Математичний Вісник
Наукового товариства
імені Шевченка
2013. — Т.10

Mathematical Bulletin
of the Shevchenko
Scientific Society
2013. — V.10

ПОКРАЩЕННЯ НИЖНЬОЇ ОЦІНКИ ДЛЯ ПОРЯДКУ ЕЛЕМЕНТІВ ОДНОГО КЛАСУ СКІНЧЕННИХ ПОЛІВ

Роман Попович

Національний університет "Львівська політехніка", вул. Бандери, 12, Львів, Україна

Р. Попович. *Покращення нижньої оцінки для порядку елементів одного класу скінченних полів* // Мат. вісник НТШ. — 2013. — Т.10. — С. 39–44.

Ми явно будуємо в будь-якому скінченному полі виду $\mathbb{F}_q[x]/(x^m - a)$ елементи мультиплікативного порядку не меншого за максимум двох чисел, які прямо залежать від m.

R. Popovych, *Improved lower bound on order of elements of one class of finite fields*, Math. Bull. Shevchenko Sci. Soc. **10** (2013), 39–44.

We construct explicitly in any finite field of the form $\mathbb{F}_q[x]/(x^m - a)$ elements with multiplicative order at least maximum of two numbers that depend directly on m.

1. Вступ

Загальновідомо, що мультиплікативна група скінченного поля є циклічною. Твірну цієї групи називають примітивним елементом. Задача ефективної побудови примітивного елемента для заданого скінченного поля є важкою в обчислювальній теорії скінченних полів. Ось чому розглядають менш обмежуюче питання: знайти елемент великого мультиплікативного порядку. У цьому випадку не вимагається обчислити точний порядок елемента: достатньо отримати нижню межу для порядку. Елементи великого порядку потрібні для низки застосувань. Такі застосування, зокрема, включають криптографію, теорію кодування, генератори псевдовипадкових чисел та комбінаторику.

У даній роботі $\mathbb{F}_q$ позначає поле з q елементів, де q – степінь простого числа p.

Гао [1] дав алгоритм побудови елементів великого порядку для багатьох (згідно з висловленою ним, проте не доведеною, гіпотезою для всіх) загальних розширень $\mathbb{F}_{q^m}$ скінченого поля $\mathbb{F}_q$ з нижньою межею для порядку $\exp(\Omega((\log m)^2/\log\log m))$. Волох [2, 3] запропонував метод побудови елементів порядку принаймні $\exp(\Omega(\log m)^2))$.

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

Для часткових випадків скінченних полів можна збудувати елементи, що мають набагато більші порядки.

Розширення, пов'язані з поняттям ґаусового періоду, розглянуто в [4, 5, 6]. Нижня межа для порядку дорівнює $\exp(\Omega(\sqrt{m}))$. Ці розширення існують для нескінченної кількості чисел m, якщо для числа q виконується гіпотеза Артіна (див. [7]). Розширення на основі поліномів Куммера розглянуто в [8]. Узагальнення останніх наведено в [7]. Такі розширення існують для нескінченної кількості чисел m без виконання будь-яких припущень.

Розширення на основі полінома Куммера мають вигляд $\mathbb{F}_q[x]/(x^m - a)$. Їх, зокрема, застосовують в криптографії, що ґрунтується на спарюванні [9]. У [8] показано, як будувати елементи великого порядку в розширеннях $\mathbb{F}_q[x]/(x^m - a)$ при умові $q \equiv 1 \pmod{m}$. У цьому разі отримано нижню межу $\exp(\Omega(m))$. У [10] збудовано елементи великого порядку для таких розширень без умови $q \equiv 1 \pmod{m}$. Нижня межа для мультиплікативного порядку дорівнює $2^{\lfloor \sqrt[3]{2m} \rfloor}$.

У даній роботі ми покращуємо отриману в [10] межу. Розглядаємо будь-яке розширення вигляду $\mathbb{F}_q[x]/(x^m - a)$, і будуємо в ньому елементи мультиплікативного порядку не меншого за максимум двох чисел, які прямо залежать від m.

