ACTA ARITHMETICA
122.1 (2006)

Polynomial extension of Fleck's congruence

by

ZHI-WEI SUN (Nanjing)

1. Introduction. As usual, we let $\binom{x}{0} = 1$ and

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!} \quad \text{for every } k = 1, 2, \ldots.$$

For convenience, we also set $\binom{x}{k} = 0$ for any negative integer k.

Let p be a prime and r be an integer. In 1913, A. Fleck (cf. Dickson [D, p. 274]) discovered that

$$\sum_{k \equiv r \,(\mathrm{mod}\, p)} \binom{n}{k}(-1)^k \equiv 0 \ (\mathrm{mod}\, p^{\lfloor (n-1)/(p-1) \rfloor}) \tag{1.1}$$

for all $n \in \mathbb{Z}^+ = \{1, 2, \ldots\}$, where $\lfloor \cdot \rfloor$ is the well-known floor function. Sums of the form $\sum_{k \equiv r \,(\mathrm{mod}\, m)} \binom{n}{k}$ or $\sum_{k \equiv r \,(\mathrm{mod}\, m)} \binom{n}{k}(-1)^k$ (with $m \in \mathbb{Z}^+$) have various applications in number theory and combinatorics (see, e.g., [SS], [H] and [S02]).

In 1977, by a very complicated method, C. S. Weisman [W] extended Fleck's congruence to prime power moduli in the following way:

$$\sum_{k \equiv r \,(\mathrm{mod}\, p^\alpha)} \binom{n}{k}(-1)^k \equiv 0 \ (\mathrm{mod}\, p^{\lfloor (n-p^{\alpha-1})/\varphi(p^\alpha) \rfloor}), \tag{1.2}$$

where $\alpha, n \in \mathbb{N} = \{0, 1, 2, \ldots\}$ and $n \geq p^{\alpha-1}$, and φ denotes Euler's totient function. Unaware of Fleck's previous work, Weisman was motivated by studying the relation between two different ways (Mahler's and van der Put's) to express a p-adically continuous function.

Quite recently, in his lecture notes on Fontaine's rings and p-adic L-functions given at Irvine (Spring, 2005), D. Wan got the following new ex-

---

2000 *Mathematics Subject Classification*: Primary 11B65; Secondary 05A10, 11A07, 11B68, 11S05.

The author is partially supported by the National Science Fund for Distinguished Young Scholars (no. 10425103) and a Key Program of NSF in P.R. China.

tension of Fleck's congruence:

$$\sum_{k\equiv r\ (\mathrm{mod}\, p)} \binom{n}{k}(-1)^k \binom{(k-r)/p}{l} \equiv 0 \ (\mathrm{mod}\, p^{\lfloor (n-lp-1)/(p-1)\rfloor}), \tag{1.3}$$

where $l, n \in \mathbb{N}$ and $n > lp$. Wan was led to this when trying to understand a sharp estimate for the ψ-operator in Fontaine's theory of (ϕ, Γ)-modules.

For a prime p, we let $\mathbb{Q}_p$ and $\mathbb{Z}_p$ denote the field of p-adic numbers and the ring of p-adic integers respectively; the p-adic order of $\omega \in \mathbb{Q}_p$ is defined by $\mathrm{ord}_p(\omega) = \sup\{a \in \mathbb{Z} : \omega/p^a \in \mathbb{Z}_p\}$ (whence $\mathrm{ord}_p(0) = +\infty$). Throughout this paper, the Kronecker symbol $\delta_{m,n}$ with $m, n \in \mathbb{N}$ equals 1 or 0 according as $m = n$ or not.

Clearly both Weisman's and Wan's extensions of Fleck's congruence follow from the special case $\alpha = \beta$ of the following theorem, which we will establish by a combinatorial approach.

