дорівнює $26 = 2\cdot 13$. Усього в цьому полі $\lambda(26)=\lambda(2)\cdot\lambda(13)=12$ примітивних елементів, а у полі F_3 – лише один, який дорівнює 2. Мультиплікативнй порядок елементів θ, $\theta+1$, $\theta+2$ дорівнює 13. Кожен з цих елементів породжує підгрупу з $O_p = 13$ елементів.

Згідно з теоремою 3 елемент 2θ є примітивним. Спряжені з ним примітивні елементи: $2\theta+1$, $2\theta+2$. За теоремою 3 елемент $2\theta^2$ також є примітивним. Спряжені з ним примітивні елементи: $2\theta^2+\theta+2$, $2\theta^2+2\theta+2$. Наведені шість примітивних елементів є елементами вигляду, що описаний

у теоремі 3. Наведені далі шість примітивних елементів не є примітивними елементами такого вигляду.

Обчислення дали, що елемент $2\theta^2+1$ дорівнює θ^8. Тобто цей елемент належить до підгрупи елементів з нормою 1. Тоді згідно з теоремою 4 елемент $2(2\theta^2+2)=\theta^2+1$ є примітивним. Спряжені з ним примітивні елементи: $\theta^2+2\theta+2$, $\theta^2+\theta+2$.

Виконані обчислення засвідчують, що елемент θ^2+2 дорівнює θ^{12}. Тобто він належить до підгрупи елементів з нормою 1. Тоді згідно з теоремою 4 елемент $2(\theta^2+2)=2\theta^2+1$ є примітивним. Спряжені з ним примітивні елементи: $2\theta^2+\theta$, $\theta^2+2\theta$.

Як бачимо, у цьому прикладі множина з 12 примітивних елементів розбивається на 4 підмножини по 3 спряжених примітивних елементи в кожній підмножині. Усі 12 примітивних елементів є елементами вигляду, описаного теоремою 4.

1. *Попович Р.* Елементи великого порядку в розширеннях Артіна–Шраєра скінченних полів // Матем. студії – 2013. – **39**, № 2 – С. 115–118.
2. *Burkhart J.F. et al.* Finite field elements of high order arising from modular curves // Des. Codes Cryptogr. – 2009. – **51**, № 3 – P. 301–314.
3. *Car M., Gallardo L. H., Rahavandrainy O., Vaserstein L. N.* About the period of Bell numbers modulo a prime // Bull. Korean Math. Soc. – 2008. – **45**, № 1 – P. 143–155.
4. *Cheng Q.* On the construction of finite field elements of large order // Finite Fields Appl. – 2005. – **11**, № 3 – P. 358–366.
5. *Cohen S. D.* Primitive elements on lines in extensions of finite fields // Finite fields. Theory and applications: Proc. 9-th Int. Conf. (Ireland, 13–17 July 2009). – Amer. Math. Soc., Providence, RI, 2010. – P. 113–127.
6. *Lidl R., Niederreiter H.* Finite Fields. – Cambridge: Cambridge University Press, 1997. – 756 p.
7. *Montgomery P., Nahm S., Wagstaff S.Jr.* The period of the Bell numbers modulo a prime // Math. Comp. – 2010. – **79**, № 281 – P. 1793–1800.
8. *Mullen L., Panario D.* Handbook of finite fields. – London: CRC Press, 2013. – 1068 p.
9. *Popovych R.* Elements of high order in finite fields of the form $F_g[x]/\Phi_r(x)$ // Finite Fields Appl. – 2012. – **18**, № 4 – P. 700–710.
10. *Popovych R.* Elements of high order in finite fields of the form $F_g[x]/(x^m-a)$ // Ibid. – 2013. – **19**, № 1 – P. 86–92.
11. *Wagstaff S.Jr.* Aurifeuillian factorizations and the period of the Bell numbers modulo a prime // Math. Comp. – 1996. – **65**, № 213 – P. 383–391.
12. http://maths-people.anu.edu.au/~brent/factors.html

КОНЕЧНЫЕ ПОЛЯ ПРИ СОВПАДЕНИИ ХАРАКТЕРИСТИКИ ОСНОВНОГО ПОЛЯ И СТЕПЕНИ РАСШИРЕНИЯ

Построены элементы большого порядка в мультипликативной группе конечного поля для случая, когда характеристика основного поля и степень расширения равны.

FINITE FIELDS IN COINCIDENCE OF BASIC FIELD CHARACTERISTIC AND EXTENSION DEGREE

We consider a construction of high order elements in finite field multiplicative group for the case, when base field characteristic and extension degree are equal.

Нац. ун-т "Львівська політехніка", Львів

Одержано 29.08.14