FINITE FIELDS AND THEIR APPLICATIONS **3,** 175–179 (1997)
ARTICLE NO. FF960173

NOTE

On Diagonal Equations over Finite Fields*

Sichuan University, Chengdu 610064, People's Republic of China

Communicated by Jacques Wolfmann

Received April 22, 1996; revised August 15, 1996

We get an explicit formula for the number of solutions of a diagonal equation over finite fields, under a certain natural restriction on the exponents.

Let $F = F_q$ be the finite field of q elements, where $q = p^f$, $f \geq 1$, p is a odd prime number. A diagonal equation over F is an equation of the form

$$a_1 x_1^{d_1} + a_2 x_2^{d_2} + \cdots + a_n x_n^{d_n} = c, \quad n \geq 2, a_j \in F^*, j = 1, \ldots, n, c \in F. \quad (1)$$

Finding the number of solutions $(x_1, \ldots, x_n) \in F^{(n)}$ of (1) in the general case is a very difficult problem. In 1994, Wolfmann [1] gives new results on the number of solutions of such equations from cyclic codes.

In is well known [2] that finding the number of solutions of (1) can be obtained by the number of solutions of the equations of the form

$$c_1 x_1^{d_1} + c_2 x_2^{d_2} + \cdots + c_n x_n^{d_n} = 0, \quad n \geq 2, c_j \in F^*, j = 1, \ldots, n, \quad (2)$$

where $d_i > 1$ and d_i divides $q - 1$ for all i.

Let $N(d_1, \ldots, d_n; c_1, \ldots, c_n)$ be the number of solutions of (2). Sun Qi and Yuan Ping-Zhi [3] proved that

* This project supported by National Natural Science Foundation of China.

1071-5797/97 $25.00

$$N(d_1, \ldots, d_n; c_1, \ldots, c_n) = N(u_1, \ldots, u_n; c_1, \ldots, c_n),$$

where $u_j = (d_j, d_1 \cdot \cdots \cdot d_n/d_j)$, $j = 1, \ldots, n$.

Recently, Granville, Shuguang Li, and Sun Qi [4] proved that

$$N(d_1, \ldots, d_n; c_1, \ldots, c_n) = N(w_1, \ldots, w_n; c_1, \ldots, c_n), \tag{3}$$

where $w_j = (d_j, \operatorname{lcm}[d_i: i \neq j])$, $j = 1, \ldots, n$.

In this note, we obtain the following theorem.

THEOREM. *Let* $2 \mid n$, $n \geq 2$. Let $d_j = 2m_j$, $j = 1, \ldots, n-2$; $d_{n-1} = km_{n-1}$; $d_n = k^l m_n$ $(k \geq 3, l \geq 1)$; $(2k, m_j) = 1$, $j = 1, \ldots, n$; *and* $(m_i, m_j) = 1$, $1 \leq i < j \leq n$. *Then*

$$N(d_1, \ldots, d_n; \overbrace{1, \ldots, 1}^{n}) =$$

$$\begin{cases} q^{n-1} + (k-1)(q-1)(-1)^{((q-1)/2)(n-2)/2} q^{(n-2)/2}, & \text{if } 2 \left| \dfrac{q-1}{k}, \right. \\ q^{n-1} - (q-1)(-1)^{((q-1)/2)(n-2)/2} q^{(n-2)/2}, & \text{if } 2 \nmid \dfrac{q-1}{k}. \end{cases}$$

Proof of theorem. Let g be a fixed primitive element of F and $a = g^h$, where $a \in F^*$, $0 \leq h < q-1$. We define that $\operatorname{ind}_g a = h$, or simply $\operatorname{ind} a = h$.