THEOREM 1.1. *Let p be a prime, and let $f(x) \in \mathbb{Q}_p[x]$, $\deg f \le l \in \mathbb{N}$ and $f(a) \in \mathbb{Z}_p$ for all $a \in \mathbb{Z}$. Provided that $\alpha, \beta \in \mathbb{N}$ and $\alpha \ge \beta$, we have*

$$\sum_{k\equiv r\ (\mathrm{mod}\, p^{\beta})} \binom{n}{k}(-1)^k f\left(\left\lfloor \frac{k-r}{p^{\alpha}}\right\rfloor\right) \in p^{\lfloor (n-p^{\alpha-1}-l)/\varphi(p^{\alpha})\rfloor-(l-1)\alpha-\beta}\mathbb{Z}_p \tag{1.4}$$

for all integers $n \ge p^{\alpha-1}$ and r; moreover, we can substitute $\delta_{\beta,0}$ for the first l in (1.4) *if α is greater than one.*

By Theorem 1.1 in the case $\alpha = \beta = r = 0$, if $f(x) \in \mathbb{Z}[x]$ and $f(x) \ne 0$, then for any integer $n > \deg f + 1$ we have $\sum_{k=0}^{n}\binom{n}{k}(-1)^k f(k) = 0$ since the sum is divisible by all primes. In fact, a known identity due to L. Euler (cf. [LW, pp. 90–91]) states that

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^k k^l = \begin{cases} (-1)^n n! & \text{if } l = n \in \mathbb{N}, \\ 0 & \text{if } 0 \le l < n. \end{cases}$$

Now we derive more consequences of Theorem 1.1.

COROLLARY 1.1. *Let p be a prime, $m \in \mathbb{Z}^+$ and $\alpha = \mathrm{ord}_p(m)$. Let $l, n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then*

$$\mathrm{ord}_p\Bigg(\sum_{k\equiv r\ (\mathrm{mod}\, p^{\alpha})} \binom{n}{k}(-1)^k B_l\left(\frac{k-r}{m}\right)\Bigg) \ge \left\lfloor \frac{n-p^{\alpha-1}-l(\delta_{\alpha,0}+\delta_{\alpha,1})}{\varphi(p^{\alpha})}\right\rfloor - l\alpha, \tag{1.5}$$

where $B_l(x)$ is the Bernoulli polynomial of degree l.

Proof. (1.5) holds trivially if $n < p^{\alpha-1}$. Below we suppose $n \ge p^{\alpha-1}$.

When $l = 0$, (1.5) reduces to Weisman's congruence (1.2). In the case $\alpha = 0$, if the lower bound in (1.5) is nonnegative (i.e., $l < n$) then the summation in (1.5) vanishes by Euler's identity.

Now we assume $l\alpha \neq 0$, and let $B_l = B_l(0)$ be the lth Bernoulli number. Note that $m_0 = m/p^\alpha$ is relatively prime to p. For any $a \in \mathbb{Z}$ we have $B_l(a/m_0) - B_l \in \mathbb{Z}_p$, because

$$m_0^l\left(B_l\left(\frac{a}{m_0}\right) - B_l\right) = \left(m_0^l B_l\left(\frac{a}{m_0}\right) - B_l\right) - (m_0^l B_l(0) - B_l) \in \mathbb{Z}_p$$

by [S03, Corollary 1.3]. Applying Theorem 1.1 with $f(x) = B_l(x/m_0) - B_l$ and $\beta = \alpha$, we get

$$\mathrm{ord}_p\left(\sum_{k\equiv r \,(\mathrm{mod}\, p^\alpha)} \binom{n}{k}(-1)^k B_l\left(\frac{k-r}{m}\right) - B_l\Sigma\right) \ge \left\lfloor \frac{n - p^{\alpha-1} - l\delta_{\alpha,1}}{\varphi(p^\alpha)} \right\rfloor - l\alpha,$$

where $\Sigma = \sum_{k\equiv r \,(\mathrm{mod}\, p^\alpha)} \binom{n}{k}(-1)^k$. Recall that $pB_l \in \mathbb{Z}_p$ by the von Staudt–Clausen theorem (cf. [IR, pp. 233–236]). This, together with (1.2), shows that

$$\mathrm{ord}_p(B_l\Sigma) \ge \mathrm{ord}_p(\Sigma) - 1 \ge \left\lfloor \frac{n - p^{\alpha-1}}{\varphi(p^\alpha)} \right\rfloor - 1 \ge \left\lfloor \frac{n - p^{\alpha-1} - l\delta_{\alpha,1}}{\varphi(p^\alpha)} \right\rfloor - l\alpha.$$

