

УДК 517.624

Р. Б. Попович (Національний університет "Львівська політехніка")

**ПРО ЕЛЕМЕНТИ ВЕЛИКОГО ПОРЯДКУ В РОЗШИРЕННЯХ СКІНЧЕННИХ ПОЛІВ НА ОСНОВІ ПОЛІНОМІВ КУММЕРА**

We construct explicitly in any finite field of the form  $F_q[x]/(x^m - a)$  elements with multiplicative order at least  $2^{\lfloor \sqrt[3]{\frac{(\log_2 5)^2}{2} m} \rfloor}$ .

Ми явно будуємо в будь-якому скінченному полі вигляду  $F_q[x]/(x^m - a)$  елементи мультиплікативного порядку принаймні  $2^{\lfloor \sqrt[3]{\frac{(\log_2 5)^2}{2} m} \rfloor}$ .

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 скінчених полів. Ось чому розглядають менш обмежуюче питання: знайти елемент великого мультиплікативного порядку. У цьому випадку не вимагається обчислити точний порядок елемента: достатньо отримати нижню границю для порядку. Елементи великого порядку потрібні для низки застосувань. Такі застосування, зокрема, включають криптографію, теорію кодування, генератори псевдовипадкових чисел та комбінаторику.

У даній роботі  $F_q$  позначатиме скінченне поле з  $q$  елементів, де  $q$  - степінь простого числа  $p$ .

**Огляд відомих результатів.** Гао [8] 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 [16, 17] запропонував метод побудови елементів порядку принаймні  $\exp(\Omega(\log m)^2)$ .

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

Розширення, пов'язані з поняттям гауссового періоду, розглянуті в [2, 9, 10, 13]. Нижня границя на порядок дорівнює  $\exp(\Omega(\sqrt{m}))$ . Ці розширення існують для нескінченної кількості чисел  $m$ , якщо для числа  $q$  справедлива гіпотеза Артіна (див. [7]). Розширення на основі поліномів Куммера розглянуто в [5, 6]. Узагальнення останніх наведено в [7]. Розширення існують для нескінченної кількості чисел  $m$  без виконання будь-яких умов.

Розширення на основі поліномів Куммера мають вигляд  $F_q[x]/(x^m - a)$ . Їх зокрема застосовують в криптографії, що ґрунтується на спарюванні [3]. У [5, 6] показано, як будувати елементи великого порядку в розширеннях  $F_q[x]/(x^m - a)$  при умові  $q \equiv 1 \pmod{m}$ . У цьому разі отримано нижню границю  $\exp(\Omega(m))$ . У [14] збудовано елементи великого порядку для таких розширень без умови  $q \equiv 1 \pmod{m}$ . Нижня границя на мультиплікативний порядок дорівнює  $2^{\lfloor \sqrt[3]{2m} \rfloor}$ .

**Отримані результати.** У даній роботі  $q$ ,  $m$  та  $a$  - такі цілі числа, що розширення  $F_q[x]/(x^m - a)$  існує;  $m_2$  - порядок  $q$  за модулем  $m$ . У [14] доведено (див. лему 4 далі), що  $m = m_1 m_2$ , де  $m_1$  - дільник  $q - 1$  ( $m_1 \geq 2$ ).

Покладемо  $F_q(\theta) = F_{q^m} = F_q[x]/(x^m - a)$ , де  $\theta = x \pmod{(x^m - a)}$  - клас елемента  $x$ . Очевидно, що  $\theta^m = a$ .

У даній роботі ми покращуємо отриману в [14] оцінку. Розглядаємо будь-яке розширення виду  $F_q[x]/(x^m - a)$ , і будемо в ньому елементи мультиплікативного порядку принаймні  $2^{\lfloor \sqrt[3]{(\log_2 5)^2 m} \rfloor}$ . Ідея така ж, як і в [14]: якщо  $q - 1$  має великий дільник  $m_1$ , то використовуємо для побудови метод з [5]; 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 [2, 13]. Наш основний результат - це така теорема.

