Journal de Théorie des Nombres
de Bordeaux **17** (2005), 45–50

On some equations over finite fields

par Ioulia BAOULINA

Résumé. Dans ce papier, suivant L. Carlitz, nous considérons des équations particulières à n variables sur le corps fini à q éléments. Nous obtenons des formules explicites pour le nombre de solutions de ces équations, sous une certaine condition sur n et q.

Abstract. In this paper, following L. Carlitz we consider some special equations of n variables over the finite field of q elements. We obtain explicit formulas for the number of solutions of these equations, under a certain restriction on n and q.

1. Introduction and results

Let p be an odd rational prime, $q = p^s$, $s \geq 1$, and $\mathbb{F}_q$ be the finite field of q elements. In 1954 L. Carlitz [4] proposed the problem of finding explicit formula for the number of solutions in $\mathbb{F}_q^n$ of the equation

$$a_1 x_1^2 + \cdots + a_n x_n^2 = b x_1 \cdots x_n, \tag{1.1}$$

where $a_1, \ldots, a_n, b \in \mathbb{F}_q^*$ and $n \geq 3$. He obtained formulas for $n = 3$ and also for $n = 4$ and noted that for $n \geq 5$ it is a difficult problem. The case $n = 3$, $a_1 = a_2 = a_3 = 1$, $b = 3$ (so-called Markoff equation) also was treated by A. Baragar [2]. In particular, he obtained explicitly the zeta-function of the corresponding hypersurface.

Let g be a generator of the cyclic group $\mathbb{F}_q^*$. It may be remarked that by multiplying (1.1) by a properly chosen element of $\mathbb{F}_q^*$ and also by replacing x_i by $k_i x_i$ for suitable $k_i \in \mathbb{F}_q^*$ and permuting the variables, the equation (1.1) can be reduced to the form

$$x_1^2 + \cdots + x_m^2 + g x_{m+1}^2 + \cdots + g x_n^2 = c x_1 \cdots x_n, \tag{1.2}$$

where $a \in \mathbb{F}_q^*$ and $n/2 \leq m \leq n$. It follows from this that it is sufficient to evaluate the number of solutions of the equation (1.2).

Let N_q denote the number of solutions in $\mathbb{F}_q^n$ of the equation (1.2), and $d = \gcd(n-2, (q-1)/2)$. Recently the present author [1] obtained the explicit formulas for N_q in the cases when $d = 1$ and $d = 2$. Note that in the case when $d = 1$, N_q is independent of c.

In this paper we determine explicitly N_q if d is a special divisor of $q - 1$. Our main results are the following two theorems.

Theorem 1.1. *Suppose that $d > 1$ and there is a positive integer l such that $2d \mid (p^l + 1)$ with l chosen minimal. Then*

$$\begin{aligned} N_q = q^{n-1} &+ \frac{1}{2}(1+(-1)^n)(-1)^m q^{(n-2)/2}(q-1) \\ &+ (-1)^{m+1}(q-1)^{n-m} \sum_{\substack{k=0 \\ 2\mid k}}^{2m-n} \binom{2m-n}{k} q^{k/2} \\ &+ (-1)^{((s/2l)-1)(n-1)} 2^{n-1} q^{(n-1)/2} T, \end{aligned}$$

where

$$T = \begin{cases} d-1 & \text{if } m = n \text{ and } c \text{ is a } d\text{th power in } \mathbb{F}_q^*, \\ -1 & \text{if } m = n \text{ and } c \text{ is not a } d\text{th power in } \mathbb{F}_q^*, \\ 0 & \text{if } m < n. \end{cases}$$

Theorem 1.2. *Suppose that $2 \mid n$, $m = n/2$, $2d \nmid (n-2)$ and there is a positive integer l such that $d \mid (p^l + 1)$. Then*

$$N_q = q^{n-1} + (-1)^{n/2} q^{(n-2)/2}(q-1) + (-1)^{(n-2)/2}(q-1)^{n/2}.$$

2. Preliminary lemmas

Let ψ be a nontrivial multiplicative character on $\mathbb{F}_q$. We define sum $T(\psi)$ corresponding to character ψ as

$$T(\psi) = \frac{1}{q-1} \sum_{x_1,\ldots,x_n \in \mathbb{F}_q} \psi(x_1^2 + \cdots + x_m^2 + gx_{m+1}^2 + \cdots + gx_n^2)\bar{\psi}(x_1 \cdots x_n).$$

(we extend ψ to all of $\mathbb{F}_q$ by setting $\psi(0) = 0$). The Gauss sum corresponding to ψ is defined as

$$G(\psi) = \sum_{y \in \mathbb{F}_q^*} \psi(y) \exp(2\pi i \operatorname{Tr}(y)/p),$$

where $\operatorname{Tr}(y) = y + y^p + y^{p^2} + \cdots + y^{p^{s-1}}$ is the trace of y from $\mathbb{F}_q$ to $\mathbb{F}_p$.

