Int. J. Number Theory 4(2008), no. 2, 155–170.

LUCAS-TYPE CONGRUENCES FOR CYCLOTOMIC ψ-COEFFICIENTS

Zhi-Wei Sun[1] and Daqing Wan[2]

[1]Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

[2]Department of Mathematics, University of California
Irvine, CA 92697-3875, USA
dwan@math.uci.edu
http://math.uci.edu/∼dwan

Abstract. Let p be any prime and a be a positive integer. For $l, n \in \{0, 1, \dots\}$ and $r \in \mathbb{Z}$, the normalized cyclotomic ψ-coefficient

$$\left\{ {n \atop r} \right\}_{l,p^a} := p^{-\left\lfloor \frac{n-p^{a-1}-lp^a}{p^{a-1}(p-1)} \right\rfloor} \sum_{k \equiv r \pmod{p^a}} (-1)^k \binom{n}{k} \binom{\frac{k-r}{p^a}}{l}$$

is known to be an integer. In this paper, we show that this coefficient behaves like binomial coefficients and satisfies some Lucas-type congruences. This implies that a congruence of Wan is often optimal, and two conjectures of Sun and Davis are true.

1. Introduction

As usual, the binomial coefficient $\binom{x}{0}$ is regarded as 1. For $k \in \mathbb{Z}^+ = \{1, 2, \dots\}$, we define

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}$$

Key words and phrases. Binomial coefficients, cyclotomic ψ-coefficients, Lucas-type congruences.

2000 *Mathematics Subject Classification.* Primary 11B65; Secondary 05A10, 11A07, 11R18, 11R23, 11S05.

The first author is supported by the National Science Fund for Distinguished Young Scholars in China (grant no. 10425103). The second author is partially supported by NSF.

and adopt the convention $\binom{x}{-k} = 0$.

The following remarkable result was established by A. Fleck (cf. [D, p. 274]) in the case $l = 0$ and $a = 1$, by C. S. Weisman [We] in the case $l = 0$, and by D. Wan [W] in the general case motivated by his study of the ψ-operator related to Iwasawa theory.

Theorem 1.0. *Let p be a prime and $a \in \mathbb{Z}^+$. Then, for any $l, n \in \mathbb{N} = \{0, 1, 2, \dots\}$ and $r \in \mathbb{Z}$, we have*

$$C_{l,p^a}(n,r) := \sum_{k \equiv r \pmod{p^a}} (-1)^k \binom{n}{k} \binom{(k-r)/p^a}{l} \in p^{\lfloor \frac{n-p^{a-1}-lp^a}{\phi(p^a)} \rfloor} \mathbb{Z},$$

where ϕ is Euler's totient function and $\lfloor \cdot \rfloor$ is the greatest integer function.

The above integers $C_{l,p^a}(n,r)$ $(l = 0, 1, \dots)$ arise naturally as the coefficients of the ψ-operator acting on the cyclotomic φ-module. We briefly review this connection. Let $A = \mathbb{Z}_p[\![T]\!]$ be the formal power series ring over the ring of p-adic integers. The $\mathbb{Z}_p$-linear Frobenius map φ acts on the ring A by

$$\varphi(T) = (1+T)^p - 1.$$

Equivalently, $\varphi(1+T) = (1+T)^p$. This map φ is injective and of degree p. This implies that $\{1, T, \dots, T^{p-1}\}$ and $\{1, 1+T, \dots, (1+T)^{p-1}\}$ are bases of A over the subring $\varphi(A)$. The operator $\psi : A \to A$ is defined by

$$\psi(x) = \psi\left(\sum_{i=0}^{p-1} (1+T)^i \varphi(x_i)\right) = x_0 = \frac{1}{p}\varphi^{-1}(\mathrm{Tr}_{A/\varphi(A)}(x)),$$

where $x : A \to A$ denotes the multiplication by x as a $\varphi(A)$-linear map. Note that ψ is a one-sided inverse of φ, namely $\psi \circ \varphi = I \neq \varphi \circ \psi$. The pair (A, φ) is the cyclotomic φ-module. The ψ-operator plays a basic role in L-functions of F-crystals, Fontaine's theory of (φ, Γ)-modules, Iwasawa theory, p-adic L-functions and p-adic Langlands correspondence.

For a positive integer a, let ψ^a be the a-th iteration of ψ acting on the ring A. As mentioned in [W, Lemma 4.2], it is easy to check that for any $n \in \mathbb{N}$ and $r \in \mathbb{Z}$ we have

$$\psi^a\left(\frac{T^n}{(1+T)^r}\right) = (-1)^n \sum_{l=0}^{\infty} T^l C_{l,p^a}(n,r).$$

To understand the ψ^a-action, it is thus essential to understand the p-adic property of the cyclotomic ψ-coefficients $C_{l,p^a}(n,r)$ $(l = 0, 1, \dots)$. This was the main motivation in [W], where the congruence in Theorem 1.0 was proved. Note that a somewhat weaker estimate for the cyclotomic ψ-coefficient $C_{l,p}(n,0)$ was independently given by Colmez [C, Lemma 1.7] in his work on p-adic Langlands correspondence. The cyclotomic ψ-coefficient also arises from computing the homotopy p-exponent of the special unitary group SU(n) (cf. [DS]).

To understand how sharp the congruence in Theorem 1.0 is, we define the *normalized cyclotomic ψ-coefficient*

$$\left\{ \begin{matrix} n \\ r \end{matrix} \right\}_{l,p^a} := p^{-\left\lfloor \frac{n-p^{a-1}-lp^a}{\phi(p^a)} \right\rfloor} \sum_{k \equiv r \pmod{p^a}} (-1)^k \binom{n}{k} \binom{(k-r)/p^a}{l}. \qquad (1.0)$$

Surprisingly it has many properties similar to properties of the usual binomial coefficients.

The classical Lucas theorem states that if p is a prime and n, r, s, t are nonnegative integers with $s, t < p$ then

$$\binom{pn+s}{pr+t} \equiv \binom{n}{r}\binom{s}{t} \pmod{p}.$$

It can also be interpreted as a result about cellular automata (cf. [Gr]). There are various extensions of this fundamental theorem, see, e.g., [DW], [HS], [P] and [SD]. Our first result is the following new analogue of Lucas' theorem.