**Теорема 1.** *Нехай  $b$  - ненульовий елемент із  $F_q$ .*

1. *Якщо  $2 \leq m_1 < 869$ , то елемент*

$$\gamma = \begin{cases} \theta + b, & \text{if } m_1 \leq \lfloor \log_2 5 \sqrt{\frac{m_2}{2}} \rfloor \\ \theta^{m_2} + b, & \text{if } m_1 > \lfloor \log_2 5 \sqrt{\frac{m_2}{2}} \rfloor \end{cases}$$

*має в полі  $F_q(\theta) = F_q[x]/(x^m - a)$  мультиплікативний порядок принаймні  $2^{\lfloor \sqrt[3]{(\log_2 5)^2 m} \rfloor}$ .*

2. *Якщо  $m_1 \geq 869$ , то елемент*

$$\gamma = \begin{cases} \theta + b, & \text{if } m_1 \leq \lfloor \log_2 5 \sqrt{\frac{m_2}{8}} \rfloor \\ \theta^{m_2} + b, & \text{if } m_1 > \lfloor \log_2 5 \sqrt{\frac{m_2}{8}} \rfloor \end{cases}$$

*має в полі  $F_q(\theta) = F_q[x]/(x^m - a)$  мультиплікативний порядок принаймні  $2^{\lfloor \sqrt[3]{(\log_2 5)^2 m} \rfloor}$ .*

Ми беремо в обидвох випадках лінійний двочлен від певного степеня  $\theta$  та всі його спряжені, що також належать до підгрупи, породженої цим двочленом, і будемо 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 [4] як вдосконалення алгоритму AKS [1] та розвинута в [5, 6]. У другому випадку, спряжені є нелінійними двочленами. Ідея запропонована Гатеном та Шпарлінскім [9] і розвинута в [2, 10, 13]. 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  $q$ .

**1. Попередні результати.** Для простого числа  $k$ ,  $\nu_k(l)$  позначає найбільший степінь  $k$ , що ділить число  $l$ . Для натурального числа  $n$ ,  $Z_n^*$  - це мультиплікативна група цілих чисел за модулем  $n$ .

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

**Теорема 2.** *Нехай  $m \geq 2$  - ціле число та  $a \in F_q^*$ . Тоді двочлен  $x^m - a$  нерозкладний над  $F_q[x]$  тоді і тільки тоді, коли виконуються такі умови:*

- 1) *Кожен простий дільник  $m$  ділить порядок  $e$  елемента  $a \in F_q^*$ , але не ділить  $(q - 1)/e$ ;*
- 2) *Якщо  $m \equiv 0 \pmod{4}$ , то  $q \equiv 1 \pmod{4}$ .*

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

У [14, лема 4] доведено таку лему.

**Лема 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  $Z_m^*$  може бути записана у вигляді  $\langle q \rangle = \{i \cdot m_1 + 1 \mid i = 0, \dots, m_2 - 1\}$ .*

У [14, теорема 6] також доведено таку теорему.

**Теорема 3.** *Нехай  $b$  ненульовий елемент з  $F_q$ . Тоді  $\theta + b$  має в  $F_q(\theta) = F_q[x]/(x^m - a)$  мультиплікативний порядок принаймні такий, як число розв'язків  $(e_1, \dots, e_{m_2-1})$  лінійної діофантової нерівності*

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

для яких  $0 \leq e_1, \dots, e_{m_2-1} \leq p - 1$ .

