Math-Net.Ru

Общероссийский математический портал

Ю. Н. Баулина, О числе решений уравнения $(x_1 + \dots + x_n)^m = ax_1 \dots x_n$ в конечном поле, *Дискрет. матем.*, 2004, том 16, выпуск 4, 41–48

DOI: <https://doi.org/10.4213/dm174>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.90.164.192

26 апреля 2023 г., 12:55:07

О числе решений уравнения

$$(x_1 + \dots + x_n)^m = ax_1 \dots x_n$$

в конечном поле

© 2004 г. Ю. Н. Баулина

Рассматривается уравнение

$$(x_1 + \dots + x_n)^m = ax_1 \dots x_n,$$

где a — ненулевой элемент конечного поля $\mathbf{F}_q$, $n \geq 2$, и m — натуральное число. Получена точная формула для числа решений этого уравнения в $\mathbf{F}_q^n$ при условии, что $d \in \{1, 2, 3, 6\}$, где d — наибольший общий делитель чисел $m - n$ и $q - 1$. Формулы для числа решений при произвольном $d > 2$ получены, если существует натуральное l такое, что $d \mid (p^l + 1)$, где p — характеристика $\mathbf{F}_q$.

Пусть $\mathbf{F}_q$ — конечное поле из q элементов, $\mathbf{F}_q^* = \mathbf{F}_q \setminus \{0\}$, $q = p^s$, p — простое число, η — квадратичный характер поля $\mathbf{F}_q$ (в случае нечетного q), ε — тривиальный мультипликативный характер поля $\mathbf{F}_q$. Рассмотрим уравнение

$$(x_1 + \dots + x_n)^m = ax_1 \dots x_n, \quad (1)$$

где $a \in \mathbf{F}_q^*$, $n \geq 2$, m — целое положительное число. Обозначим через N_q число решений уравнения (1) в $\mathbf{F}_q^n$. Л. Карлиц [1] доказал, что

$$N_q = \begin{cases} q^2 + 1, & \text{если } m = 2, n = 3 \text{ и } q \text{ нечетно,} \\ q^3 - 1 - \eta(a)q, & \text{если } m = 2, n = 4 \text{ и } q \text{ нечетно,} \end{cases}$$

и поставил задачу нахождения точной формулы для N_q при $m = 2$ и произвольном $n \geq 5$. Частично указанная проблема решена автором, в работе [2] найдены точные формулы для числа решений уравнения (1) в $\mathbf{F}_q^n$ при некоторых значениях наибольшего общего делителя $\gcd(n - 2, q - 1)$. В данной работе доказываются формулы для N_q при произвольном целом положительном m и $d \in \{1, 2, 3, 6\}$, где $d = \gcd(m - n, q - 1)$, а также при произвольном $d > 2$ при условии, что существует целое положительное число l такое, что $d \mid (p^l + 1)$.

Пусть $\psi, \psi_1, \dots, \psi_r$ — мультипликативные характеры поля $\mathbf{F}_q$, $r \geq 2$,

$$\mathrm{Tr}(x) = \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(x) = x + x^p + x^{p^2} + \dots + x^{p^{s-1}}$$

— абсолютный след элемента $x \in \mathbf{F}_q$. Определим суммы Гаусса и Якоби равенствами

$$G(\psi) = \sum_{x \in \mathbf{F}_q^*} \psi(x) e^{2\pi i \operatorname{Tr}(x)/p},$$

$$J(\psi) = \sum_{x \in \mathbf{F}_q} \psi(x) \psi(1-x)$$

соответственно (как обычно, полагаем $\psi(0) = 0$ для нетривиального характера ψ и $\varepsilon(0) = 1$). Определим также сумму

$$J_0(\psi_1, \dots, \psi_r) = \sum_{x_1 + \dots + x_r = 0} \psi_1(x_1) \dots \psi_r(x_r),$$

где суммирование ведется по всем r -наборам $(x_1, \dots, x_r)$ элементов поля $\mathbf{F}_q$ таким, что $x_1 + \dots + x_r = 0$. Все необходимые свойства характеров и сумм $G(\psi)$, $J(\psi)$ и $J_0(\psi_1, \dots, \psi_r)$ изложены в книге [3].

Покажем, что число решений уравнения (1) в $\mathbf{F}_q^n$ можно выразить через суммы Гаусса.