Theorem 1.1. *Let p be any prime, and let $r \in \mathbb{Z}$ and $a, l, n, s, t \in \mathbb{N}$ with $a \geqslant 2$ and $s, t < p$. Then we have the congruence*

$$\left\{ \begin{matrix} pn+s \\ pr+t \end{matrix} \right\}_{l,p^{a+1}} \equiv (-1)^t \binom{s}{t} \left\{ \begin{matrix} n \\ r \end{matrix} \right\}_{l,p^a} \pmod{p}; \qquad (1.1)$$

in other words,

$$\begin{aligned} & p^{-\left\lfloor \frac{n-p^{a-1}-lp^a}{\phi(p^a)} \right\rfloor} \sum_{k \equiv r \pmod{p^a}} (-1)^{pk} \binom{pn+s}{pk+t} \binom{(k-r)/p^a}{l} \\ \equiv & p^{-\left\lfloor \frac{n-p^{a-1}-lp^a}{\phi(p^a)} \right\rfloor} \sum_{k \equiv r \pmod{p^a}} (-1)^k \binom{n}{k}\binom{s}{t}\binom{(k-r)/p^a}{l} \pmod{p}. \end{aligned}$$

Remark 1.1. Theorem 1.1 in the case $l = 0$ is equivalent to Theorem 1.7 of Z. W. Sun and D. M. Davis [SD]. Under the same conditions of Theorem 1.1, Sun and Davis [SD] established another congruence of Lucas' type:

$$\begin{aligned} & \frac{1}{\lfloor n/p^{a-1} \rfloor !} \sum_{k \equiv r \pmod{p^a}} (-1)^{pk} \binom{pn+s}{pk+t} \left(\frac{k-r}{p^{a-1}}\right)^l \\ \equiv & \frac{1}{\lfloor n/p^{a-1} \rfloor !} \sum_{k \equiv r \pmod{p^a}} (-1)^k \binom{n}{k}\binom{s}{t} \left(\frac{k-r}{p^{a-1}}\right)^l \pmod{p}. \end{aligned}$$

Note that $a \geqslant 2$ is assumed in Theorem 1.1. To get a complete result, we need to handle the case $a = 1$ as well, which is more subtle. In fact, concerning the exceptional case $a = 1$, Sun and Davis [SD] made the following conjecture (for $l = 0$). Note also that [S02] contains a closed formula for $\left\{ {n \atop r} \right\}_{0,2^2}$ with $n \in \mathbb{N}$ and $r \in \mathbb{Z}$.

Conjecture ([SD, Conjecture 1.2])**.** *Let p be any prime, and let $n \in \mathbb{N}$, $r \in \mathbb{Z}$ and $s \in \{0, \ldots, p-1\}$. If $p \mid n$ or $p - 1 \nmid n - 1$, then*

$$\left\{ {pn+s \atop pr+t} \right\}_{0,p^2} \equiv (-1)^t \binom{s}{t} \left\{ {n \atop r} \right\}_{0,p} \pmod p$$

for every $t = 0, \ldots, p-1$. When $p \nmid n$ and $p-1 \mid n-1$, the least nonnegative residue of $\left\{ {pn+s \atop pr+t} \right\}_{0,p^2}$ modulo p does not depend on r for each integer $t \in (s, p-1]$, moreover these residues form a permutation of $1, \ldots, p-1$ if $s = 0$ and $n \neq 1$.

We get the following general result for $a = 1$ and all $l \in \mathbb{N}$ from which the above conjecture follows.

Theorem 1.2. *Let p be a prime, $l, n \in \mathbb{N}$, $r \in \mathbb{Z}$ and $s, t \in \{0, \ldots, p-1\}$. If $p \mid n$, or $p - 1 \nmid n - l - 1$, or $s = p - 1$, or $s = 2t$ and $p \neq 2$, then*

$$\left\{ {pn+s \atop pr+t} \right\}_{l,p^2} \equiv (-1)^t \binom{s}{t} \left\{ {n \atop r} \right\}_{l,p} \pmod p. \tag{1.2}$$

When $p \nmid n$, $p - 1 \mid n - l - 1$ and $t \in (s, p-1]$, we have

$$\left\{ {pn+s \atop pr+t} \right\}_{l,p^2} \equiv \begin{cases} (-1)^{s+\frac{n-l-1}{p-1}} \frac{n}{t} \binom{\frac{n-l-1}{p-1}-1}{l} \Big/ \binom{t-1}{s} \pmod p & \text{if } n > l+1, \\ 0 \pmod p & \text{if } n \leqslant l+1. \end{cases} \tag{1.3}$$

From Theorem 1.2 we can also deduce the following result conjectured by Sun and Davis (cf. [SD, Remark 1.4]) as a complement to Theorem 1.5 of [SD].

Corollary 1.3. *Let p be any prime, and let $l, n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then*

$$T_{l,2}^{(p)}(n, r) \equiv (-1)^{\{r\}_p} \binom{\{n\}_p}{\{r\}_p} T_{l,1}^{(p)}\left(\left\lfloor \frac{n}{p} \right\rfloor, \left\lfloor \frac{r}{p} \right\rfloor \right) \pmod p, \tag{1.4}$$

where

$$T_{l,a}^{(p)}(n, r) := \frac{l! p^l}{\lfloor n/p^{a-1} \rfloor !} \sum_{k \equiv r \pmod{p^a}} (-1)^k \binom{n}{k} \binom{(k-r)/p^a}{l} \text{ for } a \in \mathbb{Z}^+,$$

and we use $\{x\}_m$ to denote the least nonnegative residue of an integer x modulo $m \in \mathbb{Z}^+$.

When $s = t = 0$, the Lucas-type congruences in Theorems 1.1 and 1.2 can be further improved unless $p = 2$ and $2 \nmid n$. Namely, we have the following result.

