Український математичний вісник
Том 12 **(2015)**, № 1, 85 – 95

Деякі примітивні елементи для розширень Артіна–Шраєра скінченних полів

Роман Б. Попович

(*Представлена В. Я. Гутлянським*)

Анотація. Дається явний опис певних твірних елементів мультиплікативної групи скінченних полів вигляду F_{p^p} для $p \geq 2$.

2010 MSC. 11T30.

Ключові слова та фрази. скінченне поле, примітивний елемент, мультиплікативний порядок.

1. Вступ та допоміжні результати

Відомо, що мультиплікативна група скінченого поля є циклічною. Її твірний елемент називають примітивним елементом. Дослідження питання, як ефективно збудувати примітивний елемент та який вигляд він має, є важливим як з теоретичної, так і з прикладної точки зору. Зокрема, примітивні елементи або принаймні елементи великого порядку потрібні в низці криптографічних побудов [1–5].

Скінченне поле з q елементів позначаємо F_q. Відомий [6] 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 проводилось вивчення розширень степеня 2 та 3 [6]. Зокрема, показано, що для розширень $F_{q^2} = F_q(\theta)$ існують примітивні елементи вигляду $\beta(\theta + a)$, $a \in F_q$, для довільного $\beta \in F_q^*$. Також доведено, що для розширень $F_{q^3} = F_q(\theta)$ існують примітивні елементи вигляду $\theta + a$, $a \in F_q$. Проте, як явно знайти згадані примітивні елементи (тобто знайти a у випадку розширень степеня 2 чи a та β у випадку розширень степеня 3) невідомо.

У даній роботі розглядаємо питання явної побудови деяких примітивних елементів для розширень полів вигляду F_{p^p}, де p - просте число. При цьому позначаємо $O_p = (p^p - 1)/(p - 1) = \sum_{i=0}^{p-1} p^i$.

Стаття надійшла в редакцію 20.01.2014

Для будь-якого простого числа p розширенням Артіна–Шраєра [1,7] скінченого поля F_p називають поле F_{p^p}. Відомо [8,9], 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 $F_{p^p} = F_p[x]/(x^p-x-a)$. Нехай $\theta = x(\bmod\ x^p-x-a)$. Зрозуміло, що $\theta^p = \theta+a$.

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 [7,8]. Два елементи α, β з F_q називаємо спряженими, якщо

$$\alpha = \beta^{p^t}.$$

Тобто, елементи спряжені, коли $\alpha = \varphi^t(\beta)$ для деякого степеня φ^t автоморфізму Фробеніуса.

Лема 1.1. *У полі F_{p^p} спряжені елемента θ мають вигляд $\theta+ia$ для $i = 0, \ldots, p-1$.*

Доведення. Спряжені елемента θ дорівнюють у даному випадку θ^{p^i}, $i = 0, \ldots, p-1$. Покажемо, що $\theta^{p^i} = \theta+ia$ для будь-якого натурального 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:

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

Отже, рівність справедлива для будь-якого натурального i. □

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

Відносно розширення F_{q^n} поля F_q норма [7,8] елемента $\alpha \in F_{q^n}$ дорівнює $N_{F_{q^n}/F_q}(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i}$. Норма елемента витримує всі степені $\varphi^t,\ t = 0, \ldots, p-1$ 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 $(q^n-1)/(q-1)$. Зрозуміло, що до неї належать елементи з нормою рівною 1.

Лема 1.2. *Елемент θ має в F_{p^p} мультиплікативний порядок, який є дільником O_p.*

Доведення. Зрозуміло, що $\beta = \theta^{c_p} = \prod_{i=0}^{p-1} \theta^{p^i}$ — 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 $(p-1)! \equiv -1(\bmod\ p)$ (за теоремою Вільсона), то, враховуючи $\theta^p - \theta = 1$ та $\sum_{i=2}^{p-1} a_i\theta^i = 0$, маємо $\beta = 1$. □

Лема 1.3. *Всі елементи вигляду $\theta + ia$, $i = 0, \dots, p-1$, мають однаковий мультиплікативний порядок.*

Доведення. Візьмемо довільні два елементи α, β вказаного в формулюванні леми вигляду. Згідно з лемою 1.1 ці елементи є спряженими. Тобто існує такий степінь φ^t автоморфізму Фробеніуса, що

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

Зрозуміло, що φ^t також є автоморфізмом. Якщо φ^t — автоморфізм і $\beta^k = 1$, то тоді $\varphi^t(\beta^k) = \alpha^k = 1$. □

2. Основні результати

Числа Белла $B(n), n = 0, 1, \dots$ [9–11] 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. У [10] висловлено гіпотезу, що для будь-якого простого p виконується $b_p = O_p$, та виконано певні обчислення з перевірки гіпотези.

