Сибирский математический журнал
Январь—февраль, 2003. Том 44, № 1

УДК 512.624.3

О ТОЧНЫХ ФОРМУЛАХ ДЛЯ ЧИСЛА РЕШЕНИЙ УРАВНЕНИЯ $(x_1 + \cdots + x_n)^2 = ax_1 \cdots x_n$ В КОНЕЧНОМ ПОЛЕ

Ю. Н. Баулина

Аннотация: Рассматривается уравнение заголовка в конечном поле из q элементов. При некоторых соотношениях между n и q получены точные формулы для числа решений указанного уравнения.

Ключевые слова: уравнение в конечном поле, сумма Гаусса, сумма Якоби

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

$$(x_1 + \cdots + x_n)^2 = ax_1 \cdots x_n, \tag{1}$$

где $a \in \mathbb{F}_q^*$, $n \geq 3$. Обозначим через N_q число решений (1) в $\mathbb{F}_q^n$. Л. Карлиц в работе [1] доказал, что

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

В той же работе поставлена задача нахождения точной формулы для N_q при $n \geq 5$. В данной статье указанная проблема решена для всех n и q, для которых $d = \text{НОД}(n-2, q-1) \leq 4$. Частично исследован случай $d > 4$. При условии, что существует натуральное число l такое, что $d \mid p^l + 1$, также найдены точные формулы для N_q.

Пусть ψ — мультипликативный, а χ — канонический аддитивный характеры $\mathbb{F}_q$. Определим суммы Гаусса и Якоби равенствами

$$G(\psi, \chi) = \sum_{x \in \mathbb{F}_q^*} \psi(x)\chi(x), \quad J(\psi) = \sum_{x \in \mathbb{F}_q} \psi(x)\psi(1-x)$$

соответственно (как обычно, полагаем $\psi(0) = 0$ для нетривиального характера ψ и $\varepsilon(0) = 1$). Для данных мультипликативных характеров $\psi_1, \dots, \psi_r$ определим сумму

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

где суммирование ведется по всем наборам $(x_1, \dots, x_r) \in \mathbb{F}_q^r$ таким, что $x_1 + \cdots + x_r = 0$. Все необходимые свойства характеров и сумм $G(\psi, \chi)$, $J(\psi)$ и $J_0(\psi_1, \dots, \psi_r)$ изложены в книгах [2, 3].

Покажем сначала, что проблема нахождения точной формулы для N_q сводится к проблеме вычисления точных значений сумм Гаусса.

Результаты статьи были доложены на Международной конференции «Мальцевские чтения — 2000».

Лемма. *Пусть* НОД$(n-2, q-1) = d$. *Если* d *нечетно, то*

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

если d *четно, то*

$$N_q = q^{n-1} - 1 - (-1)^{\frac{n(q-1)}{4}} \eta(a) q^{\frac{n-2}{2}} + \frac{1}{q} \sum_{\substack{\psi^d=\varepsilon \\ \psi^2 \neq \varepsilon}} \bar{\psi}(a) G(\bar{\psi}, \chi)^n G(\psi^2, \chi),$$

где суммирование ведется по всем мультипликативным характерам ψ *поля* $\mathbb{F}_q$, *удовлетворяющим указанным условиям.*

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

$$x_1 + \cdots + x_n = 0$$

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

$$N_q = N_q^* + N_q(0) - N_q^*(0). \tag{2}$$

Из соотношения ортогональности для мультипликативных характеров [3] следует, что

$$N_q^* = \frac{1}{q-1} \sum_{\substack{x_1,\ldots,x_n \in \mathbb{F}_q^* \\ x_1+\cdots+x_n \neq 0}} \sum_{\psi} \psi((x_1 + \cdots + x_n)^2) \bar{\psi}(a x_1 \cdots x_n).$$

Выделяя во внутренней сумме слагаемые, соответствующие тривиальному и квадратичному (в случае нечетного q) характерам, получаем

$$N_q^* = \frac{1}{q-1} \Big[\sum_{\substack{x_1,\ldots,x_n \in \mathbb{F}_q^* \\ x_1+\cdots+x_n \neq 0}} 1 + T + \sum_{\psi^2 \neq \varepsilon} \bar{\psi}(a) \sum_{x_1,\ldots x_n \in \mathbb{F}_q} \bar{\psi}(x_1) \cdots \bar{\psi}(x_n) \psi^2(-x_1 - \cdots - x_n) \Big],$$