Theorem 1.4. *Let p be a prime, and let $a, n \in \mathbb{Z}^+$, $l \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then*

$$\mathrm{ord}_p\left(\left\{ {pn \atop pr} \right\}_{l,p^{a+1}} - \left\{ {n \atop r} \right\}_{l,p^a}\right) \geqslant \frac{p-1}{p}(2\mathrm{ord}_p(n) + \delta), \tag{1.5}$$

where $\mathrm{ord}_p(n) = \sup\{m \in \mathbb{N} : p^m \mid n\}$ *and*

$$\delta = \begin{cases} 0 & \text{if } p = 2, \\ 1 & \text{if } p = 3, \\ 2 & \text{if } p \geqslant 5. \end{cases}$$

Remark 1.2. Let p be a prime, $a, n \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$. Substituting $p^{a-1}n$ for n in (1.5), we obtain that

$$\begin{aligned} &\mathrm{ord}_p\left(\left\{ {p^a n \atop pr} \right\}_{l,p^{a+1}} - \left\{ {p^{a-1} n \atop r} \right\}_{l,p^a}\right) \\ \geqslant &\frac{p-1}{p}(2\mathrm{ord}_p(p^{a-1}n) + \delta) \geqslant \frac{p-1}{p}(2(a-1) + \delta). \end{aligned}$$

On the other hand, in the case $l = 0$ Sun and Davis [SD, Theorem 3.1] proved the congruence

$$\left\{ {p^a n \atop pr} \right\}_{0,p^{a+1}} \equiv \left\{ {p^{a-1} n \atop r} \right\}_{0,p^a} \pmod{p^{(2-\delta_{p,2})(a-1)}}$$

(where the Kronecker symbol $\delta_{i,j}$ takes 1 or 0 according as $i = j$ or not) and they conjectured that the exponent $(2 - \delta_{p,2})(a-1)$ can be replaced by $2a - \delta_{p,3} = 2(a-1) + \delta$ when $p \neq 2$.

Here is one more result, which shows that Theorem 1.0 is often sharp.

Theorem 1.5. *Let p be any prime, and let $a \in \mathbb{Z}^+$ and $l \in \mathbb{N}$. If $n = (l+1)p^{a-1} - 1 + m\phi(p^a)$ for some $m \in \mathbb{Z}^+$, then*

$$\left\{ {n \atop r} \right\}_{l,p^a} \equiv (-1)^{m-1}\binom{m-1}{l} \pmod{p} \quad \text{for all } r \in \mathbb{Z}. \tag{1.6}$$

Remark 1.3. Theorem 1.5 in the case $l = 0$ was first obtained by Weisman [We] in 1977. Given $l \in \mathbb{Z}^+$, for any integer $m > l$ with $m \equiv l + 1 \pmod{p^{\lfloor \log_p l \rfloor + 1}}$ we have $\binom{m-1}{l} \equiv \binom{l}{l} = 1 \pmod{p}$ by Lucas' theorem.

In the next section we include a new proof of Theorem 1.0 of a combinatorial nature. In Section 3 we will show Theorem 1.1. Theorems 1.2 and Corollary 1.3 will be proved in Section 4. Section 5 is devoted to proofs of Theorems 1.4 and 1.5. Instead of the ψ-operator, we use combinatorial arguments throughout this paper.

2. A combinatorial proof of Theorem 1.0

Lemma 2.1. *Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then*

$$\left\lfloor\frac{a}{m}\right\rfloor+\left\lfloor\frac{b}{m}\right\rfloor+1-\left\lfloor\frac{a+b+1}{m}\right\rfloor\in\{0,1\}. \tag{2.1}$$

Proof. Observe that

$$\left\lfloor\frac{a+b+1}{m}\right\rfloor=\left\lfloor\frac{a}{m}\right\rfloor+\left\lfloor\frac{b}{m}\right\rfloor+\left\lfloor\frac{\{a\}_m+\{b\}_m+1}{m}\right\rfloor.$$

The last term is obviously either 0 or 1, so (2.1) follows. □

Lemma 2.2. *Let $l, m, n \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$. Then we have*

$$\sum_{k\equiv r\ (\mathrm{mod}\ m)}(-1)^k\binom{n}{k}\binom{(k-r)/m}{l}-\binom{\lfloor (n-r)/m\rfloor}{l}\sum_{m\mid k-r}(-1)^k\binom{n}{k}$$
$$=-\sum_{j=0}^{n-1}\binom{n}{j}\sum_{m\mid i-r}(-1)^i\binom{j}{i}\sum_{m\mid k-r_j}(-1)^k\binom{n-j-1}{k}\binom{(k-r_j)/m}{l-1},$$

where $r_j = r - j + m - 1$.

Proof. Note that $\binom{x+1}{l}-\binom{x}{l}=\binom{x}{l-1}$. So Lemma 2.2 is just Lemma 3.3 of [DS] in the case $f(x)=\binom{x}{l}$. □

Proof of Theorem 1.0. We use induction on $l + n$.

The case $n = 0$ is trivial. The case $l = 0$ was handled by Weisman [W] (see also [S06]).

Now let l and n be positive, and assume that $\left\{{n' \atop r'}\right\}_{l',p^a} \in \mathbb{Z}$ whenever $l', n' \in \mathbb{N}$, $l' + n' < l + n$ and $r' \in \mathbb{Z}$. By Lemma 2.2,

$$\left\{{n \atop r}\right\}_{l,p^a}-\binom{\lfloor\frac{n-r}{p^a}\rfloor}{l}p^{\lfloor\frac{n-p^{a-1}}{\phi(p^a)}\rfloor-\lfloor\frac{n-p^{a-1}-lp^a}{\phi(p^a)}\rfloor}\left\{{n \atop r}\right\}_{0,p^a}$$
$$=-\sum_{j=0}^{n-1}\binom{n}{j}p^{c_j}\left\{{j \atop r}\right\}_{0,p^a}\left\{{n-j-1 \atop r_j}\right\}_{l-1,p^a}$$

where

$$c_j=\left\lfloor\frac{j-p^{a-1}}{\phi(p^a)}\right\rfloor+\left\lfloor\frac{n-j-1-p^{a-1}-(l-1)p^a}{\phi(p^a)}\right\rfloor-\left\lfloor\frac{n-p^{a-1}-lp^a}{\phi(p^a)}\right\rfloor$$
$$=\left\lfloor\frac{a_j}{\phi(p^a)}\right\rfloor+\left\lfloor\frac{b_j}{\phi(p^a)}\right\rfloor+1-\left\lfloor\frac{a_j+b_j+1}{\phi(p^a)}\right\rfloor\geqslant 0\quad\text{(by Lemma 2.1)}$$

with $a_j = j - p^{a-1}$ and $b_j = n - j - 1 - lp^a$. For any $j = 0, 1, \dots, n-1$, both $\left\{ {j \atop r} \right\}_{0,p^a}$ and $\left\{ {n-j-1 \atop r_j} \right\}_{l-1,p^a}$ are integers by the induction hypothesis. Therefore $\left\{ {n \atop r} \right\}_{l,p^a} \in \mathbb{Z}$ by the above.

