Preprint (arXiv:math.NT/0508087)

COMBINATORIAL CONGRUENCES MODULO PRIME POWERS

ZHI-WEI SUN[1] AND DONALD M. DAVIS[2]

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

[2]Department of Mathematics, Lehigh University
Bethlehem, PA 18015, USA
dmd1@lehigh.edu
http://www.lehigh.edu/~dmd1

ABSTRACT. Let p be any prime, and let α and n be nonnegative integers. Let $r \in \mathbb{Z}$ and $f(x) \in \mathbb{Z}[x]$. We establish the congruence

$$p^{\deg f} \sum_{k \equiv r \,(\mathrm{mod}\ p^\alpha)} \binom{n}{k} (-1)^k f\left(\frac{k-r}{p^\alpha}\right) \equiv 0 \ \left(\mathrm{mod}\ p^{\sum_{i=\alpha}^{\infty} \lfloor n/p^i \rfloor}\right)$$

(motivated by a conjecture arising from algebraic topology), and obtain the following vast generalization of Lucas' theorem: If $\alpha > 1$ and l, s, t are nonnegative integers with $s, t < p$, then

$$\frac{1}{\lfloor n/p^{\alpha-1} \rfloor !} \sum_{k \equiv r \,(\mathrm{mod}\ p^\alpha)} \binom{pn+s}{pk+t} (-1)^{pk} \left(\frac{k-r}{p^{\alpha-1}}\right)^l$$
$$\equiv \frac{1}{\lfloor n/p^{\alpha-1} \rfloor !} \sum_{k \equiv r \,(\mathrm{mod}\ p^\alpha)} \binom{n}{k} \binom{s}{t} (-1)^k \left(\frac{k-r}{p^{\alpha-1}}\right)^l \ (\mathrm{mod}\ p).$$

We also present an application of the first congruence to Bernoulli polynomials, and apply the second congruence to show that a p-adic order bound given by the authors in a previous paper is sharp.

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

The first author is responsible for communications, and supported by the National Science Fund for Distinguished Young Scholars (No. 10425103) and the Key Program of NSF (No. 10331020) in P. R. China.

1. Introduction

In this paper we establish a number of new congruences for sums involving binomial coefficients with the summation index restricted in a residue class modulo a prime power; some of them are vast extensions of some classical congruences. We begin by providing some historical background for these results.

Let p be a prime, and let $\mathbb{Q}_p$ and $\mathbb{Z}_p$ denote the field of p-adic numbers and the ring of p-adic integers respectively. For $\omega \in \mathbb{Q}_p \setminus \{0\}$ we define its *p-adic order* by $\mathrm{ord}_p(\omega) = \max\{a \in \mathbb{Z} : \omega/p^a \in \mathbb{Z}_p\}$; in addition, we set $\mathrm{ord}_p(0) = +\infty$.

In 1913, A. Fleck (cf. [D, p. 274]) proved that for any $n \in \mathbb{Z}^+ = \{1, 2, 3, \dots\}$ and $r \in \mathbb{Z}$ we have the congruence

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

(where $\lfloor\cdot\rfloor$ is the greatest integer function, and we regard $\binom{x}{k} = 0$ for $k = -1, -2, -3, \dots$); that is,

$$\mathrm{ord}_p\bigg(\sum_{k\equiv r \,(\mathrm{mod}\ p)} \binom{n}{k}(-1)^k\bigg) \geqslant \left\lfloor \frac{n-1}{p-1} \right\rfloor.$$

In 1977, C. S. Weisman [W] showed further that if $\alpha, n \in \mathbb{N} = \{0, 1, 2, \dots\}$ and $r \in \mathbb{Z}$ then

$$\mathrm{ord}_p\bigg(\sum_{k\equiv r \,(\mathrm{mod}\ p^\alpha)} \binom{n}{k}(-1)^k\bigg) \geqslant \left\lfloor \frac{n-p^{\alpha-1}}{\varphi(p^\alpha)} \right\rfloor,$$

where φ is the well-known Euler function. Weisman remarked that this kind of work is closely related to p-adic continuation.