т. е.

$$N_q^* = \frac{1}{q-1} \Big[(q-1)^n - N_q^*(0) + T + \sum_{\psi^2 \neq \varepsilon} \bar{\psi}(a) J_0(\underbrace{\bar{\psi}, \ldots, \bar{\psi}}_{n}, \psi^2) \Big], \tag{3}$$

где $T = 0$, если q четно, и

$$T = \eta(a) \sum_{\substack{x_1,\ldots,x_n \in \mathbb{F}_q \\ x_1+\cdots+x_n \neq 0}} \eta(x_1) \cdots \eta(x_n) = -\eta(a) J_0(\underbrace{\eta, \ldots, \eta}_{n}),$$

если q нечетно. Известно [2, 3], что сумма $J_0(\underbrace{\bar{\psi}, \ldots, \bar{\psi}}_{n}, \psi^2)$ отлична от нуля только при $\bar{\psi}^n \psi^2 = \bar{\psi}^{n-2} = \varepsilon$, т. е. при $\psi^d = \varepsilon$. В этом случае

$$\frac{1}{q-1} J_0(\underbrace{\bar{\psi}, \ldots, \bar{\psi}}_{n}, \psi^2) = \frac{1}{q} G(\bar{\psi}, \chi)^n G(\psi^2, \chi). \tag{4}$$

Аналогично сумма $J_0(\underbrace{\eta,\ldots,\eta}_{n})$ отлична от нуля только при четном n, т. е. тогда и только тогда, когда d четно. В этом случае

$$\frac{1}{q-1}J_0(\underbrace{\eta,\ldots,\eta}_{n}) = \frac{1}{q}\,G(\eta,\chi)^n = (-1)^{\frac{n(q-1)}{4}}q^{\frac{n-2}{2}}. \tag{5}$$

Кроме того,

$$N_q(0) = q^{n-1};$$

$$N_q^*(0) = q^{n-1} - \binom{n}{1}q^{n-2} + \binom{n}{2}q^{n-3} - \cdots + (-1)^{n-2}\binom{n}{n-2}q + (-1)^{n-1}\binom{n}{n-1} + (-1)^n = \frac{(q-1)^n + (-1)^n(q-1)}{q}.$$

Отсюда и из соотношений (2)–(5) получаем утверждение леммы.

Следующие две теоремы являются очевидными следствиями леммы.

Теорема 1. *Пусть* НОД$(n-2, q-1) = 1$. *Тогда*

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

Теорема 2. *Пусть* НОД$(n-2, q-1) = 2$. *Тогда*

$$N_q = q^{n-1} - 1 - (-1)^{\frac{n(q-1)}{4}}\eta(a)q^{\frac{n-2}{2}}.$$

Частичный ответ на вопрос о точном значении N_q при $d > 2$ дает

Теорема 3. *Пусть* НОД$(n-2, q-1) = d$, $d > 2$, l — *наименьшее натуральное число такое, что* $d \mid p^l + 1$. *Тогда*

$$N_q = q^{n-1} + (-1)^{n-1} + (-1)^{(\frac{s}{2l}-1)(n-1)}q^{\frac{n-1}{2}}T,$$

если d *нечетно, и*

$$N_q = q^{n-1} - 1 - \eta(a)q^{\frac{n-2}{2}} + (-1)^{\frac{s}{2l}}\eta(a)q^{\frac{n-1}{2}} + (-1)^{\frac{s}{2l}-1}q^{\frac{n-1}{2}}T,$$

если d *четно, где*

$$T = \begin{cases} d-1, & \text{если } a = b^d \text{ при некотором } b \in \mathbb{F}_q^*, \\ -1 & \text{в противном случае.} \end{cases} \tag{6}$$

