# ZEROS OF DIAGONAL EQUATIONS OVER FINITE FIELDS <br> (Communicated by Larry J. Goldstein) 

Abstract. Let $N$ be the number of solutions $\left(x_{1}, \ldots, x_{n}\right)$ of the equation

$$
\begin{equation*}
c_{1} x_{1}^{d_{1}}+c_{2} x_{2}^{d_{2}}+\cdots+c_{n} x_{n}^{d_{n}}=c \tag{1}
\end{equation*}
$$

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

$$
N(f(x)=0) \equiv \sum_{c \in F_{q}}\left(1-f(c)^{q-1}\right) \quad(\bmod p)
$$

where $f(x) \in F_{q}[x]$. After that, it was Warning [11] who first arrived at the conclusion that $p \mid N\left(f\left(x_{1}, \ldots, x_{n}\right)=0\right)$ for $f\left(x_{1}, \ldots, x_{n}\right) \in F_{q}\left[x_{1}, \ldots, x_{n}\right]$ with $\operatorname{deg}(f)<n$, 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 $q^{b} \mid N\left(f\left(x_{1}, \ldots, x_{n}\right)=0\right)$ for any polynomial $f\left(x_{1}, \ldots, x_{n}\right) \in F_{q}\left[x_{1}, \ldots, x_{n}\right]$ with $\operatorname{deg}(f)=d$. 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,

[^0]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
$$
N \equiv 0 \quad\left(\bmod q^{b}\right)
$$

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 $l_{i}\left(1 \leq l_{i} \leq d_{i}-1\right),(i=1, \ldots, n)$ with $\sum l_{i} / d_{i} \equiv 0(\bmod 1)$, suppose

$$
\frac{q-1}{d_{i}} l_{i}=a_{i 0}+a_{i 1} p+\cdots+a_{i(f-1)} p^{f-1}, \quad 0 \leq a_{i j}<p
$$

and let

$$
\begin{equation*}
S=\sum_{i=1}^{n} \sum_{j=0}^{f-1} a_{i j} \tag{2}
\end{equation*}
$$

Then $S \geq f(b+1)(p-1)$.
Proof. For any integers $j$ and $r$ with $j \equiv r(\bmod f)$ and $0 \leq r \leq f-1$, we define $a_{i j}=a_{i r}$. Since

$$
\frac{q-1}{d_{i}} l_{i}=\sum_{j=0}^{f-1} a_{i j} p^{j}
$$

it follows that, letting $\langle x\rangle_{d}$ denote the smallest nonnegative residue of $x \bmod d$, we have

$$
\frac{q-1}{d_{i}}\left\langle l_{i} p^{k}\right\rangle_{d_{i}}=\left\langle\frac{q-1}{d_{i}} l_{i} p^{k}\right\rangle_{q-1}=\sum_{j=0}^{f-1} a_{i(j-k)} p^{j}
$$

Thus

$$
\begin{equation*}
\sum_{i=1}^{n} \sum_{k=0}^{f-1} \frac{q-1}{d_{i}}\left\langle l_{i} p^{k}\right\rangle_{d_{i}}=\left(\sum_{i=1}^{n} \sum_{k=0}^{f-1} a_{i k}\right) \frac{q-1}{p-1} \tag{3}
\end{equation*}
$$

On the other hand,

$$
\begin{equation*}
\sum_{i=1}^{n} \frac{\left\langle l_{i} p^{k}\right\rangle_{d_{i}}}{d_{i}} \equiv \sum_{i=1}^{n} \frac{l_{i} p^{k}}{d_{i}} \equiv p^{k} \sum_{i=1}^{n} \frac{l_{i}}{d_{i}} \equiv 0 \quad(\bmod 1) \tag{4}
\end{equation*}
$$

and

$$
\begin{equation*}
\sum_{i=1}^{n} \frac{\left\langle l_{i} p^{k}\right\rangle_{d_{i}}}{d_{i}} \geq \sum_{i=1}^{n} \frac{1}{d_{i}}>b \tag{5}
\end{equation*}
$$

Therefore, $\sum\left\langle l_{i} p^{k}\right\rangle_{d_{i}} / d_{i}$ is integral and

$$
\sum_{i=1}^{n} \frac{\left\langle l_{i} p^{k}\right\rangle_{d_{i}}}{d_{i}} \geq b+1
$$

Now, (3) gives

$$
S \geq(p-1) \sum_{k=0}^{f-1} \sum_{i=1}^{n} \frac{\left\langle l_{i} p^{k}\right\rangle_{d_{i}}}{d_{i}} \geq(p-1) f(b+1)
$$

Lemma 2 is proved.
3. Proof of Theorem 1. If $c \neq 0$, we have the identity

$$
\begin{aligned}
& N\left(c_{1} x_{1}^{d_{1}}+\cdots+c_{n} x_{n}^{d_{n}}=c\right) \\
& \quad=\frac{1}{q-1}\left[N\left(c_{1} x_{1}^{d_{+}}+\cdots+c_{n} x_{n}^{d_{n}}-c x_{n+1}^{q-1}=0\right)-N\left(c_{1} x_{1}^{d_{1}}+\cdots+c_{N} x_{n}^{d_{n}}=0\right)\right]
\end{aligned}
$$