Позначимо мультиплікативний порядок елемента θ в полі F_{p^p} через c_p. У [9, Proposition 1.2, a)] без доведення сформульовано таке твердження: для будь-якого простого p виконується $c_p = b_p$.

Виходячи з леми 1.2 та формулювань в [9, 10] маємо таку гіпотезу відносно мультиплікативного порядку елемента θ.

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

Ми виконували перевірку гіпотези для певних значень p в середовищі комп'ютерної алгебри Maple (пакети Galois Field та NumTheory). Перевірка зводиться до розкладу числа O_p на прості множники і потім обчислення відповідних степенів елемента θ. Для піднесення до степеня використовували відомий швидкий ("індійський") алгоритм послідовних піднесень до квадрату та множень.

Для $p > 53$ розклад O_p на прості множники не вдалося виконати. У цьому разі брали відомі розклади числа O_p на прості множники, отримані в рамках так званого Cunnigham проекту [10–12].

Користуючись вказаними 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 ж елемент не дорівнює одиниці також в степені будь-якого дільника O_p/q.

Отримані чи взяті з літературних джерел прості множники для O_p наведені далі. Позначення $A_l^{(p)}$ або $B_l^{(p)}$ означають прості дільники

O_p з l десятковими розрядами. Якщо розряди дільника не поміщаються в одному рядку, то запис переносимо в наступні рядки.
$p = 2$, $A_1^{(2)} = 3$
$p = 3$, $A_2^{(3)} = 13$
$p = 5$, $A_2^{(5)} = 11$, $B_2^{(5)} = 71$
У даному випадку 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 $781 = 11 \cdot 71$. Тоді згідно з лемою 1.3 мультиплікативний порядок всіх елементів вигляду $\theta + ia$ дорівнює 781.
$p = 7$, $A_2^{(7)} = 29$, $A_4^{(7)} = 4733$
У даному випадку $O_p = 29 \cdot 4733 = 137257$. Обчислення дали, що

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

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

Значить, мультиплікативнй порядок елемента θ дорівнює $137257 = 29 \cdot 4733$. Тоді згідно з лемою 1.3 мультиплікативний порядок всіх елементів вигляду $\theta + ia$ також дорівнює 137257.
$p = 11$, $A_5^{(11)} = 15797$, $A_7^{(11)} = 1806113$
Маємо $O_p = 15797 \cdot 1806113 = 28531167061$. Обчислюючи степені θ, отримали

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

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

Отже, порядок елемента θ та всіх елементів вигляду $\theta + ia$ дорівнює $28531167061 = 15797 \cdot 1806113$.
$p = 13$, $A_2^{(13)} = 53$, $A_6^{(13)} = 264031$, $A_7^{(13)} = 1803647$
$p = 17$, $A_5^{(17)} = 10949$, $A_7^{(17)} = 1749233$, $A_{10}^{(17)} = 2699538733$
$p = 19$, $A_{24}^{(19)} = 109912203092239643840221$
Як бачимо, у випадку $p = 19$ число O_p є простим, і тому без обчислень зрозуміло, що мультиплікативний порядок елемента θ дорівнює O_p.
$p = 23$, $A_3^{(23)} = 461$, $A_4^{(23)} = 1289$, $A_{12}^{(23)} = 831603031789$,
$A_{13}^{(23)} = 1920647391913$

