Nanjing Univ. J. Math. Biquarterly 40 (2023), no. 2, in press.

EXTENSIONS OF WILSON'S LEMMA AND THE AX-KATZ THEOREM

ZHI-WEI SUN

ABSTRACT. A classical result of A. Fleck states that if p is a prime, and $n>0$ and r are integers, then

$$\sum_{k\equiv r\,(\mathrm{mod}\ p)}\binom{n}{k}(-1)^k\equiv 0\ (\mathrm{mod}\ p^{\lfloor (n-1)/(p-1)\rfloor}).$$

In 2006 R. M. Wilson used Fleck's congruence and Weisman's extension to present a useful lemma on polynomials modulo prime powers, and applied this lemma to re-prove the Ax-Katz theorem on systems of polynomial equations over finite fields and deduce various results on codewords in p-ary linear codes with weights. In light of the generalizations of Fleck's congruence given by D. Wan, and D. M. Davis and Z.-W. Sun during 2006–2007, we obtain new extensions of Wilson's lemma and the Ax-Katz theorem.

1. INTRODUCTION

Let p be a prime, and let $n\in\mathbb{N}=\{0,1,2,\ldots\}$ and $r\in\mathbb{Z}$. In 1913 A. Fleck (cf. [4, p. 274]) proved that

$$\mathrm{ord}_p\Bigg(\sum_{k\equiv r\,(\mathrm{mod}\ p)}\binom{n}{k}(-1)^k\Bigg)\geq\left\lfloor\frac{n-1}{p-1}\right\rfloor,\tag{1.1}$$

where $\lfloor\cdot\rfloor$ is the well-known floor function, and the p-adic order $\mathrm{ord}_p(\alpha)$ of a p-adic number α is given by $\sup\{a\in\mathbb{Z}:\ \alpha/p^a\in\mathbb{Z}_p\}$. (As usual $\mathbb{Z}_p$ denotes the ring of p-adic integers in the p-adic field $\mathbb{Q}_p$.)

Let $a\in\mathbb{Z}^+=\{1,2,3,\ldots\}$. In 1977, motivated by his study of p-adically continuous functions and unaware of Fleck's earlier result, C. S. Weisman [20] extended Fleck's inequality as follows:

$$\mathrm{ord}_p\Bigg(\sum_{k\equiv r\,(\mathrm{mod}\ p^a)}\binom{n}{k}(-1)^k\Bigg)\geq\left\lfloor\frac{n-p^{a-1}}{\varphi(p^a)}\right\rfloor,\tag{1.2}$$

where φ is Euler's totient function. See also [14] for another proof of this.

Key words and phrases. Ax-Katz theorem, finite fields, p-adic congruences, Wilson's lemma.

2020 *Mathematics Subject Classification.* Primary 11T06; Secondary 05A10, 11A07, 11S05, 41A10.

The initial version of this paper was posted to arXiv in 2006 as a preprint with the ID arXiv:math.NT/0608560.

For a function f from the complex field $\mathbb{C}$ to $\mathbb{C}$, let $\Delta^0 f(x) = f(x)$, $\Delta f(x) = f(x+1) - f(x)$ and $\Delta^n f(x) = \Delta(\Delta^{n-1} f(x))$ for $n = 2, 3, \ldots$. Now we recall a classical interpolation formula due to I. Newton and J. Gregory.

Newton-Gregory Interpolation Formula. *Given a function $f : \mathbb{C} \to \mathbb{C}$, for any $d \in \mathbb{N}$ we have*

$$f(x) = \sum_{n=0}^{d} c_n \binom{x}{n} + R_d(x),$$

where

$$c_n = \Delta^n f(0) = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} f(k)$$

and

$$R_d(x) = \begin{vmatrix} 1 & 0 & \cdots & 0 & f(0) \\ 1 & 1^1 & \cdots & 1^d & f(1) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & d^1 & \cdots & d^d & f(d) \\ 1 & x^1 & \cdots & x^d & f(x) \end{vmatrix} \Bigg/ \begin{vmatrix} 1^1 & 1^2 & \cdots & 1^d \\ 2^1 & 2^2 & \cdots & 2^d \\ \cdots & \cdots & \cdots & \cdots \\ d^1 & d^2 & \cdots & d^d \end{vmatrix}.$$

Note that the above $R_d(x)$ vanishes if f is a polynomial with $\deg f \le d$.