In the following lemma we have an expression for N_q in terms of sums $T(\psi)$.

Lemma 2.1. *We have*

$$N_q = q^{n-1} + \frac{1}{2}\left(1+(-1)^n\right)(-1)^{m+\lfloor n(q-1)/4\rfloor} q^{(n-2)/2}(q-1)$$
$$+ (-1)^{m+1}\left[(-1)^{(q-1)/2}q - 1\right]^{n-m} \sum_{\substack{k=0 \\ 2\mid k}}^{2m-n} (-1)^{k(q-1)/4}\binom{2m-n}{k} q^{k/2}$$
$$+ \sum_{\substack{\psi^d=\varepsilon \\ \psi\neq\varepsilon}} \bar{\psi}(c)T(\psi),$$

where $\lfloor n(q-1)/4\rfloor$ *is the greatest integer less or equal to* $n(q-1)/4$ *and* $\sum_{\substack{\psi^d=\varepsilon \\ \psi\neq\varepsilon}}$ *means that the summation is taken over all nontrivial characters* ψ *on* $\mathbb{F}_q$ *of order dividing* d.

Proof. See [1, Lemma 1]. □

Let η denote the quadratic character on $\mathbb{F}_q$ ($\eta(x) = +1, -1, 0$ according x is a square, a non-square or zero in $\mathbb{F}_q$). In the next lemma we give the expression for sum $T(\psi)$ in terms of Gauss sums.

Lemma 2.2. *Let* ψ *be a character of order* δ *on* $\mathbb{F}_q$, *where* $\delta > 1$ *and* $\delta \mid d$. *Let* λ *be a character on* $\mathbb{F}_q$ *chosen so that* $\lambda^2 = \psi$ *and*

$$\operatorname{ord}\lambda = \begin{cases} \delta & \text{if } 2\nmid\delta, \\ 2\delta & \text{if } 2\mid\delta. \end{cases}$$

Then

$$T(\psi) = \frac{1}{2q}\lambda(g^{n-m})G(\psi)\left(G(\bar{\lambda})^2 - G(\bar{\lambda}\eta)^2\right)^{n-m}$$
$$\times\left[\left(G(\bar{\lambda}) + G(\bar{\lambda}\eta)\right)^{2m-n} + (-1)^{n+((n-2)/\delta)}\left(G(\bar{\lambda}) - G(\bar{\lambda}\eta)\right)^{2m-n}\right].$$

Proof. See [1, Lemma 2]. □

The following lemma determines explicitly the values of certain Gauss sums.

Lemma 2.3. *Let* ψ *be a multiplicative character of order* $\delta > 1$ *on* $\mathbb{F}_q$. *Suppose that there is a positive integer* l *such that* $\delta \mid (p^l+1)$ *and* $2l \mid s$. *Then*

$$G(\psi) = (-1)^{(s/2l)-1+(s/2l)\cdot((p^l+1)/\delta)}\sqrt{q}.$$

Proof. It is analogous to that of [3, Theorem 11.6.3]. □

Now we use Lemmas 2.2 and 2.3 to evaluate the sum $T(\psi)$ in a special case.

Lemma 2.4. *Let ψ be a character of order δ on $\mathbb{F}_q$, where $\delta > 1$ and $\delta \mid d$. Suppose that there is a positive integer l such that $2\delta \mid (p^l + 1)$ and $2l \mid s$. Then*

$$T(\psi) = \begin{cases} (-1)^{((s/2l)-1)(n-1)} 2^{n-1} q^{(n-1)/2} & \text{if } \; m = n, \\ 0 & \text{if } \; m < n. \end{cases}$$

Proof. Let λ be a character with the same conditions as in Lemma 2.2. If δ is odd then the order of $\bar{\lambda}$ is equal δ and the order of $\bar{\lambda}\eta$ is equal 2δ. Since $2\delta \mid (p^l + 1)$ and $2l \mid s$, by Lemma 2.3, it follows that

$$G(\bar{\lambda}) = (-1)^{(s/2l)-1} \sqrt{q} \tag{2.1}$$

and

$$G(\bar{\lambda}\eta) = (-1)^{(s/2l)-1+(s/2l)\cdot((p^l+1)/2\delta)} \sqrt{q}. \tag{2.2}$$

If δ is even then $\bar{\lambda}$ and $\bar{\lambda}\eta$ are the characters of order 2δ. Then similar reasoning yields

$$G(\bar{\lambda}) = G(\bar{\lambda}\eta) = (-1)^{(s/2l)-1+(s/2l)\cdot((p^l+1)/2\delta)} \sqrt{q}. \tag{2.3}$$

In any case $G(\bar{\lambda})^2 = G(\bar{\lambda}\eta)^2$. Therefore, by Lemma 2.2, $T(\psi) = 0$ for $m < n$.

