Мальцевские чтения
Новосибирск (2000)
Тезисы докладов

О точных формулах для числа решений уравнения $(x_1 + \dots + x_n)^2 = ax_1 \dots x_n$ в конечном поле

Ю. Н. Баулина

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). Рассмотрим уравнение

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

где $a \in \mathbf{F}_q^*$, $n \geqslant 3$. Обозначим через N_q число решений уравнения (1) в $\mathbf{F}_q^n$. Л. Карлиц в работе [**1**] доказал, что при $n = 3$ и нечетном q

$$N_q = q^2 + 1,$$

а при $n = 4$ и нечетном q

$$N_q = q^3 - 1 - \eta(a)q.$$

В той же статье поставлена задача нахождения точной формулы для N_q при произвольном $n \geqslant 5$. Автором данной работы получено частичное решение указанной проблемы — найдены точные формулы для N_q при всех $d \leqslant 4$, где $d = (n-2, q-1)$, и при произвольном $d > 4$ в случае, когда существует натуральное l, такое, что $d \mid p^l + 1$.

Теорема 1. *Если $(n-2, q-1) = 1$, то*

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

Теорема 2. *Если $(n-2, q-1) = 2$, то*

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

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

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

где

$$T = \begin{cases} d-1, & \textit{если } (\exists b \in \mathbf{F}_q^*) a = b^d, \\ -1, & \textit{если } (\forall b \in \mathbf{F}_q^*) a \neq b^d. \end{cases}$$

Теорема 4. *Пусть* $(n-2, q-1) = 3$, $p \equiv 1 (\mathrm{mod}\ 3)$. *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* $\mathbf{F}_q$, *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 *однозначно определяются условиями*

$$4q = A^2 + 27B^2, \qquad A \equiv 1 \pmod 3, \qquad (A, p) = 1$$

и

$$9(a^{\frac{q-1}{3}} + 1)B \equiv A(a^{\frac{q-1}{3}} - 1) \pmod p, \ \textit{если } (\forall b \in \mathbf{F}_q^*) a \neq b^3.$$

Теорема 5. *Пусть* $(n-2, q-1) = 4$, $p \equiv 1 (\mathrm{mod}\ 4)$. *Тогда*

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

где

$$T = \begin{cases} -\sum\limits_{\substack{k=0 \\ 2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} C^{\frac{n}{2}-k} (-D^2)^{\frac{k}{2}}, & \textit{если } (\exists b \in \mathbf{F}_q^*) a = b^4, \\ \sum\limits_{\substack{k=0 \\ 2|k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} C^{\frac{n}{2}-k} (-D^2)^{\frac{k}{2}}, & \textit{если } (\exists b \in \mathbf{F}_q^*) a = b^2 \wedge \eta(b) = -1, \\ -D \sum\limits_{\substack{k=0 \\ 2\nmid k}}^{\frac{n}{2}} \binom{\frac{n}{2}}{k} C^{\frac{n}{2}-k} (-D^2)^{\frac{k-1}{2}}, & \textit{если } \eta(a) = -1, \end{cases}$$

целые числа C *и* D *однозначно определяются условиями*

$$q = C^2 + D^2, \qquad C \equiv 1 \pmod 4, \qquad (C, p) = 1$$

и

$$a^{\frac{q-1}{4}} D \equiv C \pmod p \ \textit{при } \eta(a) = -1.$$

Литература

[1] L. Carlitz, *The number of solutions of some equations in a finite field*, Port. Math. **13** (1954), no. 1, 25–31.

Московский педагогический государственный университет
E-mail: jbaulina@yahoo.com