So the desired (1.5) follows. ∎

COROLLARY 1.2. *Let p be a prime, and let $f(x) \in \mathbb{Q}_p[x]$, $\deg f = l \ge 0$ and $f(a) \in \mathbb{Z}_p$ for all $a \in \mathbb{Z}$. Let $\alpha \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then, for any integer $n \ge p^{\alpha-1}$, we have*

$$(1.6)\qquad \mathrm{ord}_p\left(\sum_{k=0}^{n}\binom{n}{k}(-1)^k (k-r, p^\alpha) f\left(\left\lfloor \frac{k-r}{p^\alpha}\right\rfloor\right)\right) \ge \left\lfloor \frac{n - p^{\alpha-1} - l(\delta_{\alpha,0} + \delta_{\alpha,1})}{\varphi(p^\alpha)} \right\rfloor - (l-1)\alpha - 1,$$

where $(k-r, p^\alpha)$ is the greatest common divisor of $k - r$ and p^α.

Proof. Let $g(1) = p$ and $g(p^\beta) = p - 1$ if $0 < \beta \le \alpha$. By Theorem 1.1, the p-adic order of

$$\sum_{\beta=0}^{\alpha} g(p^\beta)p^\beta \sum_{k\equiv r \,(\mathrm{mod}\, p^\beta)} \binom{n}{k}(-1)^k f\left(\left\lfloor \frac{k-r}{p^\alpha}\right\rfloor\right) = \sum_{k=0}^{n}\binom{n}{k}(-1)^k f\left(\left\lfloor \frac{k-r}{p^\alpha}\right\rfloor\right) \sum_{d\mid(k-r,p^\alpha)} g(d)d$$

is at least

$$\nu=\left\lfloor\frac{n-p^{\alpha-1}-l(\delta_{\alpha,0}+\delta_{\alpha,1})}{\varphi(p^\alpha)}\right\rfloor-(l-1)\alpha.$$

We note in passing that in the case $\alpha>1$,

$$\mathrm{ord}_p(g(p^0))+\left\lfloor\frac{n-p^{\alpha-1}-\delta_{0,0}}{\varphi(p^\alpha)}\right\rfloor\ge\left\lfloor\frac{n-p^{\alpha-1}}{\varphi(p^\alpha)}\right\rfloor.$$

Now, since

$$\sum_{d\mid(k-r,p^\alpha)}g(d)d=p+\sum_{1<d\mid(k-r,p^\alpha)}(p-1)d=\sum_{d\mid(k-r,p^\alpha)}\varphi(d)p=(k-r,p^\alpha)p,$$

by the above the sum in (1.6) has p-adic order at least $\nu-1$. ■

Corollary 1.3. *Let p be a prime, and let α,β,a,n,r be integers for which*

$$\alpha>1,\quad \alpha\ge\beta\ge0,\quad a\equiv\ 1\ (\mathrm{mod}\,p^\alpha),\quad n\ge p^{\alpha-1},\quad r<p^\beta.$$

Then

$$(1.7)\qquad \sum_{k\equiv r\ (\mathrm{mod}\,p^\beta)}\binom{n}{k}(-1)^k a^{\lfloor(k-r)/p^\alpha\rfloor}\equiv 0\ (\mathrm{mod}\,p^{\lfloor(n-p^{\alpha-1}-\delta_{\beta,0})/\varphi(p^\alpha)\rfloor+\alpha-\beta}).$$

Proof. When $a=1$, (1.7) holds by Theorem 1.1 in the case $l=0$. So it suffices to show that

$$D:=\sum_{k\equiv r\ (\mathrm{mod}\,p^\beta)}\binom{n}{k}(-1)^k(a^{\lfloor(k-r)/p^\alpha\rfloor}-1)$$

is divisible by p^λ where

$$\lambda=\left\lfloor\frac{n-p^{\alpha-1}-\delta_{\beta,0}}{\varphi(p^\alpha)}\right\rfloor+\alpha-\beta.$$