It is well known that $N(d_1, \ldots, d_n; c_1, \ldots, c_n)$ is given by the formula (see [3])

$$N(d_1, \ldots, d_n; c_1, \ldots, c_n) = q^{n-1} + \sum_{\substack{y_1/d_1 + \cdots + y_n/d_n \equiv 0 (\mathrm{mod}\, 1) \\ 1 \leq y_j \leq d_j - 1,\, j = 1, \ldots, n}} \chi_1^{y_1}(c_1^{-1}) \cdot \cdots \chi_n^{y_n}(c_n^{-1}) J_0(\chi_1^{y_1}, \ldots, \chi_n^{y_n}), \tag{4}$$

where $\chi_j(a) = e^{2\pi i \operatorname{ind} a d/d_j}$ is a character of order d_j on F, $a \in F^*$, $j = 1, \ldots, n$. $J_0(\chi_1, \ldots, \chi_n)$ is the Jacobi sum over F, that is,

$$J_0(\chi_1, \ldots, \chi_n) = \sum_{\substack{a_1 + \cdots + a_n = 0 \\ a_i \in F}} \chi_1(a_1) \cdot \cdots \chi_n(a_n).$$

Let $d_j = 2m_j$, $j = 1, \ldots, n-2$; $d_{n-1} = km_{n-1}$; $d_n = k^l m_n$ $(l \geq 1, k \geq 3)$; $(2k, m_j) = 1$, $j = 1, \ldots, n$; $(m_i, m_j) = 1$, $1 \leq i < j \leq n$. Let

$$\varepsilon(k) = \begin{cases} 0, & \text{if } 2 \mid k, \\ 1, & \text{if } 2 \nmid k. \end{cases}$$

Then we have

$$w_j = (d_j, \operatorname{lcm}[d_i : i \neq j]) = (2m_j, 2^{\varepsilon(k)} k^l m_1 \cdot \cdots \cdot m_n/m_j) = 2, \quad j = 1, \ldots, n-2,$$
$$w_{n-1} = (d_{n-1}, \operatorname{lcm}[d_i : i \neq n-1]) = (km_{n-1}, 2^{\varepsilon(k)} k^l m_1 \cdot \cdots \cdot m_n/m_{n-1}) = k,$$
$$w_n = (d_n, \operatorname{lcm}[d_i : i \neq n]) = (k^l m_n, 2^{\varepsilon(k)} k m_1 \cdot \cdots \cdot m_{n-1}) = k.$$

It follows from (3) that

$$N(d_1, \ldots, d_n; \overbrace{1, \ldots, 1}^{n}) = N(\overbrace{2, \ldots, 2}^{n-2}, k, k; \overbrace{1, \ldots, 1}^{n}). \tag{5}$$

Let $I(d_1, \ldots, d_n)$ denote the number of solutions $(y_1, \ldots, y_n) \in Z^{(n)}$ of the equation

$$y_1/d_1 + \cdots + y_n/d_n \equiv 0 \pmod 1, \quad 1 \leq y_j \leq d_j - 1, j = 1, \ldots, n.$$

Obviously, if $2 \mid n$, then $I(\overbrace{2, \ldots, 2}^{n-2}, k, k) = k - 1$, that is, if $2 \mid n$, then the equation

$$\frac{y_1}{2} + \cdots + \frac{y_{n-2}}{2} + \frac{y_{n-1}}{k} + \frac{y_n}{k} \equiv 0 \pmod 1; \quad y_j = 1; j = 1, \ldots, n-2,$$

$1 \leq y_j \leq k - 1, j = n - 1, n$, has $k - 1$ solutions:

$$(\overbrace{1, \ldots, 1}^{n-2}, j, k - j), j = 1, \ldots, k - 1, \tag{6}$$

So, by (4), (5), and (6), we have

$$N(d_1, \ldots, d_n; \overbrace{1, \ldots, 1}^{n}) = N(\overbrace{2, \ldots, 2}^{n-2}, k, k; \overbrace{1, \ldots, 1}^{n})$$
$$= q^{n-1} + \sum_{j=1}^{k-1} J_0(\overbrace{\eta, \ldots, \eta}^{n-2}, \sigma^j, \sigma^{k-j}),$$

where $\sigma(a) = e^{2\pi i inda/k}$ is a character of order k on F, $\eta(a) = e^{\pi i inda}$ denotes the quadratic character of F, $a \in F^*$.