2. Допоміжні твердження

У даній роботі q, m та a — цілі числа, для яких розширення $\mathbb{F}_q[x]/(x^m - a)$ існує; m_2 — порядок q за модулем m. У [10] доведено (див. лему 2.1 далі), що $m = m_1 m_2$, де m_1 - дільник $q - 1$. Покладемо $\mathbb{F}_q(\theta) = \mathbb{F}_{q^m} = \mathbb{F}_q[x]/(x^m - a)$, де $\theta = x \pmod{(x^m - a)}$ — клас елемента x. Очевидно, що $\theta^m = a$.

Для цілого числа n через $\mathbb{Z}_n^*$ позначамо мультиплікативну групу оборотніх елементів кільця $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Через $\lfloor u \rfloor$ позначимо найбільше ціле число, що не перевищує u. Розбиття числа C – це послідовність таких невід'ємних цілих чисел $u_1, \ldots, u_C$, що $\sum_{j=1}^{C} j u_j = C$. Позначимо через

- $U(C)$ число усіх розбиттів C,
- $U(C, d)$ число розбиттів C, для яких $u_1, \ldots, u_C \le d$, тобто, кожна частина з'являється не більше, ніж d разів;
- $Q(C, d)$ число розбиттів C, для яких $u_j = 0$ для усіх $j \equiv 0 \pmod{d}$, тобто, жодна частина не ділиться на d.

У скінченних полях характеристики 2 є лише один нерозкладний поліном $x - 1$. Для полів непарної характеристики, ми можемо перевіряти $x^m - a$ на нерозкладність, використовуючи теорему 3.75 [11]:

Теорема 2.1. *Для елемента $a \in \mathbb{F}_q^*$ та цілого числа $m \ge 2$ двочлен $x^m - a$ нерозкладний над $\mathbb{F}_q[x]$ тоді і лише тоді, коли виконуються умови:*

1) *кожен простий дільник m ділить порядок e елемента $a \in \mathbb{F}_q^*$, але не ділить $(q-1)/e$;*

2) *якщо $m \equiv 0 \pmod{4}$, то $q \equiv 1 \pmod{4}$.*

Як розвиток теореми 2.1, маючи число q, Панаріо й Томсон [12] точно описали для яких степенів m існують нерозкладні двочлени, а також явно збудували елемент a. У випадку $q = 3$ існує єдине можливе розширення для $m = 2$. Якщо $q \geq 5$, то можемо збудувати розширення для нескінченної кількості m. Тому приймаємо до кінця даної статті, що q непарне. Зрозуміло, що $a \neq 1$. У [10] доведено таку лему.

Лема 2.2. *Нехай q та m задовольняють умови теореми 2.1. Нехай m_2 – порядок q за модулем m. Тоді $m = m_1 m_2$, де m_1 є дільником $q - 1$, а підгрупа $\langle q \rangle$ групи $\mathbb{Z}_m^*$ може бути записана у вигляді $\langle q \rangle = \{i \cdot m_1 + 1 : 0 \leq i < m_2\}$.*

У [10] також доведено таку теорему.

Теорема 2.3. *Нехай b – ненульовий елемент поля $\mathbb{F}_q$. Тоді $\theta + b$ має в полі $\mathbb{F}_q(\theta) = \mathbb{F}_q[x]/(x^m - a)$ мультиплікативний порядок не менший за число розв'язків $(e_1, \ldots, e_{m_2-1})$ лінійної діофантової нерівності*

$$\sum_{i=0}^{m_2-1} (i \cdot m_1 + 1) e_i < m, \tag{1}$$

де $0 \leq e_1, \ldots, e_{m_2-1} < p$.

Лема 2.4. *Нехай b – ненульовий елемент поля $\mathbb{F}_q$. Тоді $\theta^{m_2} + b$ має мультиплікативний порядок принаймі 2^{m_1}.*

Доведення. Згідно з лемою 2.1, $q \equiv 1 \pmod{m_1}$. Оскільки поліном $x^m - a = (x^{m_2})^{m_1} - a$ нерозкладний над $\mathbb{F}_q$, то поліном $y^{m_1} - a$ також нерозкладний над $\mathbb{F}_q$. Покладемо $\theta_1 = \theta^{m_2}$ та розглянемо підполе $\mathbb{F}_q(\theta_1) = \mathbb{F}_q[y]/(y^{m_1} - a)$ поля $\mathbb{F}_q(\theta)$. Візьмемо $\rho = \theta_1 + b$. Тоді

$$\rho^q = (\theta_1 + b)^q = \theta_1^q + b = (\theta_1^{m_1})^{(q-1)/m_1} \theta_1 + b = a^{(q-1)/m} \theta_1 + b.$$

Позначимо $c = a^{(q-1)/m_1}$. Маємо, що $(\theta_1 + b)^{q^i} = \theta_1^{i(q-1)/m_1} + b = c^i \theta_1 + b$.