Write $a=1+p^\alpha b$ with $b\in\mathbb{Z}$. Then

$$\begin{aligned}D&=\sum_{k\equiv r\ (\mathrm{mod}\,p^\beta)}\binom{n}{k}(-1)^k\sum_{0<l\le\lfloor(k-r)/p^\alpha\rfloor}\binom{\lfloor(k-r)/p^\alpha\rfloor}{l}(p^\alpha b)^l\\&=\sum_{0<l\le\lfloor(n-r)/p^\alpha\rfloor}p^{l\alpha}b^l\sum_{k\equiv r\ (\mathrm{mod}\,p^\beta)}\binom{n}{k}(-1)^k\binom{\lfloor(k-r)/p^\alpha\rfloor}{l}.\end{aligned}$$

For each $0<l\le\lfloor(n-r)/p^\alpha\rfloor$, applying Theorem 1.1 with $f(x)=\binom{x}{l}$ we find that

$$p^{l\alpha}\sum_{k\equiv r\ (\mathrm{mod}\,p^\beta)}\binom{n}{k}(-1)^k\binom{\lfloor(k-r)/p^\alpha\rfloor}{l}\equiv0\ (\mathrm{mod}\,p^\lambda).$$

Therefore $D\equiv0\ (\mathrm{mod}\,p^\lambda)$. This concludes the proof. ■

Let $a \in \mathbb{Z}$ be congruent to 1 modulo a prime p. By induction, $a^{p^\alpha} \equiv 1 \pmod{p^{\alpha+1}}$ for any $\alpha \in \mathbb{N}$. Let $n, r \in \mathbb{Z}$ and $n \geq p^{\alpha-1}$. If $\alpha \geq 2$, then by Corollary 1.3 in the case $\beta = \alpha$ we have

$$\sum_{k \equiv r \ (\mathrm{mod}\ p^\alpha)} \binom{n}{k} (-a)^k \equiv 0 \ (\mathrm{mod}\ p^{\lfloor (n-p^{\alpha-1})/\varphi(p^\alpha) \rfloor}). \tag{1.8}$$

By the binomial theorem, (1.8) is also valid with $\alpha = 0$. We remark that (1.8) also holds when $\alpha = 1$, as pointed out by Fleck (cf. [D, p. 274]).

In the next section we will provide some lemmas. Section 3 is devoted to the proof of Theorem 1.1.

2. Some lemmas. Let us recall the following well-known convolution identity of Chu and Vandermonde (see, e.g., [GKP, (5.27)]):

$$\sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} = \binom{x+y}{n} \quad \text{for all } n = 0, 1, 2, \ldots.$$

This can be seen by comparing the power series expansions of $(1+t)^x(1+t)^y$ and $(1+t)^{x+y}$.

LEMMA 2.1. *Let $f(x)$ be a function from $\mathbb{Z}$ to a field, and let $m, n \in \mathbb{Z}^+$. Then for any $r \in \mathbb{Z}$ we have*

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k f\left(\left\lfloor \frac{k-r}{m} \right\rfloor \right) = \sum_{k \equiv \bar{r} \ (\mathrm{mod}\ m)} \binom{n-1}{k} (-1)^{k-1} \Delta f\left(\frac{k-\bar{r}}{m} \right),$$

where $\bar{r} = r + m - 1$ and $\Delta f(x) = f(x+1) - f(x)$.