Теорема 1. Пусть $\gcd(m-n, q-1) = d$. Тогда

$$N_q = q^{n-1} + (-1)^{n-1} + \frac{1}{q} \sum_{\psi^d = \varepsilon, \psi \neq \varepsilon} \psi((-1)^n a) G(\psi)^n G(\bar{\psi}^n),$$

где сумма берется по всем нетривиальным мультипликативным характерам ψ поля $\mathbf{F}_q$, порядок которых делит d . В частности, при $\gcd(m-n, q-1) = 1$

$$N_q = q^{n-1} + (-1)^{n-1}.$$

Доказательство. Пусть N_q^* — число решений уравнения (1) в $(\mathbf{F}_q^*)^n$, $N_q(0)$ и $N_q^*(0)$ — число решений уравнения

$$x_1 + \dots + x_n = 0$$

в $\mathbf{F}_q^n$ и $(\mathbf{F}_q^*)^n$ соответственно. Заметим, что множества решений этого уравнения и уравнения (1) в $\mathbf{F}_q^n \setminus (\mathbf{F}_q^*)^n$ совпадают, поэтому

$$N_q = N_q^* + N_q(0) - N_q^*(0). \quad (2)$$

Из соотношения ортогональности для мультипликативных характеров (см. (5.13) в [3]) следует, что

$$N_q^* = \frac{1}{q-1} \sum_{\substack{x_1, \dots, x_n \in \mathbf{F}_q^*, \\ x_1 + \dots + x_n \neq 0}} \sum_{\psi} \psi(ax_1 \dots x_n) \bar{\psi}((x_1 + \dots + x_n)^m),$$

где ψ пробегает множество всех мультипликативных характеров поля $\mathbf{F}_q$. Отсюда

$$N_q^* = \frac{1}{q-1} \left(\sum_{\substack{x_1, \dots, x_n \in \mathbf{F}_q^* \\ x_1 + \dots + x_n \neq 0}} 1 + \sum_{\substack{\psi^m = \varepsilon \\ \psi \neq \varepsilon}} \psi(a) \sum_{\substack{x_1, \dots, x_n \in \mathbf{F}_q \\ x_1 + \dots + x_n \neq 0}} \psi(x_1 \dots x_n) \right. \\ \left. + \sum_{\psi^m \neq \varepsilon} \psi(a) \sum_{x_1, \dots, x_n \in \mathbf{F}_q} \psi(x_1 \dots x_n) \bar{\psi}^m(x_1 + \dots + x_n) \right),$$

то есть

$$N_q^* = (q-1)^{n-1} - \frac{1}{q-1} N_q^*(0) - \frac{1}{q-1} \sum_{\psi^m = \varepsilon, \psi \neq \varepsilon} \psi(a) J_0(\psi, \dots, \psi) \\ + \frac{1}{q-1} \sum_{\psi^m \neq \varepsilon} \psi((-1)^m a) J_0(\psi, \dots, \psi, \bar{\psi}^m), \quad (3)$$

где здесь и далее число переменных ψ в функции J_0 равно n . Согласно теоремам 5.20 и 5.21 в [3], сумма $J_0(\psi, \dots, \psi)$ отлична от нуля только при $\psi^n = \varepsilon$. В этом случае

$$\frac{1}{q-1} J_0(\psi, \dots, \psi) = \frac{1}{q} G(\psi)^n = -\frac{1}{q} G(\psi)^n G(\bar{\psi}^n).$$

Аналогично, сумма $J_0(\psi, \dots, \psi, \bar{\psi}^m)$ отлична от нуля только при $\psi^m \neq \varepsilon$, $\psi^{m-n} = \varepsilon$. В этом случае

$$\frac{1}{q-1} J_0(\psi, \dots, \psi, \bar{\psi}^m) = \frac{1}{q} G(\psi)^n G(\bar{\psi}^m) = \frac{1}{q} G(\psi)^n G(\bar{\psi}^n).$$

Тогда из (3) получаем, что

$$N_q^* = (q-1)^{n-1} - \frac{1}{q-1} N_q^*(0) + \frac{1}{q} \sum_{\psi^d = \varepsilon, \psi \neq \varepsilon} \psi((-1)^n a) G(\psi)^n G(\bar{\psi}^n).$$

Кроме того, $N_q(0) = q^{n-1}$ и

$$N_q^*(0) = \sum_{j=0}^{n-1} (-1)^j \binom{n}{j} q^{n-j-1} + (-1)^n = \frac{(q-1)^n + (-1)^n (q-1)}{q}.$$

Подставляя выражения для N_q^* , $N_q(0)$ и $N_q^*(0)$ в соотношение (2), получаем утверждение теоремы.