The induction proof of Theorem 1.0 is now complete. □

Remark 2.1. Our proof of Theorem 1.0 can be refined to show the following recurrence with respect to l: If p is a prime, $a, l, n \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$, then

$$\left\{ {n \atop r} \right\}_{l,p^a} \equiv -\sum_{j \in J} \binom{n}{j} \left\{ {j \atop r} \right\}_{0,p^a} \left\{ {n-j-1 \atop r-j+p^a-1} \right\}_{l-1,p^a} \pmod{p},$$

where

$$J = \left\{ 0 \leqslant j \leqslant n-1 : \ \{j - p^{a-1}\}_{\phi(p^a)} \geqslant \{n - (l+1)p^{a-1}\}_{\phi(p^a)} \right\}.$$

3. Proof of Theorem 1.1

We can deduce Theorem 1.1 by using Remark 2.1 along with Theorem 1.7 of [SD]. However, we will present a self-contained proof by a new approach.

Lemma 3.1. *Let $d, q \in \mathbb{Z}^+$, $n \in \mathbb{N}$, $r, t \in \mathbb{Z}$ and $t < d$. Then*

$$\sum_{j \in \mathbb{N}} (-1)^j \bigg(\sum_{d \mid k-t} (-1)^k \binom{n}{k} \binom{(k-t)/d}{j} \bigg) \bigg(\sum_{q \mid i-r} (-1)^i \binom{j}{i} \binom{(i-r)/q}{l} \bigg)$$
$$= \sum_{k \equiv dr+t \,(\mathrm{mod}\ dq)} (-1)^k \binom{n}{k} \binom{(k-dr-t)/(dq)}{l}. \tag{3.1}$$

Proof. Since $t < d$, we have $(k-t)/d \in \mathbb{N}$ for those $k \in \{0, \dots, n\}$ with $k \equiv t \pmod{d}$. Let S denote the left-hand side of (3.1). Then

$$S = \sum_{k \equiv t \,(\mathrm{mod}\ d)} (-1)^k \binom{n}{k} \sum_{q \mid i-r} \binom{(i-r)/q}{l} \sum_{j \geqslant i} (-1)^{j-i} \binom{(k-t)/d}{j} \binom{j}{i}.$$

The inner-most sum has a well-known evaluation (see, e.g., [G, (3.47)] or [GKP, (5.24)]); in fact, it coincides with

$$\binom{(k-t)/d}{i} \sum_{j \geqslant i} (-1)^{j-i} \binom{(k-t)/d - i}{j-i} = \delta_{i,(k-t)/d}.$$

Therefore

$$\begin{aligned} S &= \sum_{k\equiv t\,(\mathrm{mod}\ d)} (-1)^k \binom{n}{k} \sum_{q\mid i-r} \binom{(i-r)/q}{l} \delta_{i,(k-t)/d} \\ &= \sum_{k\equiv dr+t\,(\mathrm{mod}\ dq)} (-1)^k \binom{n}{k} \binom{((k-t)/d-r)/q}{l} \\ &= \sum_{k\equiv dr+t\,(\mathrm{mod}\ dq)} (-1)^k \binom{n}{k} \binom{(k-dr-t)/(dq)}{l}. \end{aligned}$$

This concludes the proof. □

Lemma 3.2. *Let p be a prime, and let $a \in \mathbb{Z}^+$ and $l, n \in \mathbb{N}$. Let $r \in \mathbb{Z}$ and $s, t \in \{0, 1, \ldots, p-1\}$. If $n = 0$ or $s = p-1$ or $\phi(p^a) \nmid n-(l+1)p^{a-1}$, then* (1.1) *holds; otherwise,*

$$\begin{aligned} &\left\{ {pn+s \atop pr+t} \right\}_{l,p^{a+1}} - (-1)^t \binom{s}{t} \left\{ {n \atop r} \right\}_{l,p^a} \\ \equiv &(-1)^{n-1} \left\{ {n-1 \atop r} \right\}_{l,p^a} \left\{ {pn+s \atop t} \right\}_{n-1,p} \pmod p. \end{aligned} \tag{3.2}$$

Proof. Applying Lemma 3.1 with $d = p$ and $q = p^a$, we find that

$$\begin{aligned} &\sum_{j\in\mathbb{N}} (-1)^j p^{\lfloor \frac{pn+s-1-jp}{\phi(p)} \rfloor} \left\{ {pn+s \atop t} \right\}_{j,p} p^{\lfloor \frac{j-p^{a-1}-lp^a}{\phi(p^a)} \rfloor} \left\{ {j \atop r} \right\}_{l,p^a} \\ &= p^{\lfloor \frac{pn+s-p^a-lp^{a+1}}{\phi(p^{a+1})} \rfloor} \left\{ {pn+s \atop pr+t} \right\}_{l,p^{a+1}}. \end{aligned}$$

