ВІСНИК НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
"ЛЬВІВСЬКА ПОЛІТЕХНІКА"
"Фізико-математичні науки"
Вип.768 № 768, (2013) с. 59–62

JOURNAL OF NATIONAL UNIVERSITY
"LVIVSKA POLITECHNIKA"
"Physical & mathematical sciences"
Vol.768 No 768, (2013) 59–62

ПРО ОЦІНКИ ДЛЯ МУЛЬТИПЛІКАТИВНИХ ПОРЯДКІВ ЕЛЕМЕНТІВ СКІНЧЕННИХ ПОЛІВ НА ОСНОВІ ЦИКЛОТОМІЧНИХ ПОЛІНОМІВ

Попович Р.

Національний університет "Львівська політехніка"
вул. С. Бандери 12, 79013, Львів, Україна

(Отримано 5 грудня 2012 р.)

Отримано асимптотичні нижні оцінки для мультиплікативних порядків елементів скінченних полів, що мають більше загальний вигляд, ніж гауссові періоди спеціального типу.

Ключові слова: скінченне поле, мультиплікативний порядок, нижня оцінка.
2000 MSC: 11T30
УДК: 512.624

Загальновідомо, що задача ефективної побудови примітивного елемента заданого скінченного поля є важкою в обчислювальній теорії скінченних полів. Ось чому розглядають менш обмежуюче питання: знайти елемент великого мультиплікативного порядку. У цьому випадку достатньо отримати нижню границю для порядку. Елементи великого порядку потрібні для низки застосувань. Такі застосування, зокрема, об'єднують криптографію, теорію кодування, генератори псевдовипадкових чисел та комбінаторику. Елементи великого порядку також використовують в алгоритмі AKS доведення простоти чисел, запропонованому Агравалом, Кайалом та Саксеною [1, 6].

Гао [5] дав алгоритм побудови елементів великого порядку для багатьох (згідно з висловленою ним, проте не доведеною, гіпотезою для всіх) загальних розширень F_{q^m} скінченного поля F_q з нижньою границею для порядку $\exp(\Omega((\log m)^2/\log\log m))$. Волох [11] запропонував метод побудови елементів порядку принаймні $\exp(\Omega(\log m)^2))$.

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

Розширення на основі полінома Куммера мають вигляд $F_q[x]/(x^m-a)$. У [4] показано, як будувати елементи великого порядку в таких розширеннях за умови $q \equiv 1(mod\ m)$. У цьому разі отримано нижню границю $\exp(\Omega(m))$. Елементи великого порядку збудовано в [10] для довільних розширень на основі полінома Куммера . Нижня границя дорівнює $\exp(\Omega(m^{1/3}))$.

Розширення на основі циклотомічних поліномів розглянуті в [2, 9]. Нижня границя на порядок дорівнює $\exp(\Omega(m^{1/2}))$. Точніше будують такі розширення. Нехай $r = 2s+1$ просте число взаємно просте з q. Нехай q примітивний корінь за модулем r, тобто мультиплікативний порядок q за модулем r дорівнює $r-1$. Приймемо $F_{q^{r-1}} = F_q(\theta) = F_q[x]/\Phi_r(x)$, де $\Phi_r(x) = x^{r-1}+x^{r-2}+...+x+1$ є r-й циклотомічний поліном та $\theta = x\ (mod\Phi_r(x))$. Елемент $\beta = \theta+\theta^{-1}$ називають гауссовим періодом типу $((r-1)/2, 2)$. Він породжує нормальну базу над F_q [2].

Нехай q степінь простого числа p. Скінченне поле з q елементів позначаємо F_q, а його мультиплікативну групу поля позначаємо F_q^*. Розбиття числа C – це послідовність таких невід'ємних цілих $u_1, ..., u_C$, що $\sum_{j=1}^{C} ju_j = C$. $U(C)$ позначає число розбиттів C. $U(C,d)$ позначає число таких розбиттів C, для яких $u_1, ..., u_C \le d$, тобто, кожна частина з'являється не більше ніж d разів. $Q(C,d)$ позначає число таких розбиттів C, для яких $u_j = 0$, якщо $j \equiv 0\ mod\ d$, тобто, жодна частина не ділиться на d.

I. Попередні відомості та постановка задачі

У роботі [2] показано, що мультиплікативний порядок гауссового періоду β є принаймні $U((r-3)/2, p-1)$. У [9, теорема 1] покращено та узагальнено цей результат, а саме доведено таку теорему.