Таку нерівність для біноміальних коефіцієнтів було отримано в [15, наслідок 2.9, нерівність (2.13)] при  $s > 1$  та  $t \geq 2$ :

$$\binom{st}{t} > 1,08444 \cdot e^{-\frac{1}{8t}} t^{-\frac{1}{2}} \frac{s^{s(t-1)+1}}{(s-1)^{(s-1)(t-1)}}. \tag{2}$$

**Лема 2.** *Нехай  $b$  - ненульовий елемент в  $F_q$ . Тоді  $\theta^{m_2} + b$  має мультиплікативний порядок принаймні*

$$\begin{cases} 2^{m_1}, \text{ if } 2 \leq m_1 < 869 \\ 4^{m_1}, \text{ if } m_1 \geq 869 \end{cases}.$$

**Доведення.** Розглянемо спочатку випадок  $2 \leq m_1 < 869$ . Згідно з лемою 1  $q \equiv 1 \pmod{m_1}$ . Оскільки поліном  $x^m - a = (x^{m_2})^{m_1} - a$  нерозкладний над  $F_q$ , то поліном  $y^{m_1} - a$  також нерозкладний над  $F_q$ . Покладемо  $\theta_1 = \theta^{m_2}$  та розглянемо підполе  $F_q(\theta_1) = F_q[y]/(y^{m_1} - a)$  поля  $F_q(\theta)$ . Візьмемо  $\theta_1 + b$  та його спряжені  $a^i \theta_1 + b, i = 1, \dots, m_1 - 1$ . Збудуємо їх добутки  $\prod_{i=0}^{m_1-1} (a^i \theta_1 + b)^{\beta_i}$ , 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  $1, \theta_1 + b, a\theta_1 + b$  - це три різних елементи. Доведемо, що  $(\theta_1 + b)^2$  або  $(a\theta_1 + b)^2$  є четвертим відмінним від них елементом. Ясно, що  $(\theta_1 + b)^2$  відмінний від  $1, \theta_1 + b$ . Якщо  $(\theta_1 + b)^2 = a\theta_1 + b$ , то  $\theta_1^2 + (2b - a)\theta_1 + b(b - 1) = 0$ . Оскільки  $y^2 - a$  - характеристичний поліном для  $\theta_1$ , то маємо  $a = 2b$ . Елемент  $(a\theta_1 + b)^2$  відмінний від  $1, a\theta_1 + b$ . Якщо  $(a\theta_1 + b)^2 = \theta_1 + b$ , то  $a^2\theta_1^2 + (2ab - 1)\theta_1 + b(b - 1) = 0$ , й  $a^{-1} = 2b$ . Таким чином,  $a = \pm 1$ .

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

Припустимо тепер, що  $m_1 \geq 869$ . Згідно з [5, лема 2.1]  $\theta_1 + b$  має мультиплікативний порядок  $L$  принаймні

$$L \geq \max_{0 \leq d_- \leq d \leq m_1} \binom{m_1}{d_-} \binom{d-1}{d_- - 1} \binom{2m_1 - d - d_- - 2}{m_1 - d_- - 1}.$$

Покладемо  $d_- = d = 1$ . Тоді  $L \geq m_1 \binom{2(m_1 - 2)}{m_1 - 2}$ . Використовуючи нерівність (2) (беремо  $s = 2$  та  $t = m_1 - 2 \geq 867$ ), отримуємо

$$\binom{2(m_1 - 2)}{m_1 - 2} \geq 1,08444 \cdot e^{-\frac{1}{8(m_1 - 2)}} \cdot \frac{4^{m_1 - 2}}{2\sqrt{m_1 - 2}}.$$

Тоді  $L \geq 1,08444 \cdot e^{-\frac{1}{8(m_1 - 2)}} \cdot \frac{m_1}{32\sqrt{m_1 - 2}} 4^{m_1}$ . Оскільки  $1,08444 \cdot e^{-\frac{1}{8(m_1 - 2)}} \cdot m_1 \geq 32\sqrt{m_1 - 2}$  для  $m_1 \geq 869$ , то маємо  $L \geq 4^{m_1}$ .

**2. Елементи великого порядку.** Ми явно будуємо далі елементи в  $F_q[x]/(x^m -$

a) порядку принаймні  $2^{\lfloor \sqrt{\frac{3(\log_2 5)^2}{2} m} \rfloor}$ .