Thus

$$\left\{ {pn+s \atop pr+t} \right\}_{l,p^{a+1}} = \sum_{0\leqslant j\leqslant \lfloor \frac{pn+s}{p} \rfloor = n} (-1)^j p^{a_j} \left\{ {j \atop r} \right\}_{l,p^a} \left\{ {pn+s \atop t} \right\}_{j,p},$$

where

$$\begin{aligned} a_j &= \left\lfloor \frac{pn+s-1-jp}{\phi(p)} \right\rfloor + \left\lfloor \frac{j-p^{a-1}-lp^a}{\phi(p^a)} \right\rfloor - \left\lfloor \frac{pn+s-p^a-lp^{a+1}}{\phi(p^{a+1})} \right\rfloor \\ &= \left\lfloor \frac{p(n-j)+s-1}{\phi(p)} \right\rfloor + \left\lfloor \frac{j-p^{a-1}-lp^a}{\phi(p^a)} \right\rfloor - \left\lfloor \frac{n-p^{a-1}-lp^a}{\phi(p^a)} \right\rfloor. \end{aligned}$$

Observe that

$$\begin{aligned} p^{a_n}\left\{\begin{matrix} pn+s \\ t \end{matrix}\right\}_{n,p} =& \sum_{k\equiv t \pmod p} (-1)^k \binom{pn+s}{k}\binom{(k-t)/p}{n} \\ =&(-1)^{pn+t}\binom{pn+s}{pn+t}\binom{(pn+t-t)/p}{n} \\ \equiv&(-1)^{n+t}\binom{s}{t} \pmod p \end{aligned}$$

where we have applied Lucas' theorem in the last step.

When n is positive, clearly

$$\begin{aligned} a_{n-1} - \left\lfloor \frac{s}{p-1} \right\rfloor =& 1 + \left\lfloor \frac{n-1-p^{a-1}-lp^a}{\phi(p^a)} \right\rfloor - \left\lfloor \frac{n-p^{a-1}-lp^a}{\phi(p^a)} \right\rfloor \\ =& \begin{cases} 1 & \text{if } n \not\equiv p^{a-1}+lp^a \equiv (l+1)p^{a-1} \pmod{\phi(p^a)}, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Let $0 \leqslant j \leqslant n-2$. We will see that $a_j \geqslant n-j-1 \geqslant 1$. Since

$$p^a(n-j) + p^{a-1}(s-1) - (n-j)\phi(p^a) = p^{a-1}(n-j+s-1) \geqslant n-j-1,$$

we have

$$\left\lfloor \frac{p(n-j)+s-1}{\phi(p)} \right\rfloor = \left\lfloor \frac{p^a(n-j)+p^{a-1}(s-1)}{\phi(p^a)} \right\rfloor \geqslant \left\lfloor \frac{n-j-1}{\phi(p^a)} \right\rfloor + n - j$$

and therefore

$$a_j \geqslant \left\lfloor \frac{n-j-1}{\phi(p^a)} \right\rfloor + n - j + \left\lfloor \frac{j-p^{a-1}-lp^a}{\phi(p^a)} \right\rfloor - \left\lfloor \frac{n-p^{a-1}-lp^a}{\phi(p^a)} \right\rfloor \geqslant n-j-1$$

by applying Lemma 2.1.

Combining the above we immediately obtain the desired result. □

Lemma 3.3. *Let p be a prime, $n \in \mathbb{Z}^+$, $r \in \mathbb{Z}$ and $s, t \in \{0, \dots, p-1\}$ with $s \neq p-1$. If $s < t$ then*

$$\left\{\begin{matrix} pn+s \\ t \end{matrix}\right\}_{n-1,p} \equiv (-1)^{n+s} \frac{n}{t\binom{t-1}{s}} \pmod p. \tag{3.3}$$

If $s \geqslant t$, then

$$\left\{\begin{matrix} pn+s \\ t \end{matrix}\right\}_{n-1,p} \equiv (-1)^{n+t} n \binom{s}{t} \frac{\sigma_{st}}{p} \pmod p, \tag{3.4}$$

where

$$\sigma_{st} = 1 + (-1)^p \frac{\prod_{1\leqslant i\leqslant p,\, i\neq p-t}(p(n-1)+t+i)}{\prod_{1\leqslant i\leqslant p,\, i\neq p-(s-t)}(s-t+i)} \equiv 1+(-1)^p \equiv 0 \pmod{p}. \tag{3.5}$$

Proof. Clearly

$$\begin{aligned}
\left\{ {pn+s \atop t} \right\}_{n-1,p} =& p^{-\lfloor \frac{pn+s-1-(n-1)p}{p-1} \rfloor} \sum_{k\equiv t \,(\mathrm{mod}\ p)} (-1)^k \binom{pn+s}{k}\binom{(k-t)/p}{n-1} \\
=& \frac{(-1)^{pn+t}}{p}\binom{pn+s}{pn+t}\binom{n}{n-1} \\
&+ \frac{(-1)^{p(n-1)+t}}{p}\binom{pn+s}{p(n-1)+t}\binom{n-1}{n-1}.
\end{aligned}$$

`Case 1.` $s<t$. In this case, $d = t-1-s \geqslant 0$ and

$$\begin{aligned}
\left\{ {pn+s \atop t} \right\}_{n-1,p} =& \frac{(-1)^{p(n-1)+t}}{p} \prod_{i=0}^{s} \frac{pn+i}{p(n-1)+t-i} \cdot \binom{p(n-1)+p-1}{p(n-1)+d} \\
=& \frac{(-1)^{p(n-1)+t} n}{p(n-1)+t} \prod_{i=1}^{s} \frac{pn+i}{p(n-1)+t-i} \cdot \binom{p(n-1)+p-1}{p(n-1)+d} \\
\equiv& (-1)^{n-1+t} \frac{n\times s!}{\prod_{i=0}^{s}(t-i)} \binom{p-1}{d} \quad \text{(by Lucas' theorem)} \\
\equiv& (-1)^{n-s} \frac{n}{t\binom{t-1}{s}} \pmod{p}.
\end{aligned}$$

`Case 2.` $s \geqslant t$. Note that

$$\sigma_{st} \equiv 1 + (-1)^p \frac{(p-1)!}{(p-1)!} \equiv 1+(-1)^p \equiv 0 \pmod{p}$$

and

$$\begin{aligned}
\left\{ {pn+s \atop t} \right\}_{n-1,p} =& \frac{(-1)^{pn+t}}{p}\binom{pn+s}{pn+t}\left(n + (-1)^p \prod_{i=1}^{p} \frac{p(n-1)+t+i}{s-t+i}\right) \\
=& (-1)^{pn+t}\frac{n}{p}\binom{pn+s}{pn+t}\sigma_{st}.
\end{aligned}$$

Therefore

$$\left\{ {pn+s \atop t} \right\}_{n-1,p} \equiv (-1)^{n+t} n \binom{s}{t} \frac{\sigma_{st}}{p} \pmod{p}$$

by Lucas' theorem.