Таким чином, спряжені (відносно автоморфізму Фробеніуса) елементи до $\rho = \theta_1 + b$ мають вигляд $c^i \theta_1 + b$, $1 \leq i < m_1$.

Розглянемо їх добутки $\prod_{i=0}^{m_1-1} (c^i \theta_1 + b)^{\beta_i}$, де $\beta_i \in \{0, 1\}$ та

$$\sum_{i=0}^{m_1-1} \beta_i \leq m_1 - 1.$$

Очевидно, що всі ці добутки попарно різні, а їх кількість дорівнює $2^{m_1} - 1$. Якщо $m_1 > 2$, ми також беремо добуток $(\theta_1 + b)^2$, і отримуємо 2^{m_1} різних добутків.

Розглянемо випадок $m_1 = 2$. Зрозуміло, що $c \neq 1$, та 1, $\theta_1 + b$, $c\theta_1 + b$ – це три різних елементи. Доведемо, що $(\theta_1 + b)^2$ або $(c\theta_1 + b)^2$ є четвертим відмінним від них елементом. Ясно, що $(\theta_1 + b)^2$ відмінний від 1, $\theta_1 + b$. Якщо $(\theta_1 + b)^2 = c\theta_1 + b$, то $\theta_1^2 + (2b - a)\theta_1 + b(b-1) = 0$. Оскільки $y^2 - a$ – характеристичний поліном для θ_1, то маємо $c = 2b$. Отже $(c\theta_1 + b)^2$ відмінний від 1, $c\theta_1 + b$. Якщо $(c\theta_1 + b)^2 = \theta_1 + b$, то $c^2\theta_1^2 + (2cb - 1)\theta_1 + b(b-1) = 0$ й $c^{-1} = 2b$. Таким чином, $c = \pm 1$.

Оскільки $c \neq 1$, беремо $c = -1$ і будуємо добуток $(\theta_1 + b)(-\theta_1 + b) = -(\theta_1^2 - b^2)$. Так як $\theta_1^2 = -1$, то добуток дорівнює $b^2 + 1$ і є четвертим відмінним елементом. $\square$

3. Явна побудова елементів великого порядку

Далі ми явно будуємо елементи в полі $\mathbb{F}_q[x]/(x^m - a)$, мультиплікативний порядок яких не менший максимуму чисел 2^{m_1} та $U\left(\lfloor m/(m_1+1)\rfloor, p-1\right)$. Ідея така ж, як і в [10]: якщо $q-1$ має великий дільник m_1, то використовуємо для побудови метод з [8]; якщо ж $q-1$ не має великого дільника m_1, то тоді m_2 є великим, і ми використовуємо для побудови метод, аналогічний до методу з [4, 6]. Наш основний результат – це теорема 3.1.

Ми беремо в обидвох випадках лінійний двочлен від певного степеня θ та всі його спряжені, що також належать до підгрупи, породженої цим двочленом, і будуємо їх різні добутки. У першому випадку, коли $q \equiv 1 \pmod{m_1}$, усі спряжені вказаного лінійного двочлена також є лінійними двочленами. Ідея запропонована Берізбейтіа [13] як вдосконалення алгоритму AKS [14] та розвинута в [8]. У другому випадку, спряжені є нелінійними двочленами. Ідея запропонована фон Гатеном та Шпарлінскім [5], і розвинута в [4, 6]. Подібно до [7], наш підхід будує елементи великого порядку для нескінченної кількості чисел m, не спираючись ні на яке припущення. Число m прямо не залежить від q, зокрема може бути меншим від q.

Лема 3.1. *Число розв'язків лінійної діофантової нерівності* (1), *де* $0 \le e_1, \ldots, e_{m_2-1} < p$, *є не меншим за* $U(\lfloor m/(m_1+1)\rfloor, p-1)$.