In 2006 R. M. Wilson [21] rediscovered Weisman's (1.2) in the case $n \equiv p^{a-1} \pmod{\varphi(p^a)}$, and used it to obtain the following lemma (similar to the Newton-Gregory interpolation formula) and give many applications.

Wilson's Lemma. *Let p be a prime, and let $a, b \in \mathbb{Z}^+$. Let f be an integer-valued function on the integers that is periodic modulo p^a. Then there exists a polynomial*

$$w(x) = c_0 + c_1 x + c_2 \binom{x}{2} + \cdots + c_d \binom{x}{d} \quad (c_0, c_1, \ldots, c_d \in \mathbb{Z})$$

of degree smaller than $b\varphi(p^a) + p^{a-1}$ such that

$$\mathrm{ord}_p(c_n) \ge \left\lfloor \frac{n - p^{a-1}}{\varphi(p^a)} \right\rfloor \quad \text{for all } n = 0, \ldots, d,$$

and $w(x) \equiv f(x) \pmod{p^b}$ for all $x \in \mathbb{Z}$.

In this paper, for a prime p we let $\overline{\mathbb{Q}}_p$ be the algebraic closure of the field $\mathbb{Q}_p$ and let $\overline{\mathbb{Z}}_p$ be the ring of p-adic algebraic integers in $\overline{\mathbb{Q}}_p$. For $m, n \in \mathbb{N}$ we use $[m, n]$ to denote the set $\{x \in \mathbb{Z} :\ m \le x \le n\}$.

In view of the generalizations of Fleck's and Weisman's results given in [10, 18, 3, 13, 11, 15]), we are able to present the following further extension of Wilson's Lemma.

Theorem 1.1. *Let p be a prime, and let $a \in \mathbb{N}$ and $b \in \mathbb{Z}^+$. Let $f(x) \in \overline{\mathbb{Q}}_p[x]$ with $\deg f \le l \in \mathbb{N}$ and $f(m) \in \overline{\mathbb{Z}}_p$ for all $m \in \mathbb{Z}$, and let g be a function from $[0, p^a - 1]$ to $\overline{\mathbb{Z}}_p$. Let $d \in \mathbb{N}$ be the maximal integer with $M_d < b$, where*

$$M_d = \max\left\{\left\lfloor\frac{d - lp^a - p^{a-1}}{\varphi(p^a)}\right\rfloor, \mathrm{ord}_p\left(\left\lfloor\frac{d}{p^{a-1}}\right\rfloor!\right) - \mathrm{ord}_p(l!) - \min\left\{l, \left\lfloor\frac{d}{p^a}\right\rfloor\right\}\right\}.$$

Then there exists a polynomial

$$P(x) = \sum_{n=0}^{d} c_n\binom{x}{n} \quad (c_0, \dots, c_d \in \overline{\mathbb{Z}}_p) \tag{1.3}$$

with $\mathrm{ord}_p(c_n) \ge M_n$ for all $n = 0, \dots, d$, such that

$$P(p^a q + r) \equiv f(q)g(r) \pmod{p^b} \quad \text{for all } q \in \mathbb{Z} \text{ and } r \in [0, p^a - 1]. \tag{1.4}$$

The following celebrated theorem (cf. C. Chevally [2], E. Warning [19] and Theorem 2.6 of M. B. Nathanson [9, pp. 50–51]) is well known and quite useful.

Chevalley-Warning Theorem. *Let $f_1(x, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$ be polynomials over a finite field F of characteristic p with $\deg f_1 + \cdots + \deg f_m < n$. Then the number of solutions to the system of equations*

$$\begin{cases} f_1(x_1, \dots, x_n) = 0, \\ \cdots\cdots\cdots\cdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases} \tag{1.5}$$

over F^n is a multiple of p.

Here is a further refinement of the Chevalley-Warning theorem due to J. Ax [1] in the case $m = 1$, and N. Katz [7] in the general case.