Теорема 1. *Нехай q степінь простого числа p, $r = 2s+1$ просте число взаємно просте з q, q примітивний корінь за модулем r, θ породжує розширення $F_q(\theta) = F_{q^{r-1}}$, e є ціле число, f ціле число взаємно просте з q, а ненульовий елемент скінченного поля F_q. Тоді*
(a) $\theta^e(\theta^f+a)$ має мультиплікативний порядок принаймні $U(r-2, p-1)$,
(b) $(\theta^{-f}+a)(\theta^f+a)$ для $a^2 \ne \pm 1$ має мультиплікативний порядок принаймні $U((r-3)/2, p-1)$ і цей порядок ділить $q^{(r-1)/2}-1$,
(c) $\theta^{-2e}(\theta^{-f}+a)(\theta^f+a)^{-1}$ для $a^2 \ne 1$ має мультиплікативний порядок принаймні $U((r-3)/2, p-1)$ і цей порядок ділить $q^{(r-1)/2}+1$,
(d) $\theta^e(\theta^f+a)$ для $a^2 \ne \pm 1$ має мультиплікативний порядок принаймні $[U((r-3)/2, p-1)]^2/2$.

Зокрема порядок гауссового періоду $\beta = \theta+\theta^{-1} = \theta^{-1}(\theta^2+1)$є принаймні $U(r-2, p-1)$.

Нехай a ненульовий елемент в F_q. Позначимо
$\gamma = (\theta^{-1}+a)(\theta+a)^{-1}$ та
$z = \begin{cases} \beta^2\gamma, \text{якщо } \rho_2(q^{(r-1)/2}-1)=2 \\ \beta\gamma^2, , \text{якщо } \rho_2(q^{(r-1)/2}+1)=2 \end{cases}$.
З теореми 1 отримано такий наслідок [9, наслідок 3].

Наслідок 2. *Елемент z для $a^2 \neq 1$ має мультиплікативний порядок принаймні*
$[U(r-2,p-1)U((r-3)/2,p-1)]/2$.

Наведені оцінки не дозволяють наочно порівнювати різні отримані результати. Водночас у [9] даються точні оцінки порядків знизу в термінах p та r. Проте такі оцінки не є повними, бо отримані лише для випадків $r \geq p^2$ та $r < p$. Важливий у прикладних застосуваннях (передусім у криптографії) випадок $p \leq r < p^2$ залишається неописаним.

Тому в роботі вивчаються асимптотичні оцінки для довільних p та r. Такі дослідження розпочаті в [2]. Так, згідно з [2, наслідок 2], рівномірно по q, при $r \to \infty$: мультиплікативний порядок L_r гауссового періоду $\beta = \theta + \theta^{-1}$ задовольняє умову

$$L_r \geq \exp\left((\frac{\pi}{\sqrt{2}}\sqrt{\frac{2(p-1)}{3p}} + o(1))\sqrt{r-1} \right).$$

Можна вивести з теореми 1 аналогічні асимптотичні нижні границі для мультиплікативних порядків розглянутих у цій теоремі елементів.

II. Асимптотичні нижні оцінки для порядків у термінах p та r

Явні нижні оцінки порядків елементів скінченного поля в термінах p та r є особливо цікавими в прикладних застосуваннях. Ось чому ми використовуємо в цьому розділі деякі відомі оцінки з [3, 7, 8] для виведення явних нижніх оцінок для мультиплікативних порядків $\theta^e(\theta^f + a)$ та z.

Згідно з [3, наслідок 1.3], число розбиттів для n, які не мають d однакових частин, дорівнює числу розбиттів для n з частинами, які не діляться на d:

$$U(n, d-1) = Q(n, d). \qquad (1)$$

Явна нижня границя для $Q(n,d)$ при $n \geq d^2$ дається у [8]. Якщо $n < d$, то зрозуміло $U(n, d-1) = U(n)$. Явна нижня границя для $U(n)$ для довільних цілих n наведена також у [8]. Якщо ж $d \leq n < d^2$, то явна нижня границя для $Q(n,d)$ невідома.

Лема 3. *Нехай s – натуральне число, l – просте число. Тоді при $s \to \infty$ виконується нерівність*

$$Q(s,l) \geq \exp\left((\pi\sqrt{\frac{2(l-1)}{3l}} + o(1))\sqrt{s} \right). \qquad (2)$$

Доведення. Для множини $V = \{v_1, ..., v_w\}$, $1 \leq v_i \leq \frac{l-1}{2}$, згідно з [7, лема 7.2] маємо при $s \to \infty$

$$p_V(s) = \frac{(6l)^{1/2} w^{1/4}}{2^r (12sl - A)^{3/4}} \times$$

$$\times \left(\prod_{i=1}^{w} \csc(\pi v_i / l) \right) \exp(Tw^{1/2})[1 + O(s^{-1/2})],$$

де $A = \sum_{i=1}^{w}(l^2 - 6v_i l + 6v_i^2)$, $T = \frac{\pi(12sl-A)^{1/2}}{3l}$.

