An Elementary Proof of a Partial Improvement to the Ax-Katz Theorem

O. Moreno¹* and C.J. Moreno²**

¹ University of Puerto Rico Rio Piedras, PR 00931 USA
   Email: o.morenou@uprenet.bitnet,
   moreno@sun386-gauss.uprr.pr
² Baruch, CUNY Box 545 N. Salem, NY 10560 USA
   Email: carlos@kronecker.baruch.cuny.edu

Abstract. Moreno and Moreno have recently given a result that in many cases improves upon the Ax-Katz theorem. We will presently give an elementary and self contained proof of this and also give a corresponding improvement upon a result of Adolphson and Sperber.

1 Introduction.

In connection with his work on quasi-algebraically closed fields, Artin was led to make the following conjecture: If $F = F(x_1, \ldots, x_n)$ is a homogeneous polynomial of total degree $d$ over $k$, a finite field having $q = p^f$ elements, and $n > d$, then $F$ has a nontrivial zero (It seems that Dickson had also made the same conjecture a number of years earlier [2]). C. Chevalley proved this in [4] and even showed the hypothesis of homogeneity could be replaced by the weaker assumption of no constant term. E. Warning in [14], using a lemma of Chevalley, showed that even without this last assumption the characteristic $p$ of $k$ divides $N(F)$, the number of zeros of $F$ (counting the trivial zero if $F$ has no constant term).

By using an idea of B. Dwork [5], J. Ax [3] greatly improved the theorem of Warning. He proved that if $b$ is the least nonnegative integer such that $b > (n-d)/d$, then $q^b$ divides $N(F)$. As a corollary, Ax obtained the following consequence for a system of polynomials: Let $F_i(x_1, \ldots, x_n)$ $(i = 1, \ldots, r)$ be polynomials over $k$ of degree $d_i$, and $\lambda$ be the least nonnegative integer which is

$$\frac{n - \sum_{i=1}^{r} d_i}{\sum_{i=1}^{r} d_i} \geq \lambda.$$ 

Then $q^\lambda$ divides $N(F_1 = 0, \ldots, F_r = 0)$. This corollary, however, could be improved. In 1971, N. M. Katz [6] proved:

**Theorem 0.** Let $F_1, \ldots, F_r$ be polynomials in $n$ variables with coefficients in $k$, a finite field with $q = p^f$ elements. Let $\mu$ be:

$$\mu = \left[ \frac{n - \sum_{i=1}^{r} \deg(F_i)}{\max_{1 \leq i \leq r} \{\deg(F_i)\}} \right],$$

* Work partially supported by NSF grants RII-9014056, component IV of the EPSCoR of Puerto Rico Grant and the ARO grant for Cornell MSI.
** And grants DMS-8711566 and DMS-8712742 from the National Science Foundation.
where \([x]\) denotes the least integer which is \(\geq x\). Then \(q^\mu\) divides \(N(F_1 = 0, \ldots, F_r = 0)\).

Please note that in the Ax-Katz result, the divisibility depends on the degree of the equations involved. In [11] Moreno and Moreno gave an improvement to the Ax-Katz result (theorem 0-1 below) which in many cases gives an improvement over theorem 0 above, and in those cases the divisibility depends in a fundamental way on the maximal \(p\)-weight (as defined below) of the degrees of the terms of the equations. Theorem 1, which is the main theorem in [11] invokes theorem 0 above and we present here a self contained proof of said theorem 1. Our method is furthermore quite elementary, and uses among other things only a simple version of Stickelberger’s theorem which is readily established.

**Definition 1.** The \(p\)-weight degree of a monomial \(x^d = x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}\) is \(w_p(x^d) = \sigma_p(d_1) + \sigma_p(d_2) + \cdots + \sigma_p(d_n)\), where \(\sigma_p(d)\) denotes the \(p\)-weight of the integer \(d\), i.e., if \(d = a_0 + a_1 p + \cdots + a_t p^t\), \(0 \leq a_i < p\), then \(\sigma_p(d) = a_0 + a_1 + \cdots + a_t\).

**Definition 2.** The \(p\)-weight degree of a polynomial \(F(X_1, \ldots, X_n) = \sum_d a_d x^d\) is \(w_p(F) = \max_{x^d, a_d \neq 0} w_p(x^d)\), where the maximum is taken over those monomials which effectively appear in \(F\) with a non zero coefficient.

In our proof of theorems 1 below, we follow the elementary and elegant proof of Katz, given by Daqing Wan in [13].

**Theorem 1.** Let \(F_1, \ldots, F_r\) be polynomials in \(n\) variables with coefficients in \(k\), a finite field with \(q = p^f\) elements. Let \(w_p(F_i)\) be the \(p\)-weight degree of \(F_i\) and let \(\mu\) be:

\[
\mu = \left\lceil f \left( \frac{n - \sum_{i=1}^r w_p(F_i)}{\max_{1 \leq i \leq r} \{w_p(F_i)\}} \right) \right\rceil.
\]

Then \(p^\mu\) divides \(N(F_1 = 0, \ldots, F_r = 0)\).

**Theorem 0-1.** Let \(F_1, \ldots, F_r\) be polynomials in \(n\) variables with coefficients in \(k\). Let \(w_p(F_i)\) be the \(p\)-weight degree of \(F_i\) and let \(\mu\) be:

\[
\mu = \max \left( f \left( \frac{n - \sum_{i=1}^r \deg(F_i)}{\max_{1 \leq i \leq r} \{\deg(F_i)\}} \right), \left| f \left( \frac{n - \sum_{i=1}^r w_p(F_i)}{\max_{1 \leq i \leq r} \{w_p(F_i)\}} \right) \right| \right).
\]

We then have that \(p^\mu\) divides \(N(F_1 = 0, \ldots, F_r = 0)\).

**Corollary.** Let \(F(x_1, \ldots, x_n)\) be a polynomial over \(k\), and let \(l = w_p(F)\), and \(S(F)\) be the exponential sum:

\[
S(F) = \sum_{x_1, \ldots, x_n \in k} \eta(F(x_1, \ldots, x_n)),
\]

where \(\eta\) is an additive character defined over \(k\). Let \(\mu\) be the highest exponent of \(p\)-divisibility for \(S(F)\), then \(\mu \geq f(n/l)\).

The above corollary is to our knowledge new and improves in many cases upon results of Adolphson and Sperber in [1].