Рассмотрим случай, когда $\gcd(m-n, q-1)$ – четное число. Через $[r]$ будем обозначать наибольшее целое число, не превосходящее числа $r \in \mathbf{R}$.

Теорема 2. Пусть $\gcd(m - n, q - 1) = d$, d четно. Тогда

$$N_q = q^{n-1} + (-1)^{n-1} + (-1)^{n-1+[n/2](q-1)/2} \eta(a) q^{[(n-1)/2]} + \frac{1}{q} \sum_{\psi^d = \varepsilon, \psi^2 \neq \varepsilon} \psi((-1)^n a) G(\psi)^n G(\bar{\psi}^n).$$

В частности, при $\gcd(m - n, q - 1) = 2$

$$N_q = q^{n-1} + (-1)^{n-1} + (-1)^{n-1+[n/2](q-1)/2} \eta(a) q^{[(n-1)/2]}.$$

Доказательство. Согласно теореме 1, при четном d

$$N_q = q^{n-1} + (-1)^{n-1} + \frac{1}{q} \eta((-1)^n a) G(\eta)^n G(\eta^n) + \frac{1}{q} \sum_{\psi^d = \varepsilon, \psi^2 \neq \varepsilon} \psi((-1)^n a) G(\psi)^n G(\bar{\psi}^n).$$

Так как $\eta(-1) = (-1)^{(q-1)/2}$, из теорем 5.11 и 5.12 в [3] получаем, что

$$\frac{1}{q} \eta((-1)^n a) G(\eta)^n G(\eta^n) = (-1)^{n-1+[n/2](q-1)/2} \eta(a) q^{[(n-1)/2]},$$

что и требовалось доказать.

Перейдем к рассмотрению случая $\gcd(m - n, q - 1) > 2$.

Лемма 1. Пусть d — общий делитель чисел $m - n$ и $q - 1$, $d > 2$, $\gcd(d, n) = d_0$, l — наименьшее целое положительное число такое, что $d \mid (p^l + 1)$. Тогда

$$\begin{aligned} \frac{1}{q} \sum_{\psi^d = \varepsilon, \psi^2 \neq \varepsilon} \psi((-1)^n a) G(\psi)^n G(\bar{\psi}^n) \\ = (-1)^{((s/2l)-1)(n-1)} q^{(n-1)/2} T_1 - (-1)^{((s/2l)-1)n} q^{(n-2)/2} T_2, \end{aligned}$$

где

$$T_1 = \begin{cases} d - d_0, & \text{если } a - d\text{-я степень в } \mathbf{F}_q, \\ -d_0, & \text{если } a - d_0\text{-я, но не } d\text{-я степень в } \mathbf{F}_q, \\ 0 & \text{в остальных случаях,} \end{cases} \quad (4)$$

$$T_2 = \begin{cases} d_0 - 1, & \text{если } a - d_0\text{-я степень в } \mathbf{F}_q, \\ -1 & \text{в противном случае.} \end{cases} \quad (5)$$

Доказательство. Из условий леммы следует, что $2l \mid s$. Пусть ψ — характер порядка δ , $\delta > 1$, $\delta \mid d$. Покажем, что $\psi(-1) = 1$. Действительно, при $p = 2$ справедливо равенство $\psi(-1) = \psi(1) = 1$. Если $p > 2$, то из условий $2l \mid s$ и $d \mid (p^l + 1)$ следует, что $2d \mid (q - 1)$. Отсюда $\psi(-1) = \psi(g^{(q-1)/2}) = 1$, где g — примитивный элемент поля $\mathbf{F}_q$.