Візьмемо як множину V таку множину $V = \{1, 2, ..., \frac{l-1}{2}\}$, тобто $v_i = i, i = 1, ..., \frac{l-1}{2}$. Тоді $w = \frac{l-1}{2}$ і згідно з [7, с.57] отримуємо $A = \frac{l-l^2}{2}$. Також маємо

$$2^{-r}\left(\prod_{i=1}^{w} \csc(\pi v_i/l) \right) = \left(\prod_{i=1}^{(l-1)/2} 2\sin(\pi v_i/l) \right)^{-1} = l^{-1/2}.$$

У випадку вибраної раніше множини V виконується рівність $p_V(s) = U(s-1, l-1)$.

Оскільки $T = \left(\frac{2\pi}{\sqrt{3l}} + o(1)\right)\sqrt{s}$ та $w^{1/2} = \sqrt{\frac{l-1}{2}}$, то $Tw^{1/2} = \left(\pi\sqrt{\frac{2(l-1)}{3l}} + o(1)\right)\sqrt{s}$.

Отже, нерівність (2) виконується. ■

Використовуючи лему 3, можемо отримати оцінки знизу для мультиплікативних порядків елементів $\theta^e(\theta^f + a)$ при довільному ненульовому a і при $a^2 \neq \pm 1$ та для елемента z при $a^2 \neq 1$.

Теорема 4. *Рівномірно по q, при $r \to \infty$: мультиплікативний порядок $L_{r,1}$ елемента $\theta^e(\theta^f + a)$ задовольняє умову*

$$L_{r,1} \geq \exp\left((\pi\sqrt{\frac{2(p-1)}{3p}} + o(1))\sqrt{r-2} \right).$$

Доведення. Використовуючи теорему 1, частину (a), маємо таку нерівність $L_{r,1} \geq U(r-2, p-1)$. Враховуючи нерівність (1), одержуємо, що $L_{r,1} \geq Q(r-2, p)$. Нижче застосовуємо лему 3 до $Q(r-2,p)$ і отримуємо оцінку в формулюванні теореми 4. ■

Теорема 5. *Рівномірно по q, при $r \to \infty$: мультиплікативний порядок $L_{r,2}$ елемента $\theta^e(\theta^f + a)$ при $a^2 \neq \pm 1$ задовольняє умову*

$$L_{r,2} \geq \frac{1}{2}\exp\left((\pi\sqrt{2}\sqrt{\frac{2(p-1)}{3p}} + o(1))\sqrt{r-3} \right).$$

Доведення. Використовуючи теорему 1, частину (d), маємо таку нерівність $L_{r,2} \geq \frac{1}{2}[U(\frac{r-3}{2}, p-1)]^2$. Враховуючи нерівність (1), дістаємо, що $L_{r,2} \geq \frac{1}{2}[Q(\frac{r-3}{2}, p)]^2$.
Згідно з лемою 3, застосованою до $Q(\frac{r-3}{2}, p)$, отримуємо

$$L_{r,2} \geq \frac{1}{2}\exp\left((\pi\sqrt{\frac{2(p-1)}{3p}} + o(1))2\sqrt{\frac{r-3}{2}} \right).$$

З останньої нерівності випливає оцінка порядку в формулюванні цієї теореми. ■

Теорема 6. *Рівномірно по q, при $r \to \infty$: мультиплікативний порядок $L_{r,3}$ елемента z при $a^2 \neq 1$ задовольняє умову*

$$L_{r,3} \geq \frac{1}{2}\exp\left((\pi(1+\sqrt{2}/2)\sqrt{\frac{2(p-1)}{3p}}+o(1))\sqrt{r-3}\right).$$

Доведення. Використовуючи наслідок 2, маємо таку нерівність: $L_{r,3} \geq \frac{1}{2}U(r-2,p-1)U(\frac{r-3}{2},p-1)$. Беручи до уваги нерівність (1), одержуємо $L_{r,3} \geq \frac{1}{2}Q(r-2,p)Q(\frac{r-3}{2},p)$. Застосовуючи лему 3 до $Q(r-2,p)$ та до $Q(\frac{r-3}{2},p)$, отримуємо $L_{r,2} \geq \frac{1}{2}\exp\left((\pi\sqrt{\frac{2(p-1)}{3p}}+o(1))\left\{\sqrt{r-2}+\sqrt{\frac{r-3}{2}}\right\}\right)$. З останньої нерівності випливає оцінка порядку в формулюванні цієї теореми. ■