Доказательство. Из условий теоремы следует, что $2l \mid s$. Пусть ψ — характер порядка δ, $\delta > 2$, $\delta \mid d$, тогда $\delta \mid p^l + 1$. Если δ нечетно, то порядок характера ψ^2 также равен δ и из теорем Дэвенпорта — Хассе и Штикельбергера [3] получаем

$$G(\bar{\psi},\chi) = G(\psi^2,\chi) = (-1)^{\frac{s}{2l}-1}(p^l)^{\frac{s}{2l}} = (-1)^{\frac{s}{2l}-1}\sqrt{q}$$

и

$$G(\bar{\psi},\chi)^n G(\psi^2,\chi) = (-1)^{(\frac{s}{2l}-1)(n-1)}q^{\frac{n+1}{2}}. \tag{7}$$

Если δ четно, то порядок характера ψ^2 равен $\delta/2$. Так как $\delta > 2$ и $\frac{p^l+1}{\delta/2}$ четно, то

$$G(\psi^2,\chi) = (-1)^{\frac{s}{2l}-1}\sqrt{q}, \quad G(\bar{\psi},\chi) = (-1)^{\frac{s}{2l}-1}(\pm p^l)^{\frac{s}{2l}} = \pm\sqrt{q}.$$

Отсюда, учитывая, что n в данном случае четно, получаем равенство (7) при четном δ. Замечая, что q является полным квадратом и, значит, $q \equiv 1 \,(\mathrm{mod}\ 8)$ при четном d, по лемме имеем

$$N_q = q^{n-1} + (-1)^{n-1} + (-1)^{(\frac{s}{2l}-1)(n-1)} q^{\frac{n-1}{2}} \sum_{\substack{\psi^d=\varepsilon \\ \psi\neq\varepsilon}} \bar{\psi}(a)$$
$$= q^{n-1} + (-1)^{n-1} + (-1)^{(\frac{s}{2l}-1)(n-1)} q^{\frac{n-1}{2}} T,$$

если d нечетно, и

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

если d четно, где T определяется равенством (6). Теорема доказана.

Найдем значение N_q при НОД$(n-2, q-1) = 3$. Случай $p \equiv 2 \,(\mathrm{mod}\ 3)$ уже рассмотрен в теореме 3. При $p \equiv 1 \,(\mathrm{mod}\ 3)$ ответ на поставленный вопрос дает

Теорема 4. *Пусть* НОД$(n-2, q-1) = 3$, $p \equiv 1 \,(\mathrm{mod}\ 3)$. *Тогда*

$$N_q = q^{n-1} + 1 + \frac{q^{\frac{n-2}{3}}}{2^{\frac{n+1}{3}}} T,$$

где

$$T = 2 \sum_{\substack{k=0 \\ 2|k}}^{\frac{n+1}{3}} \binom{\frac{n+1}{3}}{k} A^{\frac{n+1}{3}-k} (-27B^2)^{\frac{k}{2}},$$

если a — *куб в* $\mathbb{F}_q$, *и*

$$T = -\sum_{\substack{k=0 \\ 2|k}}^{\frac{n+1}{3}} \binom{\frac{n+1}{3}}{k} A^{\frac{n+1}{3}-k} (-27B^2)^{\frac{k}{2}} - 9B \sum_{\substack{k=0 \\ 2\nmid k}}^{\frac{n+1}{3}} \binom{\frac{n+1}{3}}{k} A^{\frac{n+1}{3}-k} (-27B^2)^{\frac{k-1}{2}}$$

в противном случае, целые числа A *и* B *определяются условиями*

$$4q = A^2 + 27B^2, \quad A \equiv 1 \pmod 3, \quad p \nmid A$$

и условием

$$9B(a^{\frac{q-1}{3}} + 1) \equiv A(a^{\frac{q-1}{3}} - 1) \pmod p,$$

если a *не является кубом в* $\mathbb{F}_q$.