Ax-Katz Theorem. *Let $\mathbb{F}_q$ be the finite field with $q = p^a$ elements where p is a prime and $a \in \mathbb{Z}^+$. Let $f_1(x, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$ be nonzero polynomials over $\mathbb{F}_q$ with degrees $d_1 \ge \ldots \ge d_m$ respectively. Then, for any positive integer b satisfying $n > (b-1)d_1 + (d_1 + \cdots + d_m)$, q^b divides the number of solutions to the system (1.5) over $\mathbb{F}_q^n$.*

D. Wan [16, 17] gave a new proof of the Ax-Katz theorem via the Stickelberger theorem. In 2005 X.-D. Hou [6] reduced the Ax-Katz theorem to the Ax theorem on a single polynomial equation. In 2006 Wilson [21] re-proved the Ax-Katz theorem for prime fields by using Wilson's Lemma.

With the help of Theorem 1.1, we establish the following theorem.

Theorem 1.2. *Let p be a prime, and let $F_1(x), \dots, F_m(x) \in \overline{\mathbb{Q}}_p[x]$ with $\deg F_k \le l_k \in \mathbb{N}$ and $F_k(a) \in \overline{\mathbb{Z}}_p$ for all $a \in \mathbb{Z}$. Let $a_1, \dots, a_m \in \mathbb{N}$, and let $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$ be nonzero polynomials with integer coefficients. Assume that $d_1\varphi(p^{a_1}) = \max_{1 \le k \le m} d_k\varphi(p^{a_k})$ where $d_k = \deg f_k$ for*

$k=1,\ldots,m$. *Let $b\in\mathbb{Z}^+$ and suppose that*

$$n>(b-1)\max\left\{\frac{d_1\varphi(p^{a_1})}{p-1},1\right\}+\frac{1}{p-1}\sum_{k=1}^m((l_k+1)p^{a_k}-[\![a_k\neq 0]\!])d_k, \quad (1.6)$$

where $[\![a_k\neq 0]\!]$ takes 1 or 0 according as $a_k\neq 0$ or not. Then

$$\sum_{\substack{x_1,\ldots,x_n\in[0,p-1]\\ p^{a_k}\mid f_k(x_1,\ldots,x_n)\ \text{for all}\ k\in[1,m]}}\prod_{k=1}^m F_k\left(\frac{f_k(x_1,\ldots,x_n)}{p^{a_k}}\right)\equiv 0 \pmod{p^b}. \quad (1.7)$$

In the case $F_1(x)=\cdots=F_m(x)=1$, Theorem 1.2 yields an extension of the Ax-Katz theorem for prime fields. In 1995 O. Moreno and C. J. Moreno [8] introduced a method to reduce the general case of the Ax-Katz theorem to the prime field case.

Corollary 1.1. *Let $f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n)$ be nonzero polynomials with integer coefficients having degrees $d_1\geq\cdots\geq d_m$ respectively. If p is a prime, $a,b\in\mathbb{Z}^+$, $l_1,\ldots,l_m\in\mathbb{N}$ and*

$$n>(b-1)d_1p^{a-1}+\frac{p^a-1}{p-1}\sum_{k=1}^m d_k+\frac{p^a}{p-1}\sum_{k=1}^m l_kd_k, \quad (1.8)$$

then we have

$$\sum_{\substack{x_1,\ldots,x_n\in[0,p-1]\\ p^{a}\mid f_k(x_1,\ldots,x_n)\ \text{for all}\ k\in[1,m]}}\prod_{k=1}^m \binom{f_k(x_1,\ldots,x_n)/p^a}{l_k}\equiv 0 \pmod{p^b}. \quad (1.9)$$

Proof. Just apply Theorem 1.2 with $a_k=a$ and $F_k(x)=\binom{x}{l_k}$ for $k=1,\ldots,m$. □

Let $q=p^a$ with p prime and $a\in\mathbb{Z}^+$, and let $\zeta_{q-1}\in\overline{\mathbb{Z}}_p$ be a primitive $(q-1)$-th roots of unity. It is well known that $\mathbb{Z}_p[\zeta_{q-1}]/(p)$ is a finite field of q elements. The finite field $\mathbb{F}_q$ of $q=p^a$ elements is an extension of the prime field $\mathbb{F}_p$ with $[\mathbb{F}_q:\mathbb{F}_p]=a$. Thus $\mathbb{F}_q$ is isomorphic to $\mathbb{F}_p^a$ and the Chevalley-Warning theorem can be reduced to the prime field case. Corollary 1.1 in the case $a=b=1$ and $l_1=\ldots=l_m=0$ yields the Chevalley-Warning theorem for $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ and hence the general case of the Chevalley-Warning theorem.