Потім у таблиці наводимо чисельне порівняння оцінок порядків елементів скінченного поля, отриманих в теоремах 4, 5, 6. Наводимо залежну від характеристики p основу d, яку при оцінці порядку елемента підносимо до степеня, залежного від r. Тобто порядок вказаного в таблиці елемента принаймні $d^{\sqrt{r-3}}$, де значення d наведені в таблиці.

№	Елемент	Значення d	
		$p=2$	$p\to\infty$
1	гауссовий період [2]	3,6058	6,1337
2	елемент $\theta^e(\theta^f+a)$, який узагальнює гауссовий період [9]	6,1337	13,0019
3	елемент $\theta^e(\theta^f+a)$, який узагальнює гауссовий період, при $a^2\neq\pm1$ [9]	13,0019	37,6223
4	елемент z при $a^2\neq1$ [9]	22,1170	79,7499

Слід зауважити, зокрема, до п.2 наведеної таблиці, що в найгіршому випадку (коли $p=2$)

$$d=\exp\left((\pi\sqrt{\frac{2(p-1)}{3p}}\right)=\exp\left((\pi\sqrt{\frac{2}{6}}\right)=6,1337...$$

Якщо ж $p\to\infty$, то маємо $d=\exp\left((\pi\sqrt{\frac{2}{3}}\right)=13,0019....$

Література

[1] Agrawal M., Kayal N., Saxena N. *PRIMES is in P*, Annals of Mathematics, 160 (2), 2004, pp.781–793.

[2] Ahmadi O., Shparlinski I. E., Voloch J. F. *Multiplicative order of Gauss periods*, Intern // J. Number Theory, 6(4), 2010. – pp.877–882.

[3] Andrews G.E. *The theory of partitions*, Addison- Wesley, 1976.

[4] Cheng Q. *On the construction of finite field elements of large order*, Finite fields and Their Appl., 11(3), 2005. – pp. 358–366.

[5] Gao S. *Elements of provable high orders in finite fields*, Proc. Amer. Math. Soc., 107(6), 1999. – pp. 1615–1623.

[6] Granville A. *It is easy to determine whether a given integer is prime*, Bull. of the Amer. Math. Soc., 42 (1), 2005. – pp. 3–38.

[7] Hagis P. A problem on partitions with a prime modulus $p \geq 3$, Trans. Amer. Math. Soc., 102 (1962). – pp. 30–62.

[8] Maroti A. *On elementary lower bounds for the partition function*, Integers: Electronic J.Comb.Number Theory, 3:A10 , 2003.

[9] Popovych R. Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$, Finite Fields Appl. 18(4) (2012). – pp. 700–710.

[10] Popovych R. Elements of high order in finite fields of the form $F_q[x]/(x^m-a)$, Finite Fields Appl. 19 (1) (2013). – pp. 86–92.

[11] Voloch J.F. On the order of points on curves over finite fields, Integers 7 (2007), A49.

ОБ ОЦЕНКАХ МУЛЬТИПЛИКАТИВНЫХ ПОРЯДКОВ ЭЛЕМЕНТОВ КОНЕЧНЫХ ПОЛЕЙ НА ОСНОВЕ ЦИКЛОТОМИЧЕСКИХ ПОЛИНОМОВ

Поповыч Р.

Национальный университет "Львивська политэхника",
ул. С. Бандеры, 12, Львов, 79013, Украина

Получено асимптотические нижние оценки для мультипликативных порядков элементов конечных полей, имеющих более общий вид, чем гауссовы периоды специального типа.

Ключевые слова: конечное поле, мультипликативный порядок, нижняя оценка.

2000 MSC: 11T30

УДК: 512.624

ON BOUNDS FOR MULTIPLICATIVE ORDERS OF ELEMENTE OF FINITE FIELDS BASED ON CYCLOTOMIC POLYNOMIALS

Popovych R.

National University "Lvivska Politechnika"
12 S. Bandera Str., 79013, Lviv, Ukraine

We have obtained asymptotic lower bounds for multiplicative orders of finite field elements that have more general form than Gauss periods of a special type.

Key words: finite field, multiplicative order, lower bound.

2000 MSC: 11T30

УДК: 512.624