**Лема 3.** Число розв'язків лінійної діофантової нерівності (1), для яких  $0 \leq e_1, \dots, e_{m_2 - 1} \leq p - 1$ , принаймні  $5^{\lfloor \sqrt{\frac{m_2}{2}} \rfloor}$ .

**Доведення.** Нехай  $\tau$  ( $2 \leq \tau \leq p$ ) ціле число, яке виберемо пізніше. Візьмемо таке найбільше ціле число  $\alpha$ , що  $\sum_{i=0}^{\alpha} (i \cdot m_1 + 1)(\tau - 1) < m$ . Нагадаємо, що  $m_1 \geq 2$ . Оскільки

$$\sum_{i=0}^{\alpha} (i \cdot m_1 + 1)(\tau - 1) = (\tau - 1)(\alpha m_1 + 2)(\alpha + 1)/2 < (\tau - 1)m_1(\alpha + 1)^2/2,$$

ми вибираємо  $\alpha$  з нерівності  $(\tau - 1)m_1(\alpha + 1)^2 \leq 2m$ , тобто  $\alpha = \lfloor \sqrt{\frac{2m_2}{\tau - 1}} \rfloor - 1$ . Зрозуміло, що коли взяти  $u_i \in \{0, \dots, p - 1\}$  для  $i = 0, \dots, \alpha$  та  $u_i = 0$  для  $i = \alpha + 1, \dots, m_2 - 1$ , то отримуємо розв'язок (1). Число таких розв'язків дорівнює  $\tau^{\alpha + 1} = \tau^{\lfloor \sqrt{\frac{2m_2}{\tau - 1}} \rfloor}$ .

Для вибору  $\tau$  дослідимо функцію  $f(\tau) = \tau^{\sqrt{\frac{2m_2}{\tau - 1}}}$  ( $2 \leq \tau \leq p$ ) на максимум. Запишемо з цією метою  $f(\tau) = \exp\left(\ln \tau \cdot \sqrt{\frac{2m_2}{\tau - 1}}\right)$ . Тоді маємо

$$\begin{aligned} f'(\tau) &= \tau^{\sqrt{\frac{2m_2}{\tau - 1}}} \cdot \left( \frac{1}{\tau} \left( \frac{2m_2}{\tau - 1} \right)^{1/2} - \ln \tau \cdot \frac{1}{2} \cdot \left( \frac{2m_2}{\tau - 1} \right)^{-1/2} \cdot 2m_2 \frac{-1}{(\tau - 1)^2} \right) = \\ &= \tau^{\sqrt{\frac{2m_2}{\tau - 1}}} \cdot \frac{2m_2}{\tau - 1} \cdot \left( \frac{1}{\tau} - \frac{\ln \tau}{2(\tau - 1)} \right). \end{aligned}$$

Якщо покладаємо  $f'(\tau) = 0$ , то  $\left(\frac{1}{\tau} - \frac{\ln \tau}{2(\tau - 1)}\right) = 0$ . Точка  $4,92155 < \tau_0 < 4,921555$  є точкою максимуму функції. Найближчим цілим числом до максимуму є  $\tau = 5$ .

Таким чином, число розв'язків нерівності (1) принаймні  $5^{\lfloor \sqrt{\frac{m_2}{2}} \rfloor}$ .

Застосовуючи теорему 3 та лему 3, отримуємо таку лему.

**Лема 4.** Нехай  $b$  - довільний ненульовий елемент з  $F_q$ . Тоді  $\theta + b$  має в  $F_q(\theta) = F_q[x]/(x^m - a)$  мультиплікативний порядок принаймні  $5 \lfloor \sqrt{\frac{m_2}{2}} \rfloor$ .

Тепер ми даємо доведення нашого основного результату - теореми 1.