Доказательство. Из условий теоремы следует, что n и q нечетны. Пусть ψ — кубический характер поля $\mathbb{F}_q$. Можно считать, что если a не является кубом в $\mathbb{F}_q$, то $\psi(a) = (-1+i\sqrt{3})/2$ (в противном случае заменим ψ сопряженным характером $\bar{\psi}$). Так как $\psi^2 = \bar{\psi}$, то согласно лемме

$$N_q = q^{n-1} + 1 + \frac{1}{q} [\psi(a) G(\psi, \chi)^{n+1} + \bar{\psi}(a) G(\bar{\psi}, \chi)^{n+1}]. \tag{8}$$

Известно [2–4], что

$$G(\psi, \chi)^3 = qJ(\psi) = \frac{q(A + 3Bi\sqrt{3})}{2}, \tag{9}$$

где целые числа A и B определяются условиями

$$4q = A^2 + 27B^2, \quad A \equiv 1 \pmod 3, \quad p \nmid A, \quad 9B(g^{\frac{q-1}{3}} + 1) \equiv A(g^{\frac{q-1}{3}} - 1) \pmod p,$$

g — примитивный элемент $\mathbb{F}_q$ такой, что $\psi(g) = (-1 + i\sqrt{3}\,)/2$. Из (8) и (9) имеем

$$N_q = q^{n-1} + 1 + \frac{q^{\frac{n-2}{3}}}{2^{\frac{n+1}{3}}}[\psi(a)(A + 3Bi\sqrt{3})^{\frac{n+1}{3}} + \bar{\psi}(a)(A - 3Bi\sqrt{3})^{\frac{n+1}{3}}]. \tag{10}$$

Если a — куб в $\mathbb{F}_q$, то $\psi(a) = \bar{\psi}(a) = 1$ и из (10) следует утверждение теоремы. Если a не является кубом в $\mathbb{F}_q$, то $\psi(a) = (-1 + i\sqrt{3}\,)/2$. Тогда

$$\begin{aligned}
&\psi(a)(A + 3Bi\sqrt{3})^{\frac{n+1}{3}} + \bar{\psi}(a)(A - 3Bi\sqrt{3})^{\frac{n+1}{3}} \\
&\quad = -\sum_{\substack{k=0 \\ 2|k}}^{\frac{n+1}{3}} \binom{\frac{n+1}{3}}{k} A^{\frac{n+1}{3}-k}(3Bi\sqrt{3})^k + i\sqrt{3}\sum_{\substack{k=0 \\ 2\nmid k}}^{\frac{n+1}{3}} \binom{\frac{n+1}{3}}{k} A^{\frac{n+1}{3}-k}(3Bi\sqrt{3})^k \\
&\quad = -\sum_{\substack{k=0 \\ 2|k}}^{\frac{n+1}{3}} \binom{\frac{n+1}{3}}{k} A^{\frac{n+1}{3}-k}(-27B^2)^{\frac{k}{2}} - 9B\sum_{\substack{k=0 \\ 2\nmid k}}^{\frac{n+1}{3}} \binom{\frac{n+1}{3}}{k} A^{\frac{n+1}{3}-k}(-27B^2)^{\frac{k-1}{2}}.
\end{aligned} \tag{11}$$

Кроме того, из условия $\psi(a) = \psi(g)$ вытекает, что $\operatorname{ind}_g a \equiv 1 \pmod 3$ и $a^{\frac{q-1}{3}} = (g^{\operatorname{ind}_g a})^{\frac{q-1}{3}} = g^{\frac{q-1}{3}}$. Отсюда и из (10) и (11) получаем утверждение теоремы.

Перейдем к рассмотрению случая НОД$(n-2, q-1) = 4$. Так как при $p \equiv 3 \pmod 4$ точная формула для N_q уже установлена в теореме 3, то остается исследовать случай $p \equiv 1 \pmod 4$.

Теорема 5. *Пусть* НОД$(n-2, q-1) = 4, p \equiv 1 \pmod 4$. *Тогда*

$$N_q = q^{n-1} - 1 - \eta(a)q^{\frac{n-2}{2}} + 2q^{\frac{n-2}{4}}T,$$

где

$$T = -\sum_{\substack{k=0 \\ 2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} C^{\frac{n}{2}-k}(-D^2)^{\frac{k}{2}},$$

если a — биквадрат в $\mathbb{F}_q$,

$$T = \sum_{\substack{k=0 \\ 2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} C^{\frac{n}{2}-k}(-D^2)^{\frac{k}{2}},$$

если a — квадрат, но не биквадрат в $\mathbb{F}_q$,

$$T = -D\sum_{\substack{k=0 \\ 2\nmid k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} C^{\frac{n}{2}-k}(-D^2)^{\frac{k-1}{2}},$$

если a не является квадратом $\mathbb{F}_q$, целые числа C и D определяются условиями

$$q = C^2 + D^2, \quad C \equiv 1 \pmod 4, \quad p \nmid C$$

и условием

$$Da^{\frac{q-1}{4}} \equiv C \pmod p,$$

если a не является квадратом в $\mathbb{F}_q$.