$p = 29$, $A_2^{(29)} = 59$, $A_5^{(29)} = 16763$, $B_5^{(29)} = 84449$, $A_7^{(29)} = 2428577$, $A_8^{(29)} = 14111459$, $B_8^{(29)} = 58320973$, $A_9^{(29)} = 549334763$
Оскільки згідно з [11] кожен дільник O_p (зокрема, простий дільник) має вигляд $2kp + 1$ $(k \geq 1)$, то цей дільник не менший від $2p + 1$. У даному випадку дільник $A_2^{(29)} = 59$ точно дорівнює $2p + 1$.
$p = 31$, $A_{45}^{(31)} = 56897247102410786528702143430197715853482448 1$
У випадку $p = 31$ число O_p є простим, і тому мультиплікативний порядок елемента θ дорівнює O_p.
$p = 37$, $A_3^{(37)} = 149$, $A_4^{(37)} = 1999$, $B_4^{(37)} = 7993$, $A_5^{(37)} = 16651$,
$B_5^{(37)} = 17317$, $A_{14}^{(37)} = 10192715656759$,
$A_{26}^{(37)} = 41903425553544839998158239$
$p = 41$, $A_2^{(41)} = 83$, $A_7^{(41)} = 1752341$, $A_8^{(41)} = 20567159$,
$A_{19}^{(41)} = 1876859311090803007$,
$A_{31}^{(41)} = 592618758969149753779349775 6719$
Дільник $A_2^{(41)} = 83$, точно дорівнює $2p + 1$.
$p = 43$, $A_3^{(43)} = 173$, $A_6^{(43)} = 120401$
$A_{62}^{(43)} = 19825223972382274003506149120708429799166030881820328923772 41$
$p = 47$, $A_4^{(47)} = 1693$, $A_{36}^{(47)} = 25574249289676351147463853018887601 7$
$A_{39}^{(47)} = 19470703301609922826706829918024401163 7$
$p = 53$, $A_3^{(53)} = 107$, $A_6^{(53)} = 141829$, $A_{17}^{(53)} = 16505521259654533$
$A_{27}^{(53)} = 14347072047858931328831 3473$
$A_{41}^{(53)} = 13033960579631324880455449881408994392143$
Дільник $A_3^{(53)} = 107$ точно дорівнює $2p + 1$.
$p = 59$, $A_3^{(59)} = 709$, $A_9^{(59)} = 141579233$
$A_{92}^{(59)} = 51903291854581173295562858632977054883460514085070452515452841377260653339680557710803242913$
$p = 61$, $A_3^{(61)} = 977$, $A_{21}^{(61)} = 343625872243632312073$
$A_{30}^{(61)} = 39885328645607179260991799 5907$
$A_{55}^{(61)} = 10004032441835355657203947231405280282357118744913228 63$
$p = 67$, $A_3^{(67)} = 269$, $A_4^{(67)} = 4021$, $A_6^{(67)} = 730837$, $A_8^{(67)} = 10960933$
$A_{34}^{(67)} = 15149548850966040235622879157300 49$
$A_{69}^{(67)} = 25663373411515286834250498396501067787388492016586691622470121537867 7$
$p = 71$, $A_6^{(71)} = 105649$, $A_{16}^{(71)} = 3388409395214741$,
$A_{17}^{(71)} = 17882954877203881$

$A_{93}^{(71)} = 61368310961882973012696370112530721032236558059759308137870511508748944613891320354613482714 9$

$p = 73$, $A_2^{(73)} = 293$, $B_2^{(73)} = 439$, $A_7^{(73)} = 1414741$

$A_8^{(73)} = 25239167$, $B_8^{(73)} = 56377463$, $A_{13}^{(73)} = 1295720382587$,

$A_{16}^{(73)} = 3611379501352361$, $A_{19}^{(73)} = 1192167517020392933$

$A_{31}^{(73)} = 2026896285132395253381459595427$

$A_{32}^{(73)} = 49968169002756501987119469239579$

$p = 79$, $A_3^{(79)} = 317$, $A_{10}^{(79)} = 1558537597$,

$A_{21}^{(79)} = 171355071830508389477$, $A_{26}^{(79)} = 54493132908043378263202913$

$A_{91}^{(79)} = 22721150760046430236542239283038495399004182773576902092080250519046301344744302355875324 69$

$p = 83$, $A_4^{(83)} = 2657$, $A_8^{(83)} = 11155201$,

$A_{28}^{(83)} = 10085057076013233491567694 89$

$A_{120}^{(83)} = 78364704442815022957413014925304856084588968849736726541794648304537636331878759898652728661597945671605210035978137950 1$

