ZEROES OF DIAGONAL EQUATIONS OVER FINITE FIELDS

DAQING WAN

(Communicated by Larry J. Goldstein)

ABSTRACT. Let \( N \) be the number of solutions \((x_1, \ldots, x_n)\) of the equation
\[
  c_1 x_1^{d_1} + c_2 x_2^{d_2} + \cdots + c_n x_n^{d_n} = c
\]
over the finite field \( F_q \), where \( d_i \mid (q - 1) \), \( c_i \in F_q^* \) \((i = 1, \ldots, n)\), and \( c \in F_q \). If
\[
  \frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_n} > b \geq 1
\]
for some positive integer \( b \), we prove that \( q^b \mid N \). This result is an improvement of the theorem that \( p \mid N \) obtained by B. Morlaye [7] and also by J. R. Joly [3].

1. Introduction. Let \( F_q \) be a finite field with \( q = p^f \) elements, where \( p \) is the characteristic of the field. Some attention has been given to the divisibility properties of the number \( N \) of solutions of an equation over \( F_q \). The basic idea of this research originated from Lebesgue [5], who first noted that
\[
  N(f(x) = 0) \equiv \sum_{c \in F_q^*} (1 - f(c)^{q-1}) \quad (\text{mod } p)
\]
where \( f(x) \in F_q[x] \). After that, it was Warning [11] who first arrived at the conclusion that \( p \mid N(f(x_1, \ldots, x_n) = 0) \) for \( f(x_1, \ldots, x_n) \in F_q[x_1, \ldots, x_n] \) with \( \deg(f) < n \), and generalized this result to a system of polynomials. In 1962, J. Ax [1] found a major improvement of Warning's theorem which, in a sense, is best possible. He proved that if \( b \) is the largest integer such that \( b < n/d \), then \( q^b \mid N(f(x_1, \ldots, x_n) = 0) \) for any polynomial \( f(x_1, \ldots, x_n) \in F_q[x_1, \ldots, x_n] \) with \( \deg(f) = d \). In 1971, Ax's theorem was generalized to systems of equations by N. M. Katz [4]. This generalization, in a sense, is also best possible. A more elementary proof of Katz's theorem can be found in [10]. Therefore, the general study of the divisibility properties of the number \( N \) by powers of \( p \) may have come to an end.

For special kinds of equations, however, further results about divisibility of \( N \) by \( p \) can still be obtained by using arithmetic properties of multinomial coefficients. One such result is a theorem of Morlaye [7] and Joly [3] (see also [6, pp. 297–298]), which shows that \( p \mid N \), the number of solutions to the diagonal equation (1) over \( F_q \), provided that \( 1/d_1 + 1/d_2 + \cdots + 1/d_n > 1 \).

In this paper, using some ideas of Ax [1], we shall improve the theorem of Morlaye and Joly, and obtain a theorem with the same quality as Ax's theorem. That is,
we have

**THEOREM 1.** Let \( n \) be the number of solutions of the diagonal equation (1) over \( F_q \). If there is a positive integer \( b \) such that

\[
\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_n} > b \geq 1,
\]

then

\[
N \equiv 0 \pmod{q^b}.
\]

Note that if \( d_1 = d_2 = \cdots = d_n = d \), a divisor of \((q-1)\), then Theorem 1 reduces to a special case of Ax's theorem.

**2. An auxiliary lemma.** For convenience, first we introduce a lemma which is important in the proof of Theorem 1.

**LEMMA 2.** Let \( d_i \mid (q - 1) \) (\( i = 1, \ldots, n \)), \( q = p^f \), and \( \sum 1/d_i > b \), where \( b \) is a nonnegative integer. For any \( l_i \) (\( 1 \leq l_i \leq d_i - 1 \)), \( (i = 1, \ldots, n) \) with \( \sum l_i/d_i \equiv 0 \pmod{1} \), suppose

\[
\frac{q-1}{d_i} l_i = a_{i0} + a_{i1} p + \cdots + a_{i(f-1)} p^{f-1}, \quad 0 \leq a_{ij} < p,
\]

and let

\[
S = \sum_{i=1}^{n} \sum_{j=0}^{f-1} a_{ij}.
\]

Then \( S \geq f(b+1)(p-1) \).