In 2005, motivated by Fontaine's theory of (ϕ, Γ)-modules, D. Wan got an extension of Fleck's result in his lecture notes by giving a lower bound for the p-adic order of the sum $\sum_{k\equiv r \,(\mathrm{mod}\ p)} \binom{n}{k}(-1)^k\binom{(k-r)/p}{l}$, where $l, n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Soon after this, Z. W. Sun [S05] obtained a common generalization of Weisman's and Wan's extensions of Fleck's congruence by studying the p-adic order of the sum

$$\sum_{k\equiv r \,(\mathrm{mod}\ p^\alpha)} \binom{n}{k}(-1)^k\binom{(k-r)/p^\alpha}{l}$$

via a combinatorial approach. But, when $l \geqslant n/p^\alpha$, any result along this line yields no nonzero lower bound for the p-adic order of the last sum.

Unlike the previous development of Fleck's congruence, there is another direction motivated by algebraic topology. In order to obtain a strong lower bound for homotopy exponents of the special unitary group SU(n), the authors [DS] were led to show that if $\alpha, n \in \mathbb{N}$ and $r \in \mathbb{Z}$ then

$$\min_{f(x)\in\mathbb{Z}[x]} \operatorname{ord}_p\Bigg(\sum_{k\equiv r\ (\mathrm{mod}\ p^\alpha)} \binom{n}{k}(-1)^k f\left(\frac{k-r}{p^\alpha}\right)\Bigg) \geqslant \operatorname{ord}_p\left(\left\lfloor \frac{n}{p^\alpha}\right\rfloor!\right).$$

As shown in [DS], this inequality implies a subtle divisibility property of Stirling numbers of the second kind. Note that if $n \in \mathbb{Z}^+$ then

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

and hence $\operatorname{ord}_p(n!) \leqslant (n-1)/(p-1)$.

Now we introduce some conventions used throughout this paper. As usual, the degree of the zero polynomial is regarded as $-\infty$. For $a \in \mathbb{Z}$ and $m > 0$, we let $\{a\}_m$ denote the fractional part of a/m times m (i.e., $\{a\}_m$ is the unique number in the interval $[0, m)$ with $a - \{a\}_m \in m\mathbb{Z}$). For a prime p, if $a, b \in \mathbb{Z}$ then $\tau_p(a, b)$ stand for the number of carries when adding a and b in base p; a theorem of E. Kummer states that $\tau_p(a,b) = \operatorname{ord}_p\binom{a+b}{a}$.

Here is our first theorem.

Theorem 1.1. *Let p be a prime and $f(x) \in \mathbb{Z}_p[x]$. Let $\alpha, n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then*

$$\begin{aligned} &p^{\deg f}\sum_{k\equiv r\ (\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k f\left(\frac{k-r}{p^\alpha}\right)\\ &\equiv 0 \left(\mathrm{mod}\ p^{\sum_{i=\alpha}^{\infty}\lfloor n/p^i\rfloor + \tau_p(\{r\}_{p^{\alpha-1}},\{n-r\}_{p^{\alpha-1}})}\right),\end{aligned}$$

i.e.,

$$\begin{aligned} &\operatorname{ord}_p\Bigg(\sum_{k\equiv r\ (\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k f\left(\frac{k-r}{p^\alpha}\right)\Bigg)\\ &\geqslant \operatorname{ord}_p\left(\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\right) - \deg f + \tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}).\end{aligned} \tag{1.1}$$

Remark 1.1. It is interesting to compare (1.1) with the following inequality ([Theorem 5.1, DS]) established for topological purpose:

$$\begin{aligned} &\operatorname{ord}_p\Bigg(\sum_{k\equiv r\ (\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k f\left(\frac{k-r}{p^\alpha}\right)\Bigg)\\ &\geqslant \operatorname{ord}_p\left(\left\lfloor\frac{n}{p^{\alpha}}\right\rfloor!\right) + \tau_p(\{r\}_{p^{\alpha}}, \{n-r\}_{p^{\alpha}}).\end{aligned} \tag{1.2}$$