Доведення. Нерівність (1) рівносильна нерівності

$$m_1 \sum_{i=0}^{m_2-1} ie_i + \sum_{i=0}^{m_2-1} e_i < m, \tag{2}$$

Нехай $\sum_{i=0}^{m_2-1} ie_i$ – розбиття числа $m_2 - a$, де a слід вибрати так, щоб нерівність (2) виконувалася; $e_i = 0$ для $m_2 - a \le i \le m_2 - 1$.

Зауважимо, що $\sum_{i=0}^{m_2-1} e_i \le \sum_{i=0}^{m_2-1} ie_i$ для довільних $e_1, \ldots, e_{m_2-1}$. Тоді маємо

$$m_1 \sum_{i=0}^{m_2-1} ie_i + \sum_{i=0}^{m_2-1} e_i \le m_1(m_2 - a) + m_2 - a < m_1 m_2 = m.$$

Отримуємо $a > m_2/(m_1+1)$ та $m_2 - a < m/(m_1+1)$. Отже, можемо взяти $m_2 - a = \lfloor m/(m_1+1)\rfloor$. □

Застосовуючи теорему 2.2 та лему 3.1, отримуємо таку лему.

Лема 3.2. *Нехай b – ненульовий елемент в $\mathbb{F}_q$. Тоді $\theta + b$ має в $\mathbb{F}_q(\theta) = \mathbb{F}_q[x]/(x^m - a)$ мультиплікативний порядок не менший за*

$$\frac{\exp\left\{2,5\sqrt{(m/(m_1+1)-p)(1-1/p)-(p-1)^2}\right\}}{\{13[(m/(m_1+1)-p)/(p(p-1))-1)]\}^{p-1}}.$$

Доведення. Спочатку зауважимо, що згідно з теоремою 2.2 та лемою 3.1, елемент $\theta + b$ має в $\mathbb{F}_q(\theta) = \mathbb{F}_q[x]/(x^m - a)$ порядок не менший за $U\left(\lfloor m/(m_1+1)\rfloor, p-1\right)$. Далі знаходимо явну нижню оцінку для $U\left(\lfloor m/(m_1+1)\rfloor, p-1\right)$.

Згідно з [15, твердження 5.1], число розбиттів числа n, які не мають d однакових частин, дорівнює числу розбиттів n, для яких ні одна частина не ділиться на d:

$$U(n, d-1) = Q(n, d). \tag{3}$$

Виходячи з [15, див. доведення теореми 5.1] для $Q(n, d)$ справедлива така нерівність:

$$Q(n, d) \geq \{U(\lfloor \lfloor n/d \rfloor /(d-1) \rfloor)\}^{d-1}. \tag{4}$$

Теорема 4.2 [15] дає нижню межу

$$U(k) > \frac{\exp\left(\frac{5}{2}\sqrt{k}\right)}{13k} \tag{5}$$

для довільного цілого k.

Підставляючи (5) при $k = \lfloor \lfloor n/d \rfloor/(d-1) \rfloor$ в (4), отримуємо

$$Q(n, d) \geq \frac{\exp\left\{\frac{5}{2}(d-1)\sqrt{\lfloor \lfloor n/d \rfloor/(d-1) \rfloor}\right\}}{\left\{13\lfloor \lfloor n/d \rfloor/(d-1) \rfloor\right\}^{d-1}}.$$

Оскільки $\lfloor a \rfloor > a - 1$, маємо

$$Q(n, d) \geq \frac{\exp\left\{\frac{5}{2}\sqrt{(n-d)(1-1/d)-(d-1)^2}\right\}}{\{13((n-d)/(d(d-1))-1)\}^{d-1}}.$$

Приймаючи до уваги, що згідно з (3) $U(\lfloor m/(m_1+1) \rfloor, p-1) = Q(\lfloor m/(m_1+1) \rfloor, p)$ та $n = m/(m_1+1)-1$, $d = p$, отримуємо потрібну оцінку для $U(\lfloor m/(m_1+1) \rfloor, p-1)$. □

Наш основний результат – це така теорема.