Заметим, что порядок характера $\bar{\psi}^n$ равен $\delta / \gcd(\delta, n)$, и значит, $\bar{\psi}^n = \varepsilon$ тогда и только тогда, когда $\psi^{d_0} = \varepsilon$. Если $2 \mid n$, или $2 \nmid d$, или $2\delta \mid d$, или $2d \mid (p^l + 1)$, то

согласно теоремам Дэвенпорта–Хассе (теорема 5.14 в [3]) и Штигельбергера (теорема 5.16 в [3])

$$G(\psi)^n = (-1)^{(s/(2l)-1)n} q^{n/2}$$

и

$$G(\bar{\psi}^n) = \begin{cases} -1, & \text{если } \psi^{d_0} = \varepsilon, \\ (-1)^{s/(2l)-1} \sqrt{q}, & \text{если } \psi^{d_0} \neq \varepsilon. \end{cases}$$

Предположим, что $2 \nmid n$, $2 \mid d$, $2\delta \nmid d$ и $2d \nmid (p^l + 1)$. Тогда числа p , $(p^l + 1)/\delta$ и $(p^l + 1)/(\delta/\gcd(\delta, n))$ нечетны, $\psi^{d_0} \neq \varepsilon$, и значит, $G(\psi) = G(\bar{\psi}^n) = -\sqrt{q}$. Таким образом, в любом случае

$$\frac{1}{q} G(\psi)^n G(\bar{\psi}^n) = \begin{cases} -(-1)^{(s/(2l)-1)n} q^{(n-2)/2}, & \text{если } \psi^{d_0} = \varepsilon, \\ (-1)^{(s/(2l)-1)(n-1)} q^{(n-1)/2}, & \text{если } \psi^{d_0} \neq \varepsilon. \end{cases}$$

Следовательно,

$$\begin{aligned} \frac{1}{q} \sum_{\psi^d = \varepsilon, \psi \neq \varepsilon} \psi((-1)^n a) G(\psi)^n G(\bar{\psi}^n) \\ = -(-1)^{(s/(2l)-1)n} q^{(n-2)/2} \sum_{\psi^{d_0} = \varepsilon, \psi \neq \varepsilon} \psi(a) \\ + (-1)^{(s/(2l)-1)(n-1)} q^{(n-1)/2} \left(\sum_{\psi^d = \varepsilon} \psi(a) - \sum_{\psi^{d_0} = \varepsilon} \psi(a) \right) \\ = (-1)^{(s/(2l)-1)(n-1)} q^{(n-1)/2} T_1 - (-1)^{(s/(2l)-1)n} q^{(n-2)/2} T_2, \end{aligned}$$

где T_1 и T_2 определяются равенствами (4) и (5). Лемма доказана.

Следующая теорема является следствием теоремы 1 и леммы 1.

Теорема 3. Пусть $\gcd(m - n, q - 1) = d$, $\gcd(m, n, q - 1) = d_0$, $d > 2$, l — наименьшее целое положительное число такое, что $d \mid (p^l + 1)$. Тогда

$$N_q = q^{n-1} + (-1)^{n-1} + (-1)^{((s/2l)-1)(n-1)} q^{(n-1)/2} T_1 - (-1)^{((s/2l)-1)n} q^{(n-2)/2} T_2,$$

где T_1 и T_2 определяются равенствами (4) и (5).

Напомним (см. раздел 2 главы 5 в [3]), что поднятием мультипликативного характера ψ поля $\mathbf{F}_q$ до поля $\mathbf{F}_{q^t}$ называется характер ψ' поля $\mathbf{F}_{q^t}$, заданный соотношением $\psi'(x) = \psi(N_{\mathbf{F}_{q^t}/\mathbf{F}_q}(x))$ для всех $x \in \mathbf{F}_{q^t}$, где

$$N_{\mathbf{F}_{q^t}/\mathbf{F}_q}(x) = x x^q x^{q^2} \dots x^{q^{t-1}} = x^{(q^t-1)/(q-1)}$$

— норма элемента x над полем $\mathbf{F}_q$. Из определения следует, что характеры ψ и ψ' имеют одинаковый порядок. Кроме того, для сумм Якоби $J(\psi)$ и $J(\psi')$ имеет место соотношение (см. теорему 5.26 в [3])

$$J(\psi') = (-1)^{t-1} J(\psi)^t. \quad (6)$$

Найдем значение N_q при условии, что $\gcd(m - n, q - 1) = 3$. Случай $p \equiv 2 \pmod{3}$ уже рассмотрен в теореме 3. Для исследования случая $p \equiv 1 \pmod{3}$ нам потребуется следующее утверждение.