**PROOF.** For any integers \( j \) and \( r \) with \( j \equiv r \pmod{f} \) and \( 0 \leq r \leq f - 1 \), we define \( a_{ij} = a_{ir} \). Since

\[
\frac{q-1}{d_i} l_i = \sum_{j=0}^{f-1} a_{ij} p^j,
\]

it follows that, letting \( (x)_d \) denote the smallest nonnegative residue of \( x \mod d \), we have

\[
\frac{q-1}{d_i} (l_i p^k)_{d_i} = \left( \frac{q-1}{d_i} l_i p^k \right)_{q-1} = \sum_{j=0}^{f-1} a_{i(j-k)} p^j.
\]

Thus

\[
\sum_{t=1}^{n} \sum_{k=0}^{f-1} \frac{q-1}{d_i} (l_i p^k)_{d_i} = \left( \sum_{i=1}^{n} \sum_{k=0}^{f-1} a_{ik} \right) \frac{q-1}{p-1}.
\]

On the other hand,

\[
\sum_{t=1}^{n} \frac{(l_i p^k)_{d_i}}{d_i} \equiv \sum_{t=1}^{n} l_i p^k \equiv p^k \sum_{t=1}^{n} l_i \equiv 0 \pmod{1},
\]

and

\[
\sum_{t=1}^{n} \frac{(l_i p^k)_{d_i}}{d_i} \geq \sum_{t=1}^{n} \frac{1}{d_i} > b.
\]
Therefore, \( \sum (l_i p^k)_{d_i} / d_i \) is integral and

\[
\sum_{i=1}^{n} \frac{(l_i p^k)_{d_i}}{d_i} \geq b + 1.
\]

Now, (3) gives

\[
S \geq (p - 1) \sum_{k=0}^{f-1} \sum_{i=1}^{n} \frac{(l_i p^k)_{d_i}}{d_i} \geq (p - 1) f(b + 1).
\]

Lemma 2 is proved.

**3. Proof of Theorem 1.** If \( c \neq 0 \), we have the identity

\[
N(c_1 x_1^{d_1} + \cdots + c_n x_n^{d_n} = c)
= \frac{1}{q - 1} [N(c_1 x_1^{d_1} + \cdots + c_n x_n^{d_n} - c x_{n+1}^{q-1} = 0) - N(c_1 x_1^{d_1} + \cdots + c_N x_n^{d_n} = 0)].
\]

Since \( 1/d_1 + \cdots + 1/d_n + 1/(q - 1) > 1/d_1 + \cdots + 1/d_n \), it is sufficient to prove Theorem 1 for \( c = 0 \). In the following, we let \( N \) denote the number of solutions of the equation

\[
c_1 x_1^{d_1} + c_2 x_2^{d_2} + \cdots + c_n x_n^{d_n} = 0
\]

over \( F_q \), where \( c_i \in F_q^* \).

It is well known that \( N \) can be evaluated by means of Gauss sums. Take a multiplicative character \( \chi \) of \( F_q \) of order \( (q - 1)/d_i \) and put \( x_i = x_1^{(q - 1)/d_i} \). Then \( x_i \) is a multiplicative character of \( F_q \) of order \( d_i \) \((i = 1, \ldots, n)\). From [6, pp. 293–294], we see that

\[
(6) \quad N = q^{n-1} + \frac{q - 1}{q} \sum_{(j_1, \ldots, j_n) \in T} \chi_1(c_1)^{-j_1} \cdots \chi_n(c_n)^{-j_n} G(\chi_1^{j_1}) \cdots G(\chi_n^{j_n}),
\]

where \( T \) is the set of all \( n \)-tuples \((j_1, \ldots, j_n) \in Z^n\) such that \( 1 \leq j_i \leq d_i - 1 \) for \( 1 \leq i \leq n \) and \( \sum j_i / d_i \equiv 0 \) (mod 1), and the Gauss sums are defined by

\[
G(\chi^j) = \sum_{c \in F_q} \chi^j(c) e^{2\pi i c / q}.
\]