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 $(q-1)$ and put $\chi_{i}=\chi^{(q-1) / d_{i}}$. Then $\chi_{i}$ is a multiplicative character of $F_{q}$ of order $d_{i}(i=1, \ldots, n)$. From [6, pp. 293-294], we see that

$$
\begin{equation*}
N=q^{n-1}+\frac{q-1}{q} \sum_{\left(j_{1}, \ldots, j_{n}\right) \in T} \chi_{1}\left(c_{1}\right)^{-j_{1}} \cdots \chi_{n}\left(c_{n}\right)^{-j_{n}} G\left(\chi_{1}^{j_{1}}\right) \cdots G\left(\chi_{n}^{j_{n}}\right) \tag{6}
\end{equation*}
$$

where $T$ is the set of all $n$-tuples $\left(j_{1}, \ldots, j_{n}\right) \in Z^{n}$ such that $1 \leq j_{i} \leq d_{i}-1$ for $1 \leq i \leq n$ and $\sum j_{i} / d_{i} \equiv 0(\bmod 1)$, and the Gauss sums are defined by

$$
G\left(\chi^{j}\right)=\sum_{c \in F_{q}} \chi^{j}(c) e^{\operatorname{tr}_{F_{q} / F_{p}}(c)(2 \pi i / p)}
$$

(6) can be written as
(7) $N=q^{n-1}+\frac{q-1}{q} \sum_{\left(j_{1}, \ldots, j_{n}\right) \in T} \chi\left(c_{1}\right)^{-\left((q-1) / d_{1}\right) j_{1}}$

$$
\ldots \chi\left(c_{n}\right)^{-\left((q-1) / d_{n}\right) j_{n}} G\left(\chi^{\left((q-1) / d_{1}\right) j_{1}}\right) \cdots G\left(\chi^{\left((q-1) / d_{n}\right) j_{n}}\right)
$$

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

$$
G\left(\chi^{\left((q-1) / d_{i}\right) j_{i}}\right) \equiv 0 \quad\left(\bmod \eta_{p}^{\Delta_{1}}\right)
$$

where $\Delta_{1}=\sigma\left(\left((q-1) / d_{i}\right) j_{i}\right)$.
Since $\eta_{p}^{p-1}=p \varepsilon$, where $\varepsilon$ is a unit of $Q\left(e^{2 \pi i / p}\right)$, from (7) we deduce that

$$
\begin{equation*}
N-q^{n-1} \equiv 0 \quad\left(\bmod \eta_{p}^{\Delta}\right) \tag{8}
\end{equation*}
$$

where

$$
\Delta=\min _{\left(j_{1}, \ldots, j_{n}\right) \in T}\left[\sum_{i=1}^{n} \sigma\left(\frac{q-1}{d_{i}} j_{i}\right)-f(p-1)\right] .
$$

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

$$
N-q^{n-1} \equiv 0 \quad\left(\bmod \eta_{p}^{b f(p-1)}\right)
$$

That is,

$$
N-q^{n-1} \equiv 0 \quad\left(\bmod q^{b}\right) .
$$

Clearly, $b \leq n-1$, and so $N \equiv 0\left(\bmod q^{b}\right)$. 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 $b^{*}\left(d_{1}, \ldots, d_{n}\right)$ be the least positive integer represented by $\sum_{i=0}^{n} l_{i} / d_{i}\left(1 \leq l_{i} \leq d_{i}-1\right)$ if there is such an integer; otherwise, let $b^{*}\left(d_{1}, \ldots, d_{n}\right)$ $=n-1$. Then for equation (1) with $c=0$, we have $N \equiv 0\left(\bmod q^{b^{*}-1}\right)$.

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 $b^{*}\left(d_{1}, \ldots, d_{n}\right)$. In an earlier paper, we gave a necessary and sufficient condition for $b^{*}\left(d_{1}, \ldots, d_{n}\right)=n-1$ (the maximum value of $b^{*}$ ); see $[9]$.

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

## References

1. J. Ax, Zeros of polynomials over finite fields, Amer. J. Math. 86 (1964), 255-261.
2. K. Ireland and M. Rosen, A classical introduction to modern number theory, Graduate Texts in Math., vol. 84, Springer-Verlag, 1982.
3. J. R. Joly, Équations et variétés algébriques sur un corps fini, Enseign. Math. (2) 19 (1973), 1-117.
4. N. M. Katz, On a theorem of $A x$, Amer. J. Math. 93 (1971), 485-499.
5. V. A. Lebesgue, Recherches sur les nombres, J. Math. Pures Appl. 1 (1832), 11-111; 2 (1832), 253-292; 3 (1832), 113-144.
6. R. Lidl and H. Niederreiter, Finite fields, Addison-Wesley, 1983.
7. B. Morlaye, Équations diagonales non homogènes sur un corps fini, C. R. Acad. Sci. Paris Ser. A 272 (1971), 1545-1548.
8. W. M. Schmidt, Equations over finite fields, Lecture Notes in Math., vol. 536, Springer-Verlag, 1976.
9. Sun Qi and Daqing Wan, On the equation $\sum_{i=0}^{n} 1 / d_{i} \equiv 0(\bmod 1)$ and its application, Proc. Amer. Math. Soc. 100 (1987), 220-224.
10. Daqing Wan, An elementary proof to a theorem of Katz, Amer. J. Math. (to appear).
11. E. Warning, Bermerkung zur Vorstehenden Arbeit von Herr Chevalley, Abh. Math. Sem. Univ. Hamburg, 11 (1936), 76-83.

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


[^0]:    Received by the editors December 16, 1986 and, in revised form, July 15, 1987.
    1980 Mathematics Subject Classification (1985 Revision). Primary 11D79, 11D72; Secondary 11 T 41.