$p = 89$, $A_3^{(89)} = 179$

$A_{16}^{(89)} = 8009862103557709$, $A_{25}^{(89)} = 5964844210432006407836201$

$A_{29}^{(89)} = 37307598912253490893302199133$

$A_{43}^{(89)} = 25754788912985389860028669118711095747052 71$

$A_{58}^{(89)} = 43300753095996573226343710429674283735337995345667655225 17$

$p = 97$, $A_3^{(97)} = 389$, $A_6^{(97)} = 363751$, $A_9^{(97)} = 684640163$,

$A_{29}^{(97)} = 119437287337412947643906021 53$

$A_{51}^{(97)} = 549180361199324724418373466271912931710271534073773$

$A_{95}^{(97)} = 85411410016592864938535742262164288660754818699519364051241927961077872028620787589587608357877$

$p = 101$, $A_3^{(101)} = 607$, $A_4^{(101)} = 1213$, $B_4^{(101)} = 5657$, $A_6^{(101)} = 157561$

$A_{13}^{(101)} = 9931988588681$, $A_{15}^{(101)} = 102208068907493$,

$A_{18}^{(101)} = 393101595766008847$

$A_{53}^{(101)} = 126029656265361098723842162970857603088232945227460 17$

$A_{89}^{(101)} = 82770465842940834704887389982842639779260082532998311373342321923674635196667950706525429$

$p = 103$, $A_4^{(103)} = 1237$, $A_{23}^{(103)} = 16706917226363953216841$

$B_{29}^{(103)} = 66372424944116825940401913193$

$A_{54}^{(103)} = 16732125694923771686304068444151432374979059264593800 1$

$A_{98}^{(103)} = 89707581603220837495423746538342394651894047634741087988239408988665008750471193666771965885841573

$p = 107$, $A_9^{(107)} = 137122213$, $A_{11}^{(107)} = 10508824813$
$B_{33}^{(107)} = 847261197784821583381604854855693$
$A_{165}^{(107)} = 10766612031801322134832621304679109736373060932198056581051145604641198117773763593541448030606366150345328023553083957066087322041965629823766202433001015490024372 1$
$p = 109$, $A_4^{(109)} = 2617$, $A_{25}^{(109)} = 619609874313908289143863 1$
$B_{49}^{(109)} = 708022605183994255434421517741836511379166407220 3$,
$A_{58}^{(109)} = 208713939295518862111380319002407112397476975917955337364 9$
$A_{86}^{(109)} = 464027680737994183678386213462383636318527230770013415699738962634317307438534121839 69$
$p = 113$, $A_3^{(113)} = 227$, $A_4^{(113)} = 3391$, $B_4^{(113)} = 8363$,
$A_{14}^{(113)} = 34314816732569$,
$A_{33}^{(113)} = 785192800256197898644431714786031$
$A_{47}^{(113)} = 707392557690776166740660853180308116559329202 03$
$A_{53}^{(113)} = 463619438165353893856898038800353703519601461561358 49$
$A_{75}^{(113)} = 156188923624921598706429639869280783831517753126599083921347225838874137507$
$p = 137$, $A_4^{(137)} = 1097$, $A_6^{(137)} = 124123$, $A_{10}^{(137)} = 1918644449$,
$A_{11}^{(137)} = 12779722229$, $A_{12}^{(137)} = 574894288613$
$A_{15}^{(137)} = 271329112787027$, $A_{26}^{(137)} = 54142883557383383180139791$
$A_{34}^{(137)} = 17594294674609358799167756101806 59$
$A_{35}^{(137)} = 14502230930480689611402075474137987$
$A_{59}^{(137)} = 588561079227779241809167742182641919130595839705607470527 99$
$A_{85}^{(137)} = 934071232559400840093407339869879240982857127598597347315693390678356749364687067227 3$
$p = 163$, $A_3^{(163)} = 653$, $A_4^{(163)} = 2609$, $A_5^{(163)} = 41729$,
$A_8^{(163)} = 31943437$, $A_{13}^{(163)} = 3727539197017$, $A_{15}^{(163)} = 391683908074297$
$A_{19}^{(163)} = 8224734227858383253$
$A_{294}^{(163)} = 873731113569196990890835986192129173409524886694447044065358806870119366079877919813141944527600064407189529943532765535798175050207126450306560075493806670103079302366087579963215445882957195132391218856978994664108287290309304544935690610282525263840051036346118706712633401272010470869112209$
$p = 167$, $A_5^{(167)} = 16033$, $A_{13}^{(167)} = 1001953110409$,
$A_{27}^{(167)} = 669806250678629514045626189$
$A_{326}^{(167)} = 87444239918513347200417206763885266878486592017697475 4$

52275492802524107648922764409669764005440339999576336174215277
20575301075514494476301446175118650888938294837811574570530306
80423821568079897378037336956073346617622563769718991767361315
31905948146589448742206136634050702146473811813798265772411904
80565776657236747588854 9.