Доказательство. Из условий теоремы следует, что $q \equiv 1 \,(\mathrm{mod}\ 4)$, а n четно. Пусть ψ — биквадратичный характер поля $\mathbb{F}_q$. Можно считать, что если a не является квадратом в $\mathbb{F}_q$, то $\psi(a) = i$. По лемме имеем

$$N_q = q^{n-1} - 1 - \eta(a)q^{\frac{n-2}{2}} + \frac{1}{q}\,G(\eta,\chi)[\psi(a)G(\psi,\chi)^n + \bar{\psi}(a)G(\bar{\psi},\chi)^n]. \tag{12}$$

Известно [3, 5], что при $p \equiv 1 \,(\mathrm{mod}\ 4)$

$$G(\eta,\chi) = (-1)^{s-1}\sqrt{q}, \quad G(\psi,\chi)^2 = G(\eta,\chi)J(\psi) = (-1)^{s-1}\sqrt{q}(-C + Di),$$

где целые числа C и D определяются условиями

$$q = C^2 + D^2, \quad C \equiv 1 \pmod 4, \quad p \nmid C, \quad Dg^{\frac{q-1}{4}} \equiv C \pmod p,$$

g — примитивный элемент поля $\mathbb{F}_q$ такой, что $\psi(g) = i$. Отсюда и из (12) вытекает, что

$$N_q = q^{n-1} - 1 - \eta(a)q^{\frac{n-2}{2}} + (-1)^{\frac{(s-1)(n+2)}{2}} q^{\frac{n-2}{4}}[\psi(a)(-C+Di)^{\frac{n}{2}} + \bar{\psi}(a)(-C-Di)^{\frac{n}{2}}],$$

т. е.

$$N_q = q^{n-1} - 1 - \eta(a)q^{\frac{n-2}{2}} - q^{\frac{n-2}{4}}[\psi(a)(C - Di)^{\frac{n}{2}} + \bar{\psi}(a)(C + Di)^{\frac{n}{2}}]. \tag{13}$$

Если a — квадрат в $\mathbb{F}_q$, то $\psi(a) = \bar{\psi}(a) = 1$, если a — биквадрат, и $\psi(a) = \bar{\psi}(a) = -1$ в противном случае. Отсюда и из (13) получаем утверждение теоремы для случая, когда a — квадрат в $\mathbb{F}_q$. Если a не является квадратом в $\mathbb{F}_q$, то $\psi(a) = i$. Из условия $\psi(a) = \psi(g)$ следует, что $\mathrm{ind}_g\, a \equiv 1 \,(\mathrm{mod}\ 4)$. Тогда $a^{\frac{q-1}{4}} = (g^{\mathrm{ind}_g a})^{\frac{q-1}{4}} = g^{\frac{q-1}{4}}$. Отсюда и из (13) получаем утверждение теоремы.

ЛИТЕРАТУРА

1. *Carlitz L.* The number of solutions of some equations in a finite field // Portugal. Math. 1954. V. 13, N 1. P. 25–31.
2. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987.
3. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988.
4. *Katre S. A., Rajwade A. R.* Complete solution of the cyclotomic problem in $\mathbb{F}_q$ for any prime modulus l, $q = p^\alpha$, $p \equiv 1 \,(\mathrm{mod}\ l)$ // Acta Arith. 1985. V. 45, N 3. P. 183–199.
5. *Katre S. A., Rajwade A. R.* Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum // Math. Scand. 1987. V. 60, N 1. P. 52–62.

Статья поступила 17 мая 2002 г.

Баулина Юлия Николаевна
Московский педагогический гос. университет, математический факультет,
ул. Краснопрудная, 14, Москва 107140
jbaulina@aport.ru, jbaulina@mail.ru