It is well known that (see Proposition 8.5.1 (c) and Theorem 3 of Chapter 8 of [5])

$$J_0(\overbrace{\eta, \ldots, \eta}^{n-2}, \sigma^j, \sigma^{k-j}) = \sigma^{k-j}(-1)(q-1)J(\overbrace{\eta, , \ldots, \eta}^{n-2}, \sigma^j),$$

$$J(\overbrace{\eta, \ldots, \eta}^{n-2}, \sigma^j) = \sum_{\substack{a_1+\cdots+a_{n-1}=1 \\ a_i \in F}} \eta(a_1) \cdot \cdots \cdot \eta(a_{n-2})\sigma^j(a_{n-1}) \tag{8}$$

$$= \frac{G^{n-2}(\eta, \psi)G(\sigma^j, \psi)}{G(\eta^{n-2}\sigma^j, \psi)},$$

where $G(\eta, \psi) = \sum_{a \in F^*} \eta(a)\psi(a)$, $G(\sigma^j, \psi) = \sum_{a \in F^*} \sigma^j(a)\psi(a)$, $\psi(c) = e^{2\pi i T_r(c)/p}$. Since $2 \mid n$, thus $G^{n-2}(\eta, \psi) = (\eta(-1)q)^{(n-2)/2}$ and $G(\eta^{n-2}\sigma^j, \psi) = G(\sigma^j, \psi)$. So, (8) can be written as

$$J_0(\overbrace{\eta, \ldots, \eta}^{n-2}, \sigma^j, \sigma^{k-j}) = \sigma^{k-j}(-1)(q-1)(\eta(-1)q)^{(n-2)/2} \tag{9}$$

$$= \sigma^{k-j}(-1)(q-1)(-1)^{(q-1)/2(n-2)/2}q^{(n-2)/2},$$

and (7) can be written as

$$N(d_1, \ldots, d_n, \overbrace{1, \ldots, 1}^{n}) = q^{n-1} + (q-1)(-1)^{(q-1)/2(n-2)/2}$$

$$q^{(n-2)/2} \sum_{j=1}^{k-1} \sigma^{k-j}(-1).$$

Since $k \mid q-1$ and $\sigma(-1) = e^{\pi i(q-1)/k}$, thus

$$\sum_{j=1}^{k-1} \sigma^{k-j}(-1) = \begin{cases} k-1, & \text{if } 2 \left| \dfrac{q-1}{k}, \right. \\ -1, & \text{if } 2 \left\backslash \dfrac{q-1}{k}. \right. \end{cases}$$

This completes the proof.

Remark. By (3), (4), (6), and (9), we have

$$N(d_1, \ldots, d_n; c_1, \ldots, c_n) = q^{n-1} + \eta(c_1^{-1} \cdot \cdots \cdot c_{n-2}^{-1})(-1)^{(q-1)/2(n-2)/2}$$

$$(q-1)q^{(n-2)/2} \sum_{j=1}^{k} \sigma^j(c_{n-1}^{-1})\sigma^{k-j}(-c_n^{-1}).$$

References

1. J. Wolfmann, New results on diagonal equations over finite fields from cyclic codes, Contemporary Mathematics, Vol. 168, pp. 387–395, Amer. Math. Soc., Providence, RI, 1994.
2. D. Wan, Zeros of diagonal equations over finite fields, *Proc. Amer. Math. Soc.* **103** (1988), 1049–1052.
3. Sun Qi and Ping-Zhi Yuan, On the number of solutions of diagonal equations over a finite field, *Finite Fields Appl.* **1** (1996), 35–41.
4. A. Granville, Shuguang Li, and Sun Qi, On the number of solutions of the equations $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$ and of diagonal equations in finite fields, *J. Sichuan Univ. Natural Sci.* **3** (1995), 243–248.
5. K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," Graduate texts in Mathematics, Vol. 84, Springer-Verlag, New York, 1982.