У результаті проведених обчислень з'ясовано, що наведена раніше гіпотеза справедлива для $p < 126$ та для $p = 137, 163, 167, 173$. Тобто, з врахуванням леми 1.3 маємо такий результат.

Теорема 2.1. *Елемент $\theta+ia$, $i = 0, \ldots, p-1$, 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 повні розклади O_p на прості множники знайдені [10,11], але в літературі наведені не всі множники.
$p = 149$, $A_4^{(149)} = 1193$, $A_8^{(149)} = 51784951$,
$A_9^{(149)} = 450090559$, $B_9^{(149)} = 465814231$,
$A_{44}^{(149)} = 14897084928588789671974072568141537826492971$,
$A_9^{(149)} = 24356237167368011037018270166971738740925336580189261$,
$A_{84}^{(149)}$, $A_{115}^{(149)}$ – не наведені в літературі прості множники.
$p = 157$, $A_3^{(157)} = 347$, $A_5^{(157)} = 86351$, $A_6^{(157)} = 685081$,
$A_{13}^{(157)} = 1356984109417$,
$A_{61}^{(157)} = 269246276242763276898122337166239758557650345281852679$
3420773, $A_{99}^{(157)}$, $A_{167}^{(157)}$
$p = 173$, $A_{18}^{(173)} = 161297590410850151$, $A_{176}^{(173)}$, $A_{184}^{(173)}$

Далі наведено прості числа, для яких повні розклади O_p на прості множники на даний час невідомі. Позначення $C_l^{(p)}$ означає складений дільник O_p, розклад якого невідомий, з l десятковими розрядами.
$p = 127$, $A_3^{(127)} = 509$, $A_5^{(127)} = 22861$,
$A_{25}^{(173)} = 1320675600886906675359917$, $C_{234}^{(173)}$ – складений дільник з невідомим розкладом.
$p = 131$, $A_4^{(131)} = 1049$, $A_{18}^{(131)} = 1742643541410742623061$, $C_{251}^{(131)}$
$p = 139$, $A_3^{(139)} = 557$, $A_{12}^{(139)} = 119833345601$, $C_{282}^{(139)}$
$p = 151$, $A_4^{(151)} = 2417$, $A_5^{(151)} = 15101$, $A_7^{(151)} = 1234577$,
$A_{37}^{(151)} = 760658609581520401030226740176590735 3$, $C_{277}^{(151)}$
$p = 179$, $A_{33}^{(179)} = 6183119082113155839913145480811 49$, $C_{369}^{(179)}$

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

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

Теорема 2.2. *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}.*

Доведення. 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 $p^{p-1} + \dots + 1 \equiv 1 + \dots + 1 = p \equiv 1 \bmod t$, 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 $p-1$ елементів та з O_p елементів. Елемент α породжує підгрупу з $p-1$ елементів, елемент а $\theta + ia$ породжує підгрупу з O_p елементів. Значить, елемент $\alpha(\theta + ia)$ — примітивний в F_{p^p}

Оскільки кожен дільник O_p (зокрема простий) має вигляд $2kp+1$ $(k \geq 1)$ [11], то цей дільник не менший від $2p+1$. Тоді найбільший спільний дільник числа від 2 до $p-1$ й O_p дорівнює 1. Значить порядок елемента $(\theta + ia)^j$ $(j = 2, \dots, p-1)$ співпадає з порядком $(\theta + ia)$ і дорівнює O_p. α породжує підгрупу з $p-1$ елементів, а $(\theta + b)^i$ породжує підгрупу з O_p елементів. Таким чином, елемент $\alpha(\theta + b)^i$ — примітивний в F_{p^p}. □

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

Теорема 2.3. *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.

Доведення. Мультиплікативна група $F^*_{p^p}$ розширення Артіна–Шраєра є внутрішнім прямим добутком підгрупи F^*_p та підгрупи з O_p елементів.