To end this section, we mention an open conjecture posed by the author in 2007 which also appeared in [12, Conjecture 40].

Conjecture 1.1. *Let p be a prime, and let $l,n\in\mathbb{N}$ and $r\in\mathbb{Z}$. If n or r is not divisible by p, then we have*

$$\begin{aligned}&\mathrm{ord}_p\Bigg(\sum_{k\equiv r\pmod{p}}\binom{n}{k}(-1)^k\binom{(k-r)/p}{l}\Bigg)\\ &\geq\left\lfloor\frac{n-lp-1}{p-1}\right\rfloor+\mathrm{ord}_p\left(\binom{\lfloor(n-l-1)/(p-1)\rfloor}{l}\right).\end{aligned}$$

2. Proofs of Theorems 1.1 and 1.2

Lemma 2.1. *Let p be a prime, and let $f(x) \in \overline{\mathbb{Q}}_p[x]$ with $\deg f \le l \in \mathbb{N}$ and $f(m) \in \overline{\mathbb{Z}}_p$ for all $m \in \mathbb{Z}$. For any $a, n \in \mathbb{N}$ and $r \in \mathbb{Z}$, we have*

$$\operatorname{ord}_p\Bigg(\sum_{k \equiv r \,(\mathrm{mod}\ p^a)} \binom{n}{k} (-1)^k f\left(\frac{k-r}{p^a}\right) \Bigg) \ge \left\lfloor \frac{n - lp^a - p^{a-1}}{\varphi(p^a)} \right\rfloor \tag{2.1}$$

and

$$\begin{aligned} &\operatorname{ord}_p\Bigg(\sum_{k \equiv r \,(\mathrm{mod}\ p^a)} \binom{n}{k} (-1)^k f\left(\frac{k-r}{p^a}\right) \Bigg) \\ \ge &\operatorname{ord}_p\left(\left\lfloor \frac{n}{p^{a-1}} \right\rfloor ! \right) - \operatorname{ord}_p(l!) - \min\left\{ l, \left\lfloor \frac{n}{p^a} \right\rfloor \right\}. \end{aligned} \tag{2.2}$$

Proof. Let $c_j = \sum_{i=0}^{j} \binom{j}{i} (-1)^{j-i} f(i) \in \overline{\mathbb{Z}}_p$ for $j = 0, \ldots, l$. As $\deg f \le l$ and $f(x) - \sum_{j=0}^{l} c_j \binom{x}{j}$ vanishes at $0, \ldots, l$, we have $f(x) = \sum_{j=0}^{l} c_j \binom{x}{j}$. So it suffices to consider the case $f(x) = \binom{x}{l}$ only.

If $a \in \mathbb{Z}^+$ then

$$O := \operatorname{ord}_p\Bigg(\sum_{k \equiv r \,(\mathrm{mod}\ p^a)} \binom{n}{k} (-1)^k \binom{(k-r)/p^a}{l} \Bigg) \ge \left\lfloor \frac{n - lp^a - p^{a-1}}{\varphi(p^a)} \right\rfloor$$

by D. Wan [18, Theorem 1.3] (see also [15] for a combinatorial proof). This is also true in the case $a = 0$, since

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k \binom{k-r}{l} = [\![l \ge n]\!] (-1)^n \binom{-r}{l-n}$$

by a known identity (cf. [5, (5.24)]).