Now suppose that $m = n$. Since $(p^l + 1)/\delta$ is even, it follows that

$$G(\psi) = (-1)^{(s/2l)-1} \sqrt{q}. \tag{2.4}$$

If δ is odd then $n + ((n-2)/\delta)$ is even, and from (2.1), (2.2), (2.4) and Lemma 2.2 we obtain

$$\begin{aligned} T(\psi) &= \frac{1}{2q} (-1)^{(s/2l)-1} \sqrt{q} \cdot (-1)^{((s/2l)-1)n} q^{n/2} \\ &\quad \times \left[\left(1 + (-1)^{(s/2l)\cdot((p^l+1)/2\delta)}\right)^n + \left(1 - (-1)^{(s/2l)\cdot((p^l+1)/2\delta)}\right)^n \right] \\ &= (-1)^{((s/2l)-1)(n-1)} 2^{n-1} q^{(n-1)/2}, \end{aligned}$$

and therefore lemma is established in this case.

If δ is even then n is even, and (2.3), (2.4) and Lemma 2.2 imply

$$\begin{aligned} T(\psi) &= \frac{1}{2q} (-1)^{(s/2l)-1} \sqrt{q} \cdot (-1)^{((s/2l)-1+(s/2l)\cdot((p^l+1)/2\delta))n} 2^n q^{n/2} \\ &= (-1)^{((s/2l)-1)(n-1)} 2^{n-1} q^{(n-1)/2}. \end{aligned}$$

This completes the proof of Lemma 2.4. $\square$

3. Proof of the theorems

Proof of Theorem 1.1. Since $2d \mid (p^l+1)$ and $2d \mid (q-1)$, it follows that $2l \mid s$ and $q \equiv 1 \pmod 8$. Appealing to Lemmas 2.1 and 2.4, we deduce that

$$
\begin{aligned}
N_q = q^{n-1} &+ \frac{1}{2}(1+(-1)^n)(-1)^m q^{(n-2)/2}(q-1) \\
&+ (-1)^{m+1}(q-1)^{n-m} \sum_{\substack{k=0 \\ 2\mid k}}^{2m-n} \binom{2m-n}{k} q^{k/2} \\
&+ (-1)^{((s/2l)-1)(n-1)} 2^{n-1} q^{(n-1)/2} T,
\end{aligned} \tag{3.1}
$$

where

$$
T = \begin{cases} \displaystyle\sum_{\substack{\psi^d=\varepsilon \\ \psi\neq\varepsilon}} \bar{\psi}(c) & \text{if } m=n, \\ 0 & \text{if } m<n. \end{cases}
$$

Thus, from (3.1) and the well-known relation

$$
\sum_{\substack{\psi^d=\varepsilon \\ \psi\neq\varepsilon}} \bar{\psi}(c) = \begin{cases} d-1 & \text{if } c \text{ is a } d\text{th power in } \mathbb{F}_q^*, \\ -1 & \text{if } c \text{ is not a } d\text{th power in } \mathbb{F}_q^*, \end{cases}
$$

Theorem 1.1 follows. □

Proof of Theorem 1.2. Since $d \mid (n-2)$, $2d \nmid (n-2)$ and $2 \mid n$, it follows that $2 \mid d$. Therefore $q \equiv 1 \pmod 4$ and, by Lemma 2.1,

$$
N_q = q^{n-1} + (-1)^{n/2} q^{(n-2)/2}(q-1) + (-1)^{(n-2)/2}(q-1)^{n/2} + \sum_{\substack{\psi^d=\varepsilon \\ \psi\neq\varepsilon}} \bar{\psi}(c) T(\psi).
$$

Let ψ be a character of order δ on $\mathbb{F}_q$, where $\delta > 1$ and $\delta \mid d$. If $2\delta \mid d$ then there is a positive integer l such that $2\delta \mid (p^l+1)$ and $2l \mid s$. Thus, by Lemma 2.4, $T(\psi) = 0$. If $2\delta \nmid d$ then d/δ and $(n-2)/d$ are odd. Therefore $(n-2)/\delta$ is odd and, by Lemma 2.2, $T(\psi) = 0$, as desired. □

References

[1] I. Baoulina, *On the Problem of Explicit Evaluation of the Number of Solutions of the Equation* $a_1x_1^2 + \cdots + a_nx_n^2 = bx_1 \cdots x_n$ *in a Finite Field.* In Current Trends in Number Theory, Edited by S. D. Adhikari, S. A. Katre and B. Ramakrishnan, Hindustan Book Agency, New Delhi, 2002, 27–37.

[2] A. Baragar, *The Markoff Equation and Equations of Hurwitz.* Ph. D. Thesis, Brown University, 1991.

[3] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi Sums.* Wiley-Interscience, New York, 1998.

[4] L. Carlitz, *Certain special equations in a finite field.* Monatsh. Math. **58** (1954), 5–12.

Ioulia Baoulina
The Institute of Mathematical Sciences
CIT Campus, Taramani
Chennai 600113, India
E-mail : jbaulina@mail.ru, baoulina@imsc.res.in