Note that $\mathrm{ord}_p(\lfloor n/p^\alpha\rfloor!) = \mathrm{ord}_p(\lfloor n/p^{\alpha-1}\rfloor!) - \lfloor n/p^\alpha\rfloor$ and

$$0 \leqslant \tau_p(\{r\}_{p^\alpha}, \{n-r\}_{p^\alpha}) - \tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}) \leqslant 1.$$

In general, when $\deg f < \lfloor n/p^\alpha\rfloor$, the term $\tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}})$ in (1.1) cannot be replaced by $\tau_p(\{r\}_{p^\alpha}, \{n-r\}_{p^\alpha})$. A principal motivation for the development of Theorem 1.1 is that the inequality (1.2), although quite sharp when $\deg f \geqslant \lfloor n/p^\alpha\rfloor$, is not a good estimate for smaller values of $\deg f$.

Example 1.1. Let $p = \alpha = 2$, $r = 1$ and $n = 20$. Then, for each $0 < l < \lfloor n/p^\alpha\rfloor = 5$, equality in (1.1) with $f(x) = x^l$ is attained while

$$\tau_p(\{r\}_{p^\alpha}, \{n-r\}_{p^\alpha}) = \tau_2(1,3) = \tau_2(1,1)+1 = \tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}})+1.$$

Example 1.2. Let $p = 3$, $\alpha = r = 2$, $90 \leqslant n \leqslant 98$ and $0 \leqslant l < \lfloor n/p^\alpha\rfloor = 10$. In Table 1 below, $\delta_n(l)$ denotes the left hand side of (1.1) minus the right hand side with $f(x) = x^l$.

Table 1: Values of $\delta_n(l)$ with $0 \leqslant l \leqslant 9$ and $90 \leqslant n \leqslant 98$

n \ l	0	1	2	3	4	5	6	7	8	9
90	1	0	2	0	1	0	1	0	3	0
91	1	0	1	0	3	0	1	0	1	0
92	0	1	0	3	0	1	0	1	0	2
93	0	2	0	1	0	1	0	4	0	1
94	0	1	0	2	0	1	0	1	0	3
95	1	0	0	0	0	1	1	0	0	0
96	1	0	0	0	0	1	2	0	0	0
97	1	0	0	0	0	1	1	0	0	0
98	1	3	0	1	0	1	1	4	0	1

Example 1.3. The combination of using Theorem 1.1 when $\deg f \leqslant \lfloor n/p^\alpha\rfloor$ and the inequality (1.2) for larger values of $\deg f$ provides an excellent estimate for

$$\mathrm{ord}_p\bigg(\sum_{k\equiv r \,(\mathrm{mod}\ p^\alpha)} \binom{n}{k}(-1)^k f\left(\frac{k-r}{p^\alpha}\right)\bigg).$$

For example, if $p = 2$, $\alpha = 1$, $r = 0$, $n = 20$ and $f(x) = x^l$, then the actual values of the expression for $l = 0, \ldots, 21$ are

$$19, 19, 17, 17, 14, 14, 12, 12, 10, 10, 8, 8, 8, 8, 11, 9, 9, 9, 8, 8, 8, 8.$$

The inequality (1.2) guarantees that each of the 22 numbers should be at least 8, while Theorem 1.1 gives the lower bounds

$$18, 17, 16, 15, 14, 13, 12, 11, 10, 9, 8$$

for the first 11 of the above 22 values respectively. The bound given by (1.1) is attained in this example with $l = 4$, while $\mathrm{ord}_p(\lfloor (n/p^{\alpha-1})\rfloor !) = 18 < 19 = \lfloor (n-p^{\alpha-1})/\varphi(p^\alpha)\rfloor$; this shows that for a general $f(x) \in \mathbb{Z}_p[x]$ we cannot replace $\mathrm{ord}_p(\lfloor (n/p^{\alpha-1})\rfloor !)$ in (1.1) by Weisman's bound $\lfloor (n-p^{\alpha-1})/\varphi(p^\alpha)\rfloor$ even if $r = 0$ (and hence the τ-term vanishes).