(6) can be written as

\[
(7) \quad N = q^{n-1} + \frac{q - 1}{q} \sum_{(j_1, \ldots, j_n) \in T} \chi(c_1)^{-((q - 1)/d_1)j_1} \cdots \chi(c_n)^{-((q - 1)/d_n)j_n} G(\chi^{((q - 1)/d_1)j_1}) \cdots G(\chi^{((q - 1)/d_n)j_n}).
\]

If \( 0 \leq a \leq q - 1 \), write \( a = \sum_{i=0}^{f-1} a_i p^i \) with \( 0 \leq a_i < p \) and define \( \sigma(a) = \sum_{i=0}^{f-1} a_i \).

Suppose \( \eta_p = 1 - e^{2\pi i / p} \); then Stickelberger’s congruence [2, p. 212] gives

\[
G(\chi^{((q - 1)/d_i)j_i}) \equiv 0 \pmod{\eta_p^{\Delta_1}},
\]

where \( \Delta_1 = \sigma(((q - 1)/d_i)j_i) \).

Since \( \eta_p^{p-1} = p \varepsilon \), where \( \varepsilon \) is a unit of \( Q(e^{2\pi i / p}) \), from (7) we deduce that

\[
(8) \quad N - q^{n-1} \equiv 0 \pmod{\eta_p^{\Delta_1}},
\]
where
\[ \Delta = \min_{(j_1, \ldots, j_n) \in T} \left[ \sum_{i=1}^{n} \sigma \left( \frac{q-1}{d_i} j_i \right) - f(p-1) \right]. \]

According to Lemma 2,
\[ \sum_{i=1}^{n} \sigma \left( \frac{q-1}{d_i} j_i \right) = S \geq (b + 1) f(p-1). \]

This and (8) together give
\[ N - q^{n-1} \equiv 0 \pmod{\eta_p^b f(p-1)}. \]

That is,
\[ N - q^{n-1} \equiv 0 \pmod{b}. \]

Clearly, \( b \leq n - 1 \), and so \( N \equiv 0 \pmod{b} \). The proof is complete.

Observing our proof of Lemma 2 and Theorem 1, it is not hard to prove the following better result for equation (1) with \( c = 0 \). That is,

**Theorem 3.** Let \( b^*(d_1, \ldots, d_n) \) be the least positive integer represented by \( \sum_{i=1}^{n} l_i/d_i \) \((1 \leq l_i \leq d_i - 1)\) if there is such an integer; otherwise, let \( b^*(d_1, \ldots, d_n) = n - 1 \). Then for equation (1) with \( c = 0 \), we have \( N \equiv 0 \pmod{b^*(p-1)} \).

The fact that \( b^* - 1 \geq b \) can be easily proved. Thus, Theorem 3 is in general stronger than Theorem 1.

The above discussion suggests that it would be of interest to determine \( b^*(d_1, \ldots, d_n) \). In an earlier paper, we gave a necessary and sufficient condition for \( b^*(d_1, \ldots, d_n) = n - 1 \) (the maximum value of \( b^* \)); see [9].

The author is grateful to Professor Koblitz, who suggested some comments and corrections.

REFERENCES

5. V. A. Lebesgue, Recherches sur les nombres, J. Math. Pures Appl. **1** (1832), 11-111; **2** (1832), 253-292; **3** (1832), 113-144.
9. Sun Qi and Daqing Wan, On the equation \( \sum_{i=0}^{n} 1/d_i \equiv 0 \pmod{1} \) and its application, Proc. Amer. Math. Soc. **100** (1987), 220-224.

Department of Mathematics, GN-50, University of Washington, Seattle, Washington 98195