The proof of Lemma 3.3 is now complete. $\square$

Proof of Theorem 1.1. If $n = 0$ or $s = p - 1$ or $\phi(p^a) \nmid n - (l + 1)p^{a-1}$, then (1.1) holds by Lemma 3.2.

Now we suppose that $n > 0$, $s \neq p-1$ and $\phi(p^a) \mid n-(l+1)p^{a-1}$. Then $p^{a-1} \mid n$, and hence $p \mid n$ since $a \geqslant 2$. Therefore $\left\{ {pn+s \atop t} \right\}_{n-1,p} \equiv 0 \pmod p$ by Lemma 3.3, and thus we have (1.1) by (3.2).

This concludes the proof. $\square$

4. Proofs of Theorem 1.2 and Corollary 1.3

Lemma 4.1. *Let p be a prime, and let $a \in \mathbb{Z}^+$, $l \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then, for any $n \in \mathbb{N}$ with $n \equiv l \pmod{p-1}$, we have*

$$\left\{ {n \atop r} \right\}_{l,p} \equiv \begin{cases} (-1)^{\frac{n-l}{p-1}-1}\binom{\frac{n-l}{p-1}-1}{l} \pmod p & \text{if } n > l, \\ 0 \pmod p & \text{if } n \leqslant l. \end{cases} \tag{4.1}$$

Proof. We use induction on $m = (n - l)/(p - 1)$.

If $m \leqslant l$ (i.e., $n \leqslant lp$), then $\lfloor (n - lp - 1)/(p - 1)\rfloor < 0$, and hence

$$\left\{ {n \atop r} \right\}_{l,p} = p^{-\lfloor \frac{n-lp-1}{p-1} \rfloor} \sum_{k \equiv r \pmod p} (-1)^k \binom{n}{k} \binom{(k-r)/p}{l} \equiv 0 \pmod p$$

which yields (4.1). If $l < m \leqslant 1$, then $l = 0$ and $m = 1$, hence $n = p - 1$ and

$$\left\{ {n \atop r} \right\}_{l,p} \equiv \sum_{k \equiv r \pmod p} \binom{p-1}{k}(-1)^k \equiv 1 = (-1)^{m-1}\binom{m-1}{l} \pmod p.$$

Thus the desired result always holds in the case $m \leqslant \max\{l, 1\}$.

Now let $m > \max\{l, 1\}$ and assume that whenever $l_*, n_* \in \mathbb{N}$ and $(n_* - l_*)/(p - 1) = m - 1 > 0$ we have

$$\left\{ {n_* \atop i} \right\}_{l_*,p} = (-1)^{\frac{n_*-l_*}{p-1}-1}\binom{\frac{n_*-l_*}{p-1} - 1}{l_*} = (-1)^m \binom{m-2}{l_*} \pmod p$$

for all $i \in \mathbb{Z}$.

For $n' = n - (p - 1)$ clearly $(n' - l)/(p - 1) = m - 1 \geqslant \max\{l, 1\}$. By the induction hypothesis, $\left\{ {n' \atop i} \right\}_{l,p} \equiv (-1)^m \binom{m-2}{l} \pmod p$ for each $i \in \mathbb{Z}$. In view of the Chu-Vandermonde convolution identity (cf. [GKP, (5.27)]),

$$\binom{n}{k} = \sum_{j=0}^{p-1} \binom{p-1}{j}\binom{n'}{k-j}$$

for every $k = 0, 1, 2, \ldots$. Therefore

$$\begin{aligned}
\left\{ n \atop r \right\}_{l,p} =& p^{-\lfloor \frac{n-lp-1}{p-1} \rfloor} \sum_{j=0}^{p-1} \binom{p-1}{j} \sum_{p \mid k-r} (-1)^k \binom{n'}{k-j} \binom{(k-r)/p}{l} \\
=& \sum_{j=0}^{p-1} \binom{p-1}{j} \frac{(-1)^j}{p} \left\{ n' \atop r-j \right\}_{l,p} \\
=& \sum_{j=0}^{p-1} \binom{p-1}{j} (-1)^j \frac{\left\{ n' \atop r-j \right\}_{l,p} - (-1)^m \binom{m-2}{l}}{p},
\end{aligned}$$

since $\sum_{j=0}^{p-1} \binom{p-1}{j} (-1)^j = (1-1)^{p-1} = 0$. Thus

$$\left\{ n \atop r \right\}_{l,p} \equiv \sum_{j=0}^{p-1} \frac{\left\{ n' \atop r-j \right\}_{l,p} - (-1)^m \binom{m-2}{l}}{p} \pmod p.$$

Observe that

$$\begin{aligned}
& p^{\lfloor \frac{n'-lp-1}{p-1} \rfloor} \sum_{j=0}^{p-1} \left\{ n' \atop r-j \right\}_{l,p} \\
=& \sum_{j=0}^{p-1} \sum_{k \equiv r-j \pmod p} (-1)^k \binom{n'}{k} \binom{(k-(r-j))/p}{l} \\
=& \sum_{k=0}^{n'} (-1)^k \binom{n'}{k} \binom{\lfloor (k-r+p-1)/p \rfloor}{l} \\
=& \begin{cases} \sum_{k=0}^{n'} (-1)^k \binom{n'}{k} = (1-1)^{n'} = 0 & \text{if } l = 0, \\ -\sum_{k \equiv r \pmod p} (-1)^k \binom{n'-1}{k} \binom{(k-r)/p}{l-1} & \text{if } l > 0, \end{cases}
\end{aligned}$$

where we have applied Lemma 2.1 of Sun [S06] to get the last equality. Also,

$$\left\lfloor \frac{n'-1-(l-1)p-1}{p-1} \right\rfloor = \left\lfloor \frac{n'-lp-1}{p-1} \right\rfloor + 1$$

and

$$\frac{n'-1-(l-1)}{p-1} = m-1.$$

Therefore

$$\begin{aligned}
\frac{1}{p} \sum_{j=0}^{p-1} \left\{ n' \atop r-j \right\}_{l,p} =& \begin{cases} 0 & \text{if } l = 0, \\ -\left\{ n'-1 \atop r \right\}_{l-1,p} & \text{if } l > 0, \end{cases} \\
\equiv& (-1)^{m-1} \binom{m-2}{l-1} \pmod p \quad \text{(by the induction hypothesis).}
\end{aligned}$$