As $l!\binom{x}{l} \in \mathbb{Z}[x]$, by [3, Theorem 1.5] we have

$$O + \operatorname{ord}_p(l!) \ge \operatorname{ord}_p\left(\left\lfloor \frac{n}{p^a} \right\rfloor ! \right) = \sum_{s=a+1}^{\infty} \left\lfloor \frac{n}{p^s} \right\rfloor = \operatorname{ord}_p\left(\left\lfloor \frac{n}{p^{a-1}} \right\rfloor ! \right) - \left\lfloor \frac{n}{p^a} \right\rfloor .$$

By [13, Theorem 1.2], we also have

$$O \ge \operatorname{ord}_p\left(\left\lfloor \frac{n}{p^{a-1}} \right\rfloor ! \right) - l - \operatorname{ord}_p(l!).$$

Combining the above we obtain both (2.1) and (2.2). □

`Proof of Theorem 1.1.` Let $F(x) = f(\lfloor x/p^a \rfloor) g(\{x\}_{p^a})$ for $x \in \mathbb{Z}$, where $\{x\}_{p^a}$ denotes the least nonnegative residue of x modulo p^a. For

$$\begin{aligned} c_n :=& \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} F(k) \\ =& (-1)^n \sum_{r=0}^{p^a-1} g(r) \sum_{k \equiv r \ (\mathrm{mod}\ p^a)} \binom{n}{k} (-1)^k f\left(\frac{k-r}{p^a}\right), \end{aligned}$$

we have $\mathrm{ord}_p(c_n) \geq M_n$ by Lemma 2.1. If $n > d$, then $\mathrm{ord}_p(c_n) \geq M_n \geq b$. Set $P(x) = \sum_{n=0}^{d} c_n \binom{x}{n}$. Then, for each $m \in \mathbb{N}$ we have

$$\begin{aligned} F(m) =& \sum_{k=0}^{m}\binom{m}{k}F(k)(1-1)^{m-k} = \sum_{k=0}^{m}\binom{m}{k}F(k)\sum_{n=k}^{m}\binom{m-k}{n-k}(-1)^{n-k} \\ =& \sum_{n=0}^{m}\binom{m}{n}\sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}F(k) = \sum_{n\in\mathbb{N}}\binom{m}{n}c_n \\ \equiv& \sum_{n=0}^{d}\binom{m}{n}c_n = P(m) \pmod{p^b}. \end{aligned}$$

Therefore $P(p^a q + r) \equiv F(p^a q + r) = f(q)g(r) \pmod{p^b}$ for all $q \in \mathbb{N}$ and $r \in [0, p^a - 1]$.

Choose $N \in \mathbb{N}$ such that $N - b \geq \mathrm{ord}_p(k)$ for all $k \in [1, \max\{d, l\}]$. For any $x \in \mathbb{Z}$ and $n \in [0, \max\{d, l\}]$, by the Chu-Vandermonde convolution identity (cf. [5, (5.27)]) we have

$$\begin{aligned} &\binom{x+p^N}{n} = \sum_{k=0}^{n}\binom{p^N}{k}\binom{x}{n-k} \\ =&\binom{x}{n} + \sum_{0<k\leq n}\frac{p^N}{k}\binom{p^N-1}{k-1}\binom{x}{n-k} \equiv \binom{x}{n} \pmod{p^b}. \end{aligned}$$

Therefore $P(x + p^N) \equiv P(x) \pmod{p^b}$ and $f(x + p^N) \equiv f(x) \pmod{p^b}$ for all $x \in \mathbb{Z}$. For $m = -p^a q + r$ with $q \in \mathbb{Z}^+$ and $r \in [0, p^a - 1]$, clearly $m + p^{a+q+N} \geq 0$ and hence

$$\begin{aligned} P(m) \equiv& P(m + p^{a+q+N}) \equiv F(m + p^{a+q+N}) \\ \equiv& f\left(\left\lfloor \frac{m}{p^a} \right\rfloor + p^{q+N}\right) g(\{m\}_{p^a}) \\ \equiv& f\left(\left\lfloor \frac{m}{p^a} \right\rfloor\right) g(\{m\}_{p^a}) = F(m) \pmod{p^b}. \end{aligned}$$

By the above, we do have $P(p^a q + r) \equiv F(p^a q + r) = f(q)g(r) \pmod{p^b}$ for all $q \in \mathbb{Z}$ and $r \in [0, p^a - 1]$. □