Лемма 2. Пусть $p \equiv 1 \pmod{3}$ и ψ — кубический характер поля $\mathbb{F}_q$. Тогда

$$\begin{aligned} \frac{1}{q}(\psi(a)G(\psi)^n G(\bar{\psi}^n) + \bar{\psi}(a)G(\bar{\psi})^n G(\psi^n)) \\ = \begin{cases} (-1)^n q^{\lfloor (n-1)/3 \rfloor} A, & \text{если } a \text{ — куб в } \mathbb{F}_q, \\ (-1)^{n-1} q^{\lfloor (n-1)/3 \rfloor} (A + 9B)/2 & \text{в противном случае.} \end{cases} \end{aligned} \quad (7)$$

Целые числа A и $|B|$ однозначно определяются условиями

$$4q^{\lfloor (n+1)/3 \rfloor} = A^2 + 27B^2, \quad A \equiv 1 \pmod{3}, \quad p \nmid A. \quad (8)$$

Если a не является кубом в $\mathbb{F}_q$, то знак числа B определяется сравнением

$$9B(a^{(q-1)/3} + 1) \equiv A(a^{(q-1)/3} - 1) \pmod{p}. \quad (9)$$

Доказательство. Можно считать, что $\psi(a) = (-1 + i\sqrt{3})/2$, если a не является кубом в $\mathbb{F}_q$ (в противном случае заменим ψ сопряженным характером $\bar{\psi}$). Из теорем 5.11, 5.12, 5.21 в [3] и из соотношения (6) следует, что

$$G(\psi)^3 = G(\psi)G(\bar{\psi})J(\psi) = qJ(\psi)$$

и

$$\frac{1}{q} G(\psi)^n G(\bar{\psi}^n) = (-1)^n q^{\lfloor (n-1)/3 \rfloor} J(\psi'), \quad (10)$$

где ψ' — поднятие характера ψ до поля $\mathbb{F}_{q^{\lfloor (n+1)/3 \rfloor}}$, то есть кубический характер поля $\mathbb{F}_{q^{\lfloor (n+1)/3 \rfloor}}$. Согласно предложению 1 из [4]

$$J(\psi') = (A + 3Bi\sqrt{3})/2,$$

где целые числа A и $|B|$ однозначно определяются условиями (8). Если g — примитивный элемент поля $\mathbb{F}_{q^{\lfloor (n+1)/3 \rfloor}}$ такой, что $\psi'(g) = (-1 + i\sqrt{3})/2$, то знак числа B определяется сравнением

$$9B(g^{(q^{\lfloor (n+1)/3 \rfloor} - 1)/3} + 1) \equiv A(g^{(q^{\lfloor (n+1)/3 \rfloor} - 1)/3} - 1) \pmod{p}. \quad (11)$$

Отсюда и из (10) получаем равенство (7). Заметим, что в случае, когда a является кубом в $\mathbb{F}_q$, искомая сумма не зависит от числа B . Если a не является кубом в $\mathbb{F}_q$, то из условия $\psi(a) = \psi'(g) = \psi(g^{(q^{\lfloor (n+1)/3 \rfloor} - 1)/(q-1)})$ следует, что $a^{(q-1)/3} = g^{(q^{\lfloor (n+1)/3 \rfloor} - 1)/3}$. Тогда условие (11) равносильно условию (9). Лемма доказана.

Теорема 4 следует из теоремы 1 и леммы 2.

Теорема 4. Пусть $\gcd(m - n, q - 1) = 3$ и $p \equiv 1 \pmod{3}$. Тогда

$$N_q = q^{n-1} + (-1)^{n-1} + (-1)^n q^{\lfloor (n-1)/3 \rfloor} A,$$

если a — куб в $\mathbb{F}_q$, и

$$N_q = q^{n-1} + (-1)^{n-1} + (-1)^{n-1} q^{\lfloor (n-1)/3 \rfloor} (A + 9B)/2$$

в противном случае. Целые числа A и $|B|$ однозначно определяются соотношениями (8). Если a не является кубом в $\mathbb{F}_q$, то знак числа B определяется сравнением (9).

Найдем формулу для N_q при условии, что $\gcd(m - n, q - 1) = 6$. Согласно теореме 3 достаточно исследовать случай $p \equiv 1 \pmod{6}$.