Combining the above we finally obtain that

$$\begin{aligned}\left\{ n \atop r \right\}_{l,p} &\equiv \frac{1}{p}\sum_{j=0}^{p-1}\left\{ n' \atop r-j \right\}_{l,p} - (-1)^m\binom{m-2}{l} \\ &\equiv (-1)^{m-1}\binom{m-2}{l-1} + (-1)^{m-1}\binom{m-2}{l} \\ &\equiv (-1)^{m-1}\binom{m-1}{l} \pmod p.\end{aligned}$$

This concludes the induction proof. □

Proof of Theorem 1.2. By Lemma 3.2, if $s = p-1$, or $\phi(p) = p-1$ does not divide $n-l-1$, then (1.2) holds. If $s \neq p-1$ and $p \mid n$, then we also have (1.2) by Lemmas 3.2 and 3.3. Below we assume that $s \neq p-1$, $p-1 \mid n-l-1$ and $p \nmid n$.

When $s = 2t$, clearly

$$\begin{aligned}\sigma_{st} &= 1 + (-1)^p \prod_{\substack{1\leqslant i\leqslant p \\ i\neq p-t}}\left(1 + \frac{p(n-1)}{t+i}\right) \\ &\equiv 1 + (-1)^p\left(1 + p(n-1)\sum_{\substack{1\leqslant i\leqslant p \\ i\neq p-t}}\frac{1}{t+i}\right) \equiv p\delta_{p,2} \pmod{p^2},\end{aligned}$$

for, n is odd if $p = 2$, and

$$\sum_{\substack{1\leqslant i\leqslant p \\ i\neq p-t}}\frac{1}{t+i} \equiv \sum_{k=1}^{p-1}\frac{1}{k} = \sum_{k=1}^{(p-1)/2}\left(\frac{1}{k} + \frac{1}{p-k}\right) \equiv 0 \pmod p$$

if $p \neq 2$. Therefore, in the case $s = 2t$ and $p \neq 2$, we have (1.2) by Lemmas 3.2 and 3.3.

Now we consider the case $s < t$. By Lemmas 3.2, 3.3 and 4.1,

$$\begin{aligned}\left\{ pn+s \atop pr+t \right\}_{l,p^2} &\equiv (-1)^{n-1}\left\{ pn+s \atop t \right\}_{n-1,p}\left\{ n-1 \atop r \right\}_{l,p} \\ &\equiv (-1)^{n-1}(-1)^{n+s}\frac{n}{t\binom{t-1}{s}} \\ &\quad\times\begin{cases} (-1)^{\frac{(n-1)-l}{p-1}-1}\binom{\frac{n-1-l}{p-1}-1}{l} \pmod p & \text{if } n-1 > l, \\ 0 \pmod p & \text{if } n-1 \leqslant l.\end{cases}\end{aligned}$$

In view of the above we have completed the proof of Theorem 1.2. □

Proof of Corollary 1.3. We just modify the third case in the proof of Theorem 1.5 of [SD]. The only thing we require is that in the case $n > 0$ and $n \equiv r \equiv 0 \pmod{p}$ we still have

$$T_{0,2}^{(p)}(n,r) = \frac{p^{\lfloor \frac{n/p-1}{p-1} \rfloor}}{(n/p)!} \begin{Bmatrix} n \\ r \end{Bmatrix}_{0,p^2} \equiv \frac{p^{\lfloor \frac{n_0-1}{p-1} \rfloor}}{n_0!} \begin{Bmatrix} n_0 \\ r_0 \end{Bmatrix}_{0,p} = T_{0,1}^{(p)}(n_0,r_0) \pmod{p}$$

where $n_0 = n/p$ and $r_0 = r/p$. Note that

$$\mathrm{ord}_p(n_0!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n_0}{p^i} \right\rfloor < \sum_{i=1}^{\infty} \frac{n_0}{p^i} = \frac{n_0}{p-1}$$

and thus $\mathrm{ord}_p(n_0!) \leqslant \lfloor (n_0-1)/(p-1) \rfloor$.

If $p \neq 2$, then by applying (1.2) with $l = s = t = 0$ we find that

$$\begin{Bmatrix} n \\ r \end{Bmatrix}_{0,p^2} = \begin{Bmatrix} pn_0 \\ pr_0 \end{Bmatrix}_{0,p^2} \equiv \begin{Bmatrix} n_0 \\ r_0 \end{Bmatrix}_{0,p} \pmod{p}$$

and so $T_{0,2}^{(p)}(n,r) \equiv T_{0,1}^{(p)}(n_0,r_0) \pmod{p}$. The last congruence also holds when $p = 2$, because by Lemma 4.2 of [SD] we have

$$2 \nmid T_{0,2}^{(2)}(n,r) \iff n = 2n_0 \text{ is a power of } 2 \iff 2 \nmid T_{0,1}^{(2)}(n_0,r_0).$$