Елемент α 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. □

Зауваження 2.1. Крім примітивних елементів вигляду $\alpha(\theta + b)^i$ (кількість яких дорівнює $\varphi(p-1)(p-1)p$) в полі F_{p^p} є також інші

примітивні елементи, оскільки їх загальне число дорівнює $\varphi(p^p-1) = \varphi(p-1)\varphi(O_p)$.

Теорема 2.4. *Множина примітивних елементів поля F_{p^p} розбивається на підмножини по p спряжених елементів у кожній.*

Доведення. Спочатку покажемо, що загальне число примітивних елементів $\varphi(p-1)\varphi(O_p)$ ділиться на p. Для цього досить показати, що на p ділиться співмножник $\varphi(O_p)$. Дійсно, функція Ейлера φ має властивість мультиплікативності. O_p має хоча б один простий дільник і він є вигляду $2kp+1$ для деякого натурального k. Тоді $\varphi(O_p)$=2kp.

Будь-який примітивний елемент поля F_{p^p} має p спряжених елементів [7]. Неважко перевірити, що спряженість елементів є відношенням еквівалентності. Тоді дві підмножини попарно спряжених елементів або не перетинаються або співпадають. □

Приклад 2.1. Випишемо всі примітивні елементи у випадку $p = 3$, тобто для поля F_{3^3}. Кількість елементів мультиплікативної групи поля дорівнює $26 = 2{\cdot}13$. Усього в цьому полі є $\varphi(26) = \varphi(2)\varphi(13) = 12$ примітивних елементів. У полі F_3 є лише один примітивний елемент, 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 2.3 елемент 2θ є примітивним. Спряжені з ним примітивні елементи: $2\theta+1$, $2\theta+2$.

Згідно з теоремою 2.3 елемент $2\theta^2$ також є примітивним. Спряжені з ним примітивні елементи: $2\theta^2+\theta+2$, $2\theta^2+2\theta+2$.

Наведені 6 примітивних елементів є елементами вигляду, описаного в теоремі 2.3. 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 2.4 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 показують, що елемент θ^2+2 дорівнює θ^{12}. Тобто цей елемент належить до підгрупи елементів з нормою 1. Тоді згідно з теоремою 2.4 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 даному 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 2.4.

Література

[1] Р. Попович, *Елементи великого порядку в розширеннях Артіна–Шраєра скінченних полів* // Мат. студії, **39** (2013), No. 3, 115–118.

[2] J. F. Burkhart et al., *Finite field elements of high order arising from modular curves* // Des. Codes Cryptogr., **51**, (2009) No. 3, 301–314.

[3] Q. Cheng, *On the construction of finite field elements of large order* // Finite Fields Appl., **11** (2005), No. 3, 358–366.

[4] R. Popovych, *Elements of high order in finite fields of the form* $F_q[x]/\Phi_r(x)$ // Finite Fields Appl., **18** (2012), No. 4, 700–710.

[5] R. Popovych, *Elements of high order in finite fields of the form* $F_q[x]/(x^m - a)$ // Finite Fields Appl., **19** (2013), No. 1, 86–92.

[6] S. D. Cohen, *Primitive elements on lines in extensions of finite fields*, In: G. McGuire, G. L. Mullen, D. Panario, I. E. Shparlinski (eds.), Finite Fields: Theory and Applications. Series: Contemporary Mathematics, **518**, Providence, RI: Amer. Math. Soc., (2010), 113–127.

[7] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge: Cambridge Univ. Press, 1997.

[8] G.L. Mullen, D. Panario, *Handbook of finite fields*, Boca Raton: CRC Press, 2013.

[9] M. Car, L. H. Gallardo, O. Rahavandrainy, L. N. Vaserstein, *About the period of Bell numbers modulo a prime* // Bull. Korean Math. Soc., **45** (2008), No. 1, 143–155.

[10] S. Wagstaff, jr., *Aurifeuillian factorizations and the period of the Bell numbers modulo a prime* // Math. Comp., **65** (1996), No. 213, 383–391.

[11] P. Montgomery, S. Nahm, S. Wagstaff, jr., *The period of the Bell numbers modulo a prime* // Math. Comp., **79** (2010), No. 281, 1793–1800.

[12] http://maths-people.anu.edu.au/ brent/factors.html

Відомості про авторів

Роман Б. Попович Національний університет
"Львівська політехніка"
Львів, 79013
Україна
E-Mail: rombp07@gmail.com