Лемма 3. Пусть $p \equiv 1 \pmod{6}$ и ψ — характер порядка 6 поля $\mathbf{F}_q$. Тогда

$$\begin{aligned} & \frac{1}{q} (\psi((-1)^n a) G(\psi)^n G(\bar{\psi}^n) + \bar{\psi}((-1)^n a) G(\bar{\psi})^n G(\psi^n)) \\ &= \begin{cases} (-1)^{n+[n/2](q-1)/2} \eta(a) q^{\lfloor (n-1)/6 \rfloor} C, & \text{если } b \text{ — куб в } \mathbf{F}_q, \\ (-1)^{n-1+[n/2](q-1)/2} \eta(a) q^{\lfloor (n-1)/6 \rfloor} (C - 9D)/2 & \text{в противном случае,} \end{cases} \end{aligned}$$

где

$$b = \begin{cases} 4a, & \text{если } n \equiv -2 \pmod{6}, \\ 2a, & \text{если } n \equiv -1 \pmod{6}, \\ a & \text{в остальных случаях,} \end{cases} \quad (12)$$

$$t = \begin{cases} \lfloor (2n+1)/3 \rfloor, & \text{если } n \equiv \pm 2 \pmod{6}, \\ 2\lfloor (n+1)/3 \rfloor & \text{в остальных случаях.} \end{cases} \quad (13)$$

Целые числа C и $|D|$ однозначно определяются условиями

$$4q^t = C^2 + 27D^2, \quad C \equiv 1 \pmod{3}, \quad p \nmid C. \quad (14)$$

Если b не является кубом в $\mathbf{F}_q$, то знак числа D определяется сравнением

$$9D(b^{(q-1)/3} + 1) \equiv C(b^{(q-1)/3} - 1) \pmod{p}. \quad (15)$$

Доказательство. Представим ψ в виде $\psi = \lambda\eta$, где λ — кубический характер поля $\mathbf{F}_q$. Можно считать, что $\lambda(b) = (-1 + i\sqrt{3})/2$, если b не является кубом в $\mathbf{F}_q$ (b определяется равенством (12)). Из теорем 5.11, 5.12, 5.21, 5.28 в [3] и из соотношения (6) следует равенство

$$\frac{1}{q} \psi((-1)^n a) G(\psi)^n G(\bar{\psi}^n) = (-1)^{n+[n/2](q-1)/2} q^{\lfloor (n-1)/6 \rfloor} J(\bar{\lambda}'),$$

где λ' — поднятие характера λ до поля $\mathbf{F}_{q'}$, t определяется равенством (13). Далее доказательство аналогично доказательству леммы 3.

Теорема 5 является следствием теоремы 2 и лемм 2 и 3.

Теорема 5. Пусть $\gcd(m - n, q - 1) = 6$ и $p \equiv 1 \pmod{6}$. Тогда

$$\begin{aligned} N_q &= q^{n-1} + (-1)^{n-1} + (-1)^{n-1+[n/2](q-1)/2} \eta(a) q^{\lfloor (n-1)/2 \rfloor} \\ &\quad + (-1)^{n-1} q^{\lfloor (n-1)/3 \rfloor} T_1 + (-1)^{n-1+[n/2](q-1)/2} \eta(a) q^{\lfloor (n-1)/6 \rfloor} T_2, \end{aligned}$$

где

$$\begin{aligned} T_1 &= \begin{cases} -A, & \text{если } a \text{ — куб в } \mathbf{F}_q, \\ (A + 9B)/2 & \text{в противном случае,} \end{cases} \\ T_2 &= \begin{cases} -C, & \text{если } b \text{ — куб в } \mathbf{F}_q, \\ (C - 9D)/2 & \text{в противном случае,} \end{cases} \end{aligned}$$

элемент b и число t определяются равенствами (12) и (13) соответственно. Целые числа A , $|B|$, C и $|D|$ однозначно определяются условиями (8) и (14). Если a не является кубом в $\mathbb{F}_q$, то знак числа B определяется сравнением (9). Если b не является кубом в $\mathbb{F}_q$, то знак числа D определяется сравнением (15).

Автор благодарит В. Н. Чубарикова за постоянное внимание и интерес к этой работе.

Список литературы

1. Carlitz L., The number of solutions of some equations in a finite field. *Portug. Math.* (1954) **13**, №1, 25–31.
2. Баулина Ю. Н., *Формулы для числа решений уравнений марковского типа в конечных полях*. Дисс. канд. физ.-матем. наук, МПГУ, 2001.
3. Лидл Р., Нидеррайтер Г., *Конечные поля*. Мир, Москва, 1988.
4. Katre S. A., Rajwade A. R., Complete solution of the cyclotomic problem in $\mathbb{F}_q$ for any prime modulus l , $q = p^\alpha$, $p \equiv 1 \pmod{l}$. *Acta Arithm.* (1985) **45**, №3, 183–199.

Статья поступила 22.04.2003.