Proof. By the Chu–Vandermonde identity, for any $h \in \mathbb{N}$ we have

$$\sum_{k=0}^{h} \binom{n}{k} (-1)^k = (-1)^h \sum_{k=0}^{h} \binom{n}{k} \binom{-1}{h-k} = (-1)^h \binom{n-1}{h}.$$

Therefore

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k f\left(\left\lfloor \frac{k-r}{m} \right\rfloor \right) = \sum_{j \in \mathbb{Z}} c_j f(j),$$

where

$$\begin{aligned} c_j &= \sum_{\substack{k \in \mathbb{Z} \\ \lfloor (k-r)/m \rfloor = j}} \binom{n}{k} (-1)^k \\ &= \sum_{0 \leq k < (j+1)m+r} \binom{n}{k} (-1)^k - \sum_{0 \leq k < jm+r} \binom{n}{k} (-1)^k \\ &= (-1)^{(j+1)m+r-1} \binom{n-1}{(j+1)m+r-1} - (-1)^{jm+r-1} \binom{n-1}{jm+r-1}. \end{aligned}$$

(Note that $\binom{n-1}{i} \neq 0$ only for $i \in \{0, \ldots, n-1\}$.) So we have

$$\begin{aligned}\sum_{k=0}^{n} \binom{n}{k} (-1)^k f\left(\left\lfloor \frac{k-r}{m} \right\rfloor \right) \\ &= \sum_{j \in \mathbb{Z}} (-1)^{(j+1)m+r-1} \binom{n-1}{(j+1)m+r-1} f(j) \\ &\quad - \sum_{j \in \mathbb{Z}} (-1)^{jm+r-1} \binom{n-1}{jm+r-1} f(j) \\ &= \sum_{k \equiv \bar{r} \, (\mathrm{mod}\, m)} \binom{n-1}{k} (-1)^k \left(f\left(\frac{k-\bar{r}}{m} \right) - f\left(\frac{k-\bar{r}}{m} + 1 \right) \right) \\ &= \sum_{k \equiv \bar{r} \, (\mathrm{mod}\, m)} \binom{n-1}{k} (-1)^{k-1} \Delta f\left(\frac{k-\bar{r}}{m} \right).\end{aligned}$$

This proves the desired identity. ■

It is interesting to compare the identity in Lemma 2.1 with the following observation:

$$\sum_{\substack{0 \le k \le n \\ k \equiv r \, (\mathrm{mod}\, m)}} \Delta f\left(\frac{k-r}{m} \right) = f\left(\left\lfloor \frac{n-r}{m} \right\rfloor + 1 \right) - f\left(\left\lfloor \frac{-r-1}{m} \right\rfloor + 1 \right),$$

which appeared in the author's proof of [S03, Lemma 3.1].

LEMMA 2.2. *Let p be a prime and α be a positive integer. Then, for any $k = 0, 1, \ldots, \varphi(p^\alpha)$, we have*

$$\binom{\varphi(p^\alpha)}{k} \equiv \begin{cases} (-1)^k \pmod{p} & \textit{if } p^{\alpha-1} \mid k, \\ 0 \pmod{p} & \textit{otherwise.} \end{cases}$$

Proof. Let $k = k_0 + k_1 p + \cdots + k_{\alpha-1} p^{\alpha-1}$ be the p-adic expansion of k, where $k_0, k_1, \ldots, k_{\alpha-1} \in \{0, \ldots, p-1\}$. By a well-known theorem of E. Lucas (see, e.g., [HS]),

$$\begin{aligned}\binom{\varphi(p^\alpha)}{k} &= \binom{\sum_{0 \le j < \alpha-1} 0 p^j + (p-1)p^{\alpha-1}}{\sum_{0 \le j < \alpha-1} k_j p^j + k_{\alpha-1} p^{\alpha-1}} \\ &\equiv \binom{p-1}{k_{\alpha-1}} \prod_{0 \le j < \alpha-1} \binom{0}{k_j} \pmod{p}.\end{aligned}$$

If $p^{\alpha-1}\nmid k$, then $k_j>0$ for some $j<\alpha-1$, and hence $\binom{\varphi(p^\alpha)}{k}\equiv 0 \pmod p$. When $p^{\alpha-1}\mid k$, we have $k_j=0$ for all $j<\alpha-1$, and thus

$$\begin{aligned}\binom{\varphi(p^\alpha)}{k}\equiv\binom{p-1}{k_{\alpha-1}}&=\prod_{0<s\le k_{\alpha-1}}\frac{p-s}{s}\pmod p\\ &\equiv(-1)^{k_{\alpha-1}}\equiv(-1)^{p^{\alpha-1}k_{\alpha-1}}=(-1)^k\pmod p.\end{aligned}$$

This completes the proof. ■

3. Proof of Theorem 1.1. We use induction on $w_l(\alpha,\beta):=l(\alpha+1)+\beta$.

In the case $w_l(\alpha,\beta)=0$ (i.e., $l=\beta=0$), the desired result is trivial because $\sum_{k=0}^n\binom{n}{k}(-1)^k=(1-1)^n=0$ for all $n\in\mathbb{Z}^+$.