Теорема 3.3. *У полі $\mathbb{F}_q(\theta) = \mathbb{F}_q[x]/(x^m - a)$ можна явно збудувати елемент, мультиплікативний порядок якого не менший за*

$$\max\left\{2^{m_1}, \frac{\exp\left\{\frac{5}{2}\sqrt{(m/(m_1+1)-p)(1-1/p)-(p-1)^2}\right\}}{\{13[(m/(m_1+1)-p)/(p(p-1))-1)]\}^{p-1}}\right\}.$$

Доведення. Маємо такі дві нижні оцінки мультиплікативного порядку. Згідно з лемою 3.2, елемент $\gamma = \theta + b$ має порядок принаймі

$$\frac{\exp\left\{\frac{5}{2}\sqrt{(m/(m_1+1)-p)(1-1/p)-(p-1)^2}\right\}}{\{13[(m/(m_1+1)-p)/(p(p-1))-1)]\}^{p-1}}.$$

Згідно з лемою 2.2, елемент $\gamma = \theta^{m_2} + b$ має порядок принаймі 2^{m_1}.

Отже, ми можемо явно збудувати (взявши елемент $\theta + b$ або елемент $\theta^{m_2} + b$) в полі $\mathbb{F}_q[x]/(x^m - a)$ елемент мультиплікативного порядку принаймі максимум двох вказаних чисел. Це завершує доведення теореми. □

Зауважимо, що оцінка з леми 3.2 є точною оцінкою знизу для порядку елементів виду $\theta + b$ у заданому скінченному полі. Разом з тим, вона громіздка і її не завжди зручно використовувати для порівняння різних скінченних полів. Як наближену оцінку можна взяти $\exp(\frac{5}{2}\sqrt{m/m_1})$. Тоді прирівнюємо (розраховуючи на найгірший випадок) $2^{m_1} = \exp(\frac{5}{2}\sqrt{m/m_1})$ і отримуємо $m_1 = \sqrt[3]{\frac{25}{4}(\log_2 e)^2 m}$. Як наслідок, можемо явно збудувати в полі $\mathbb{F}_q(\theta) = \mathbb{F}_q[x]/(x^m - a)$ елемент з такою наближеною нижньою оцінкою на порядок: $2^{\sqrt[3]{6{,}25(\log_2 e)^2 m}}$.

ЛІТЕРАТУРА

1. S. Gao, *Elements of provable high orders in finite fields*, Proc. Amer. Math. Soc. **127**:6 (1999), 1615–1623.
2. J.F. Voloch, *On the order of points on curves over finite fields*, Integers **7** (2007), A49.
3. J.F. Voloch, *Elements of high order on finite fields from elliptic curves*, Bull. Aust. Math. Soc. **81**:3 (2010), 425–429.
4. O. Ahmadi, I.E. Shparlinski, J.F. Voloch, *Multiplicative order of Gauss periods*, Int. J. Number Theory **6**:4 (2010), 877–882.
5. J. Gathen, I.E. Shparlinski, *Orders of Gauss periods in finite fields*, Appl. Algebra Engrg. Comm. Comput. **9**:1 (1998), 15–24.
6. 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.
7. Q. Cheng, S. Gao, D. Wan, *Constructing high order elements through subspace polynomials*, in: Proc. 23d ACM–SIAM Symp. on Discrete Algorithms (Kyoto, Japan, January 17–19, 2012) (ed.: Y. Rabanil), Omnipress (2011), 1457–1463.
8. Q. Cheng, *On the construction of finite field elements of large order*, Finite Fields Appl. **11**:3 (2005), 358–366.
9. N. Benger, M. Scott, *Constructing tower extensions of finite fields for implementation of pairing-based cryprography*, in: 3d Int. Workshop on Arithmetic of Finite Fields (Istanbul, Turkey, June 27-30, 2010) (ed.: M.A. Hasan, T. Helleseth), Springer, LNCS 6087 (2010), 180–195.
10. 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.
11. R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press (1997), 755p.
12. D. Panario, D. Thomson, *Efficient* p*th root computations in finite fields of characteristic* p, Des. Codes Cryptogr. **50**:3 (2009), 351–358.
13. P. Berrizbeitia, *Sharpening "Primes is in P" for a large family of numbers*, Math. Comp. **74** (2005), 2043–2059.
14. M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, Ann. of Math. **160**:2 (2004), 781–793.
15. A. Maróti, *On elementary lower bounds for the partition function*, Integers **3** (2003), A10.

Надійшло 14.05.2013

Після переробки 23.08.2013