**Доведення.** Спочатку даємо доведення для випадку  $2 \leq m_1 < 869$ . Якщо  $2^{m_1} \leq 5 \lfloor \sqrt{\frac{m_2}{2}} \rfloor$ , то будемо згідно з лемою 4 елемент  $\gamma = \theta + b$  з нижньою границею  $5 \lfloor \sqrt{\frac{m_2}{2}} \rfloor$  на його порядок. Якщо  $2^{m_1} > 5 \lfloor \sqrt{\frac{m_2}{2}} \rfloor$ , то будемо згідно з лемою 2 елемент  $\gamma = \theta^{m_2} + b$  з нижньою границею  $2^{m_1}$  на його порядок. Отже, можна явно збудувати в полі  $F_q[x]/(x^m - a)$  елемент з мультиплікативним порядком принаймні максимум таких двох нижніх границь:  $2^{m_1}$  та  $5 \lfloor \sqrt{\frac{m_2}{2}} \rfloor$ . У найгіршому випадку ці нижні границі співпадають:  $2^{m_1} = 5 \lfloor \sqrt{\frac{m_2}{2}} \rfloor$ . Тоді  $m_1 = \left\lfloor \sqrt[3]{\frac{(\log_2 5)^2 m}{2}} \right\rfloor$  і порядок є принаймні  $2 \left\lfloor \sqrt[3]{\frac{(\log_2 5)^2 m}{2}} \right\rfloor$ .

Тепер даємо доведення для випадку  $m_1 \geq 869$ . Якщо  $4^{m_1} \leq 5 \lfloor \sqrt{\frac{m_2}{2}} \rfloor$ , то будемо згідно з лемою 4 елемент  $\gamma = \theta + b$  з нижньою границею  $5 \lfloor \sqrt{\frac{m_2}{2}} \rfloor$  на його порядок. Якщо ж  $4^{m_1} > 5 \lfloor \sqrt{\frac{m_2}{2}} \rfloor$ , то будемо згідно з лемою 2 елемент  $\gamma = \theta^{m_2} + b$  з нижньою границею  $4^{m_1}$  на його порядок. Таким чином, можна явно збудувати в полі  $F_q[x]/(x^m - a)$  елемент з мультиплікативним порядком принаймні максимум таких нижніх границь:  $4^{m_1}$  та  $5 \lfloor \sqrt{\frac{m_2}{2}} \rfloor$ . У найгіршому випадку ці нижні границі співпадають:  $2^{2m_1} = 5 \lfloor \sqrt{\frac{m_2}{2}} \rfloor$ . У цьому разі  $m_1 = \left\lfloor \sqrt[3]{\frac{(\log_2 5)^2 m}{8}} \right\rfloor$  і порядок є принаймні  $2 \left\lfloor \sqrt[3]{(\log_2 5)^2 m} \right\rfloor$ .

Далі розглядаємо певні часткові розширення на основі поліномів Куммера.

**Приклад 1.** Нехай  $q$  такий степінь простого числа, що  $q \equiv 1 \pmod{4}$ . Тоді згідно з теоремою 2 існує таке розширення  $F_{q^{2^t}} = F_q[x]/(x^{2^t} - a)$ . Згідно з теоремою 1  $\gamma$  має мультиплікативний порядок принаймні  $2 \left\lfloor \sqrt[3]{(\log_2 5)^2 \cdot 2^{t-1}} \right\rfloor$ . Ця границя покращує попередню границю, отриману в [14]. Якщо  $\nu_2(q-1)$  мале, наприклад при  $q = 5$ , то границя з [5] є малою.

**Приклад 2.** Нехай  $q$  такий степінь простого числа, що  $q \equiv 1 \pmod{3}$ . Тоді згідно з теоремою 2 існує таке розширення  $F_{q^{3^t}} = F_q[x]/(x^{3^t} - a)$ . Згідно з теоремою 1  $\gamma$  має порядок принаймні  $2 \left\lfloor \sqrt[3]{\frac{(\log_2 5)^2 \cdot 3^t}{2}} \right\rfloor$ . Ця границя покращує попередню границю, отриману в [14]. Якщо  $\nu_3(q-1)$  мале, наприклад при  $q = 7$ , то границя з [5] є малою.