Let w be a positive integer, and assume that the desired result holds whenever $w_l(\alpha,\beta)<w$. Now we deal with the case $w_l(\alpha,\beta)=w$.

Case 1: $\beta=0$. In this case, l is positive. Let $n\in\mathbb{N}$, $n\ge p^{\alpha-1}$, $r\in\mathbb{Z}$ and $\bar r=r+p^\alpha-1$. By Lemma 2.1,

$$\begin{aligned}\sum_{k=0}^n\binom{n}{k}(-1)^k f\left(\left\lfloor\frac{k-r}{p^\alpha}\right\rfloor\right)\\ =\sum_{k\equiv\bar r\ (\mathrm{mod}\ p^\alpha)}\binom{n-1}{k}(-1)^{k-1}\Delta f\left(\frac{k-\bar r}{p^\alpha}\right).\end{aligned}\tag{3.1}$$

Clearly $\Delta f(x)$ is a polynomial of degree at most $l-1$, and $\Delta f(a)\in\mathbb{Z}_p$ for all $a\in\mathbb{Z}$. Also, $w_{l-1}(\alpha,\alpha)<w_l(\alpha,0)=w$. In view of (3.1) and the induction hypothesis,

$$\begin{aligned}\mathrm{ord}_p&\left(\sum_{k=0}^n\binom{n}{k}(-1)^k f\left(\left\lfloor\frac{k-r}{p^\alpha}\right\rfloor\right)\right)\\ &\ge\left\lfloor\frac{(n-1)-p^{\alpha-1}-(l-1)}{\varphi(p^\alpha)}\right\rfloor-(l-2)\alpha-\alpha\\ &=\left\lfloor\frac{n-p^{\alpha-1}-l}{\varphi(p^\alpha)}\right\rfloor-(l-1)\alpha-0.\end{aligned}$$

(Note that this is trivial if $n-1<p^{\alpha-1}$.) Similarly, when $\alpha>1$, by (3.1) and the induction hypothesis we have

$$\begin{aligned}\mathrm{ord}_p&\left(\sum_{k=0}^n\binom{n}{k}(-1)^k f\left(\left\lfloor\frac{k-r}{p^\alpha}\right\rfloor\right)\right)\\ &\ge\left\lfloor\frac{(n-1)-p^{\alpha-1}-\delta_{\alpha,0}}{\varphi(p^\alpha)}\right\rfloor-(l-2)\alpha-\alpha\\ &=\left\lfloor\frac{n-p^{\alpha-1}-\delta_{0,0}}{\varphi(p^\alpha)}\right\rfloor-(l-1)\alpha-0.\end{aligned}$$

Case 2: $0<\beta\le\alpha$. If $l=0$ (i.e., $f(x)$ is constant), then $w_l(\beta,\beta)=w_l(\alpha,\beta)=w$ and it suffices to handle the case $\alpha=\beta$. In fact, when $l=0$, $n\ge p^{\alpha-1}$ and $r\in\mathbb{Z}$, provided that

$$\sum_{k\equiv r\,(\mathrm{mod}\,p^{\beta})}\binom{n}{k}(-1)^k f\left(\frac{k-r}{p^{\beta}}\right)\in p^{\lfloor (n-p^{\beta-1})/\varphi(p^{\beta})\rfloor}\mathbb{Z}_p$$

we have

$$\sum_{k\equiv r\,(\mathrm{mod}\,p^{\beta})}\binom{n}{k}(-1)^k f\left(\left\lfloor\frac{k-r}{p^{\alpha}}\right\rfloor\right)\in p^{\lfloor (n-p^{\alpha-1})/\varphi(p^{\alpha})\rfloor-(0-1)\alpha-\beta}\mathbb{Z}_p,$$

because

$$\frac{n-p^{\beta-1}}{\varphi(p^{\beta})}-\frac{n-p^{\alpha-1}}{\varphi(p^{\alpha})}=\frac{n}{p^{\alpha-1}}\sum_{0\le s<\alpha-\beta}p^s\ge\alpha-\beta.$$