This concludes the proof. □

5. Proofs of Theorems 1.4 and 1.5

Proof of Theorem 1.4. By Lemma 3.2 of [SD] and its proof, if $j \in \mathbb{N}$ then

$$\sum_{k \equiv 0 \,(\mathrm{mod}\ p)} (-1)^k \binom{pn}{k} \binom{k/p}{j} = \sum_{j \leqslant k \leqslant n} (-1)^{pk} \binom{pn}{pk} \binom{k}{j}$$

is congruent to

$$\sum_{j \leqslant k \leqslant n} (-1)^k \binom{n}{k} \binom{k}{j} = \binom{n}{j} \sum_{k \geqslant j} (-1)^k \binom{n-j}{k-j} = (-1)^j \, \delta_{j,n}$$

modulo $p^{2\mathrm{ord}_p(n)+1+\delta}$. Therefore

$$\mathrm{ord}_p\left(\begin{Bmatrix} pn \\ 0 \end{Bmatrix}_{j,p} \right) \geqslant 2\mathrm{ord}_p(n) + 1 + \delta - \left\lfloor \frac{pn - jp - 1}{p-1} \right\rfloor$$

for any $j \in \mathbb{N}$ with $j \neq n$. As in the proof of Lemma 3.2,

$$\left\{ pn \atop pr \right\}_{l,p^{a+1}} = (-1)^n(-1)^{pn}\left\{ n \atop r \right\}_{l,p^a} + \sum_{0\leqslant j<n} (-1)^j p^{a_j}\left\{ j \atop r \right\}_{l,p^a}\left\{ pn \atop 0 \right\}_{j,p}$$

where $a_j \in \mathbb{Z}$ and $a_j \geqslant n-j-1$.

Let m be the least integer greater than or equal to $\frac{p-1}{p}(2\mathrm{ord}_p(n)+\delta)$. Then $m-1 < \frac{p-1}{p}(2\mathrm{ord}_p(n)+\delta)$ and hence

$$m + \left\lfloor \frac{m-1}{p-1} \right\rfloor = \left\lfloor \frac{p(m-1)}{p-1} \right\rfloor + 1 \leqslant 2\mathrm{ord}_p(n)+\delta.$$

For $0 \leqslant j < n$, if $n-j \geqslant m+1$ then $a_j \geqslant n-j-1 \geqslant m$; if $n-j \leqslant m$ then

$$\begin{aligned} a_j + \mathrm{ord}_p\left(\left\{ pn \atop 0 \right\}_{j,p}\right) \geqslant& n-j-1+2\mathrm{ord}_p(n)+1+\delta - \left\lfloor \frac{p(n-j)-1}{p-1} \right\rfloor \\ =& 2\mathrm{ord}_p(n)+\delta - \left\lfloor \frac{n-j-1}{p-1} \right\rfloor \\ \geqslant& 2\mathrm{ord}_p(n)+\delta - \left\lfloor \frac{m-1}{p-1} \right\rfloor \geqslant m. \end{aligned}$$

Combining the above we get that

$$\mathrm{ord}_p\left(\left\{ pn \atop pr \right\}_{l,p^{a+1}} - (-1)^{(p-1)n}\left\{ n \atop r \right\}_{l,p^a}\right) \geqslant m \geqslant \frac{p-1}{p}(2\mathrm{ord}_p(n)+\delta).$$

If $(p-1)n$ is odd, then $p=2$ and $2 \nmid n$, hence $2\mathrm{ord}_p(n)+\delta = 0$. So (1.5) holds. $\square$

Proof of Theorem 1.5. We use induction on a.

When $a=1$, the desired result follows from Lemma 4.1.

In the case $a=2$, by Theorem 1.2 and Lemma 4.1, we have

$$\begin{aligned} \left\{ n \atop r \right\}_{l,p^2} =& \left\{ p(l+m(p-1))+p-1 \atop p\lfloor r/p \rfloor + \{r\}_p \right\}_{l,p^2} \\ \equiv& (-1)^{\{r\}_p}\binom{p-1}{\{r\}_p}\left\{ l+m(p-1) \atop \lfloor r/p \rfloor \right\}_{l,p} \equiv \left\{ l+m(p-1) \atop \lfloor r/p \rfloor \right\}_{l,p} \\ \equiv& (-1)^{m-1}\binom{m-1}{l} \pmod p. \end{aligned}$$

Now let $a > 2$ and assume Theorem 1.5 with a replaced by $a-1$. Then, with helps of Theorem 1.1 and the induction hypothesis, we have

$$\begin{aligned}\left\{ n \atop r \right\}_{l,p^a} =&\left\{ p^{a-1}(l+m(p-1)+1)-1 \atop r \right\}_{l,p^a} \\ =&\left\{ p(p^{a-2}(l+m(p-1)+1)-1)+(p-1) \atop p\lfloor r/p \rfloor + \{r\}_p \right\}_{l,p^a} \\ \equiv&(-1)^{\{r\}_p}\binom{p-1}{\{r\}_p}\left\{ p^{a-2}(l+m(p-1)+1)-1 \atop \lfloor r/p \rfloor \right\}_{l,p^{a-1}} \\ \equiv&\left\{ (l+1)p^{a-2}-1+m\phi(p^{a-1}) \atop \lfloor r/p \rfloor \right\}_{l,p^{a-1}} \\ \equiv&(-1)^{m-1}\binom{m-1}{l} \pmod p.\end{aligned}$$

This concludes the induction step and we are done. □

References

[C] P. Colmez, *Une correspondance de Langlands locale p-adique pour les representations semi-stables de dimension 2*, preprint, 2004.

[DS] 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.

[DW] K. S. Davis and W. A. Webb, *A binomial coefficient congruence modulo prime powers*, J. Number Theory **43** (1993), 20–23.

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

[G] H. W. Gould, *Combinatorial Identities,* Revised Edition, Gould Publications, Morgantown, W. Va., 1972.

[GKP] R. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics,* Second Edition, Addison Wesley, New York, 1994.

[Gr] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers,* in: Organic mathematics (Burnaby, BC, 1995), J. Borwein, P. Borwein, L. Jörgenson and R. Corless, CMS Conf. Proc., Vol. 20 (Amer. Math. Soc., Providence, RI, 1997), pp. 253–276.

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

[P] H. Pan, *A congruence of Lucas' type*, Discrete Math. **288** (2004), 173–175.

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

[S06] Z. W. Sun, *Polynomial extension of Fleck's congruence*, Acta Arith. **122** (2006), 91–100.

[SD] Z. W. Sun and D. M. Davis, *Combinatorial congruences modulo prime powers*, Trans. Amer. Math. Soc. **359** (2007), 5525–5553.

[W] D. Wan, *Combinatorial congruences and ψ-operators*, Finite Fields Appl. **12** (2006), 693–703.

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