не є ні квадратом ні кубом у  $F_p$ . Тоді існує таке розширення  $F_{p^2}[x]/(x^m - (a \pm b\sqrt{-1}), m = k/2, k = 2^i 3^j$ . Такі розширення використовують у криптографії, що ґрунтується на спарюванні [3]. Згідно з теоремою 1 елемент  $\gamma$  має порядок принаймні  $2 \left\lfloor \sqrt[3]{(\log_2 5)^2 \cdot 2^i \cdot 3^j} \right\rfloor$ .

1. Agrawal M., Kayal N., Saxena N. PRIMES is in P // Ann. of Math. – 2004. – **160**, №2. – P. 781–793.
2. Ahmadi O., Shparlinski I. E., Voloch J. F. Multiplicative order of Gauss periods // Int. J. Number Theory. – 2010. – **6**, №4. – P. 877–882.

3. *Benger N., Scott M.* Constructing tower extensions of finite fields for implementation of pairing-based cryptography // Proc. 3d Int. Workshop on Arithmetic of Finite Fields. – 2010. – **LNCS 6087**, Springer. – P. 180–195.
4. *Berrizbeitia P.* Sharpening Primes is in P for a large family of numbers // Math. Comp. – 2005. – **74**, №252. – P. 2043–2059.
5. *Cheng Q.* Constructing finite field extensions with large order elements // Proc. 15-th ACM-SIAM Symp. on Discrete algorithms. – 2004. – P. 1123–1124.
6. *Cheng Q.* On the construction of finite field elements of large order // Finite Fields Appl. – 2005. – **11**, №3. – P. 358–366.
7. *Cheng Q., Gao S., Wan D.* Constructing high order elements through subspace polynomials // Proc. 23-rd ACM-SIAM Symp. on Discrete algorithms. – 2012. – P. 1457–1463.
8. *Gao S.* Elements of provable high orders in finite fields // Proc. Amer. Math. Soc. – 1999. – **127**, №6. – P. 1615–1623.
9. *von zur Gathen J., Shparlinski I.E.* Orders of Gauss periods in finite fields // Proc. 6th Intern. Symp. on Algorithms and Computation. – 1995. – **LNCS 1004**, Springer – P. 208–215.
10. *von zur Gathen J., Shparlinski I.E.* Gauss periods in finite fields // Proc. 5th Conf. of Finite Fields and their Applications. – 1999. – P. 162–177.
11. *Lidl R., Niederreiter H.* Finite Fields – Cambridge University Press – 1997. – 755 p.
12. *Panario D., Thomson D.* Efficient  $p$ th root computations in finite fields of characteristic  $p$  // Des. Codes Cryptogr. – 2009. – **50**, №3. – P. 351–358.
13. *Popovych R.* Elements of high order in finite fields of the form  $F_q[x]/\Phi_r(x)$  // Finite Fields Appl. – 2012. – **18**, №4. – P. 700–710.
14. *Popovych R.* Elements of high order in finite fields of the form  $F_q[x]/(x^m - a)$  // Finite Fields Appl. – 2013. – **19**, №1. – P. 86–92.
15. *Stanica P.* Good lower and upper bounds on binomial coefficients // J. Inequal. Pure Appl. Math. – 2001. – **2**, №3. – Art. 30
16. *Voloch J.F.* On the order of points on curves over finite fields // Integers. – 2007. – **7**, A49.
17. *Voloch J.F.* Elements of high order on finite fields from elliptic curves // Bull. Austral. Math. Soc. – 2010. – **81**. – P. 425–429.

Одержано 28.04.2013