Below we simply let $(l-1)\alpha+\beta\ge 0$ (i.e., $\alpha=\beta$ if $l=0$).

Let us use induction on $n\ge p^{\alpha-1}$. The desired result is trivial when $n-p^{\alpha-1}<\varphi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}$.

Below we let $n\ge p^{\alpha}$ and assume that the desired result holds for smaller values of n not less than $p^{\alpha-1}$. Note that $n'=n-\varphi(p^{\beta})<n$ and also $n'\ge n-\varphi(p^{\alpha})\ge p^{\alpha-1}$.

Let r be any integer, and set

$$S=\sum_{k\equiv r\,(\mathrm{mod}\,p^{\beta})}\binom{n}{k}(-1)^k f\left(\left\lfloor\frac{k-r}{p^{\alpha}}\right\rfloor\right). \tag{3.2}$$

By the Chu–Vandermonde identity,

$$\begin{aligned}S&=\sum_{k\equiv r\,(\mathrm{mod}\,p^{\beta})}\sum_{j=0}^{\varphi(p^{\beta})}\binom{\varphi(p^{\beta})}{j}\binom{n'}{k-j}(-1)^k f\left(\left\lfloor\frac{k-r}{p^{\alpha}}\right\rfloor\right)\\&=\sum_{j=0}^{\varphi(p^{\beta})}\binom{\varphi(p^{\beta})}{j}\sum_{k\equiv r\,(\mathrm{mod}\,p^{\beta})}\binom{n'}{k-j}(-1)^k f\left(\left\lfloor\frac{k-j-(r-j)}{p^{\alpha}}\right\rfloor\right)\\&=\sum_{j=0}^{\varphi(p^{\beta})}\binom{\varphi(p^{\beta})}{j}(-1)^j S_j,\end{aligned}$$

where

$$S_j=\sum_{k\equiv r-j\,(\mathrm{mod}\,p^{\beta})}\binom{n'}{k}(-1)^k f\left(\left\lfloor\frac{k-(r-j)}{p^{\alpha}}\right\rfloor\right). \tag{3.3}$$

For any $j=0,1,\dots,\varphi(p^{\beta})$, by the induction hypothesis we have

$$\mathrm{ord}_p(S_j)\ge\gamma=\left\lfloor\frac{n'-p^{\alpha-1}-l\delta_{\alpha,1}}{\varphi(p^{\alpha})}\right\rfloor-(l-1)\alpha-\beta,$$

and Lemma 2.2 yields

$$\binom{\varphi(p^\beta)}{j} \equiv \begin{cases} (-1)^j \pmod p & \text{if } p^{\beta-1} \mid j, \\ 0 \pmod p & \text{if } p^{\beta-1} \nmid j. \end{cases}$$

Thus, if $\gamma \ge 0$ then

$$S \equiv \sum_{j=0}^{p-1} \binom{\varphi(p^\beta)}{p^{\beta-1}j} (-1)^{p^{\beta-1}j} S_{p^{\beta-1}j} \equiv \sum_{j=0}^{p-1} S_{p^{\beta-1}j} \pmod{p^{\gamma+1}}.$$