Lemma 2.2. *Let p be a prime, and let*

$$F(x_1, \ldots, x_n) = \binom{f_1(x_1, \ldots, x_n)}{j_1} \cdots \binom{f_m(x_1, \ldots, x_n)}{j_m},$$

where $j_k \in \mathbb{N}$ and $f_k(x_1, \ldots, x_n) \in \overline{\mathbb{Z}}_p[x_1, \ldots, x_n]$ for $k = 1, \ldots, m$. If the total degree of $F(x_1, \ldots, x_n)$ is smaller than $(n-c+1)(p-1)$ for some $c \in \mathbb{N}$, then

$$\sum_{x_1,\ldots,x_n\in[0,p-1]} F(x_1, \ldots, x_n) \equiv 0 \pmod{p^c}.$$

Proof. See [21, Lemma 4] and its proof. □

Proof of Theorem 1.2. Given $k \in [1, m]$, by Theorem 1.1 there is a polynomial

$$P_k(x) = \sum_{j=0}^{n_k} c_j^{(k)} \binom{x}{j} \quad (c_1^{(k)}, \ldots, c_{n_k}^{(k)} \in \overline{\mathbb{Z}}_p)$$

such that

$$\mathrm{ord}_p(c_j^{(k)}) \geq \left\lfloor \frac{j - l_k p^{a_k} - p^{a_k - 1}}{\varphi(p^{a_k})} \right\rfloor$$

for all $j = 0, \ldots, n_k$, and

$$P_k(x) \equiv [\![p^{a_k} \mid x]\!] F_k\left(\frac{x}{p^{a_k}}\right) \pmod{p^b} \quad \text{for all } x \in \mathbb{Z}.$$

Therefore

$$\begin{aligned} &\sum_{\substack{x_1, \ldots, x_n \in [0, p-1] \\ p^{a_k} \mid f_k(x_1, \ldots, x_n) \text{ for all } k \in [1,m]}} \prod_{k=1}^{m} F_k\left(\frac{f_k(x_1, \ldots, x_n)}{p^{a_k}}\right) \\ \equiv &\sum_{x_1, \ldots, x_n \in [0, p-1]} \prod_{k=1}^{m} P_k(f_k(x_1, \ldots, x_n)) \\ \equiv &\sum_{j_1=0}^{n_1} c_{j_1}^{(1)} \cdots \sum_{j_m=0}^{n_m} c_{j_m}^{(m)} S(j_1, \ldots, j_m) \pmod{p^b}, \end{aligned}$$

where

$$S(j_1, \ldots, j_m) = \sum_{x_1, \ldots, x_n \in [0, p-1]} \prod_{k=1}^{m} \binom{f_k(x_1, \ldots, x_n)}{j_k}.$$

Fix $j_1 \in [0, n_1], \ldots, j_m \in [0, n_m]$, and let

$$\alpha_k = \max\left\{ \left\lfloor \frac{j_k - l_k p^{a_k} - p^{a_k - 1}}{\varphi(p^{a_k})} \right\rfloor, 0 \right\} \quad \text{for } k = 1, \ldots, m.$$

Then

$$\mathrm{ord}_p\left(c_{j_1}^{(1)} \cdots c_{j_m}^{(m)}\right) = \sum_{k=1}^{m} \mathrm{ord}_p\left(c_{j_k}^{(k)}\right) \geq \sum_{k=1}^{m} \alpha_k.$$

So it suffices to show that $\mathrm{ord}_p(S(j_1, \ldots, j_m)) \geq c = b - \sum_{k=1}^{m} \alpha_k$.

Assume that $c > 0$. By the definition of α_k, we have $j_k - l_k p^{a_k} - p^{a_k - 1} < (\alpha_k + 1)\varphi(p^{a_k})$ and hence

$$j_k \leq l_k p^{a_k} + (\alpha_k + 1)\varphi(p^{a_k}) + [\![a_k \neq 0]\!](p^{a_k - 1} - 1).$$