Observe that

$$\sum_{j=0}^{p-1} S_{p^{\beta-1}j} = \sum_{k\equiv r \pmod{p^{\beta-1}}} \binom{n'}{k} (-1)^k f\left(\left\lfloor \frac{k-(r-p^{\beta-1}j_k)}{p^\alpha} \right\rfloor\right),$$

where j_k is the unique integer in $\{0,\dots,p-1\}$ with $p^\beta \mid k-(r-p^{\beta-1}j_k)$. For $k \equiv r \pmod{p^{\beta-1}}$, clearly

$$\frac{k-r+p^{\beta-1}j_k}{p^\beta} = \frac{k-r'-p^{\beta-1}(p-1-j_k)}{p^\beta} = \left\lfloor \frac{k-r'}{p^\beta} \right\rfloor$$

where $r' = r-\varphi(p^\beta)$. Therefore $\sum_{j=0}^{p-1} S_{p^{\beta-1}j} = S'$, where

$$S' = \sum_{k\equiv r' \pmod{p^{\beta-1}}} \binom{n'}{k} (-1)^k f\left(\left\lfloor \frac{k-r'}{p^\alpha} \right\rfloor\right). \tag{3.4}$$

From the above it follows that

$$\operatorname{ord}_p(S-S') \ge \gamma+1 \ge \left\lfloor \frac{n-p^{\alpha-1}-l\delta_{\alpha,1}}{\varphi(p^\alpha)} \right\rfloor - (l-1)\alpha - \beta.$$

Let $l_0 = l$ if $\alpha = 1$, and $l_0 = \min\{l, \delta_{\beta-1,0}\}$ if $\alpha > 1$. As $w_l(\alpha,\beta-1) < w_l(\alpha,\beta) = w$, by the induction hypothesis we have

$$\begin{aligned} \operatorname{ord}_p(S') &\ge \left\lfloor \frac{n'-p^{\alpha-1}-l_0}{\varphi(p^\alpha)} \right\rfloor - (l-1)\alpha - (\beta-1) \\ &\ge \left\lfloor \frac{n-p^{\alpha-1}-l\delta_{\alpha,1}}{\varphi(p^\alpha)} \right\rfloor - (l-1)\alpha - \beta. \end{aligned}$$

(Note that if $\alpha > 1 = \delta_{\beta-1,0}$ then $\beta = 1 < \alpha$ and hence $n'-1+\varphi(p^\alpha) \ge n'+\varphi(p^\beta) = n$.)

Combining the above we finally obtain

$$\operatorname{ord}_p(S) = \operatorname{ord}_p((S-S')+S') \ge \left\lfloor \frac{n-p^{\alpha-1}-l\delta_{\alpha,1}}{\varphi(p^\alpha)} \right\rfloor - (l-1)\alpha - \beta.$$

Since $\delta_{\beta,0} = 0$, this concludes the induction step in Case 2.

The proof of Theorem 1.1 is now complete. ∎

Acknowledgments. The work was done during the author's visit to the University of California at Irvine, and he would like to thank Prof. Daqing Wan for the kind invitation. The author is also indebted to the referee for helpful comments.

References

[D] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York, 1999.

[GKP] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, Reading, MA, 1994.

[H] C. Helou, *Norm residue symbol and cyclotomic units*, Acta Arith. 73 (1995), 147–188; Corrigendum, ibid. 98 (2001), 311.

[HS] H. Hu and Z. W. Sun, *An extension of Lucas' theorem*, Proc. Amer. Math. Soc. 129 (2001), 3471–3478.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, New York, 1990.

[LW] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed., Cambridge Univ. Press, Cambridge, 2001.

[SS] Z. H. Sun and Z. W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. 60 (1992), 371–388.

[S02] Z. W. Sun, *On the sum* $\sum_{k\equiv r \pmod m}\binom{n}{k}$ *and related congruences*, Israel J. Math. 128 (2002), 135–156.

[S03] —, *General congruences for Bernoulli polynomials*, Discrete Math. 262 (2003), 253–276.

[W] C. S. Weisman, *Some congruences for binomial coefficients*, Michigan Math. J. 24 (1977), 141–151.

Department of Mathematics (and Institute of Mathematical Science)
Nanjing University
Nanjing 210093, People's Republic of China
E-mail: zwsun@nju.edu.cn
http://pweb.nju.edu.cn/zwsun

Received on 3.7.2005
and in revised form on 19.12.2005 (5028)