Thus

$$\begin{aligned}\sum_{k=1}^m j_kd_k \le& \sum_{k=1}^m \left(l_kp^{a_k} + [\![a_k\ne 0]\!](p^{a_k-1}-1) + (\alpha_k+1)\varphi(p^{a_k})\right)d_k\\ =&\sum_{k=1}^m \left(l_kp^{a_k} + p^{a_k} - [\![a_k\ne 0]\!] + \alpha_k\varphi(p^{a_k})\right)d_k\\ \le&\sum_{k=1}^m \left((l_k+1)p^{a_k} - [\![a_k\ne 0]\!]\right)d_k + \varphi(p^{a_1})d_1\sum_{k=1}^m \alpha_k\end{aligned}$$

and hence

$$\begin{aligned}\sum_{k=1}^m j_kd_k <& n(p-1)-(b-1)\max\{d_1\varphi(p^{a_1}),p-1\} + (b-c)d_1\varphi(p^{a_1})\\ \le& n(p-1)-(c-1)\max\{d_1\varphi(p^{a_1}),p-1\}.\end{aligned}$$

Therefore

$$\deg\prod_{k=1}^m \binom{f_k(x_1,\ldots,x_n)}{j_k} \le \sum_{k=1}^m j_kd_k < (p-1)(n-c+1)$$

and hence $S(j_1,\ldots,j_m)\equiv 0 \pmod{p^c}$ by Lemma 2.2. This concludes the proof. □

References

[1] J. Ax, *Zeroes of polynomials over finite fields*, Amer. J. Math. **86** (1964), 255–261.
[2] C. Chevalley, *Démonstration d'une hypothèse de M. Artin* Abh. Math. Sem. Hamburg **11** (1936), 73–75.
[3] D. M. Davis and Z. W. Sun, *A number-theoretic approach to homotopy exponents of $SU(n)$*, J. Pure Appl. Algebra **209** (2007), 57–69.
[4] L. E. Dickson, History of the Theory of Numbers, Vol. I, AMS Chelsea Publ., 1999.
[5] R. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics, Addison-Wesley, New York, 1989.
[6] X.-D. Hou, *A note on the proof of a theorem of Katz*, Finite Fields Appl. **11** (2005), 316–319.
[7] N. Katz, *On a theorem of Ax*, Amer. J. Math. **93** (1971), 485–499.
[8] O. Moreno and C. J. Merono, *Improvements of the Chevalley-Warning and the Ax-Katz theorem*, Amer. J. Math. **117** (1995), 241–244.
[9] M. B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Graduate Texts in Math., Vol. 165, Springer, New York, 1996.
[10] Z.-W. Sun, *Polynomial extension of Fleck's congruence*, Acta Arith. **122** (2006), 91–100.
[11] Z.-W. Sun, *Combinatorial congruences and Stirling numbers*, Acta Arith. **126** (2007), 387–398.
[12] Z.-W. Sun, *Open conjectures on congruences*, Nanjing Univ. J. Math. Biquarterly **36** (2019), no. 1, 1–99.
[13] Z.-W. Sun and D. M. Davis, *Combinatorial congruences modulo prime powers*, Trans. Amer. Math. Soc. **359** (2007), 5525–5553.
[14] Z. W. Sun and D. Wan, *On Fleck quotients*, Acta Arith. **127** (2007), 337–363.
[15] Z. W. Sun and D. Wan, *Lucas-type congruences for cyclotomic ψ-coefficients*, Int. J. Number Theory **4** (2008), 155–170.

[16] D. Wan, *An elementary proof of a theorem of Katz*, Amer. J. Math. **111** (1989), 1–8.
[17] D. Wan, *A Chevalley-Warning approach to p-adic estimates of character sums*, Proc. Amer. Math. Soc. **123** (1995), 45–54.
[18] D. Wan, *Combinatorial congruences and ψ-operators*, Finite Fields Appl. **12** (2006), 693–703.
[19] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abh. Math. Sem. Hamburg **11** (1936), 76–83.
[20] C. S. Weisman, *Some congruences for binomial coefficients*, Michigan Math. J. **24** (1977), 141–151.
[21] R. M. Wilson, *A lemma on polynomials modulo p^m and applications to coding theory*, Discrete Math. **306** (2006), 3154–3165.

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China
E-mail address: zwsun@nju.edu.cn
Homepage: http://maths.nju.edu.cn/~zwsun