Here is an application of Theorem 1.1 to Bernoulli polynomials. (The reader is referred to [IR] and [S03] for some basic properties and known congruences concerning Bernoulli polynomials.)

Corollary 1.1. *Let p be a prime, and let $\alpha \in \mathbb{N}$, $m, n \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$. Then*

$$\begin{aligned}&\mathrm{ord}_p\left(\frac{p^{m-1}}{m}\sum_{k=0}^{n}\binom{n}{k}(-1)^k B_m\left(\left\lfloor\frac{k-r}{p^\alpha}\right\rfloor\right)\right)\\ &\geqslant \sum_{i=\alpha}^{\infty}\left\lfloor\frac{n-1}{p^i}\right\rfloor + \tau_p(\{r-1\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}).\end{aligned} \tag{1.3}$$

Proof. Set $\bar{r} = r + p^\alpha - 1$. In view of [S05, Lemma 2.1] and the known identity $B_m(x+1) - B_m(x) = mx^{m-1}$, we have

$$\begin{aligned}&\sum_{k=0}^{n}\binom{n}{k}\frac{(-1)^k}{m}B_m\left(\left\lfloor\frac{k-r}{p^\alpha}\right\rfloor\right)\\ =&\sum_{k\equiv \bar{r}\ (\mathrm{mod}\ p^\alpha)}\binom{n-1}{k}\frac{(-1)^{k-1}}{m}\left(B_m\left(\frac{k-\bar{r}}{p^\alpha}+1\right) - B_m\left(\frac{k-\bar{r}}{p^\alpha}\right)\right)\\ =&\sum_{k\equiv \bar{r}\ (\mathrm{mod}\ p^\alpha)}\binom{n-1}{k}(-1)^{k-1}\left(\frac{k-\bar{r}}{p^\alpha}\right)^{m-1}.\end{aligned}$$

This, together with Theorem 1.1, yields that

$$\begin{aligned}&\mathrm{ord}_p\left(\sum_{k=0}^{n}\binom{n}{k}\frac{(-1)^k}{m}B_m\left(\left\lfloor\frac{k-r}{p^\alpha}\right\rfloor\right)\right)\\ \geqslant&\,\mathrm{ord}_p\left(\left\lfloor\frac{n-1}{p^{\alpha-1}}\right\rfloor !\right) - (m-1) + \tau_p(\{\bar{r}\}_{p^{\alpha-1}}, \{n-1-\bar{r}\}_{p^{\alpha-1}}).\end{aligned}$$

So (1.3) follows. □

Let $f(x)\in\mathbb{Q}_p[x]$ and $\deg f\leqslant l\in\mathbb{N}$. It is well known that $f(a)\in\mathbb{Z}_p$ for all $a\in\mathbb{Z}$ if and only if $f(x)=\sum_{j=0}^{l}a_j\binom{x}{j}$ for some $a_0,\ldots,a_l\in\mathbb{Z}_p$.

Since any $f(x)\in\mathbb{Z}_p[x]$ with $\deg f=l\in\mathbb{N}$ can be written in the form $\sum_{j=0}^{l}b_j\,j!\binom{x}{j}$ with $b_j\in\mathbb{Z}_p$ (e.g., $x^l=\sum_{j=0}^{l}S(l,j)\,j!\binom{x}{j}$ where $S(l,j)$ $(0\leqslant j\leqslant l)$ are Stirling numbers of the second kind), we can reformulate Theorem 1.1 as follows.

Theorem 1.2. *Let p be a prime, $\alpha,n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Let $f(x)\in\mathbb{Q}_p[x]$, $\deg f\leqslant l\in\mathbb{N}$, and $f(a)\in\mathbb{Z}_p$ for all $a\in\mathbb{Z}$. Then we have*

$$\begin{aligned}&\operatorname{ord}_p\Bigg(\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k f\left(\frac{k-r}{p^\alpha}\right)\Bigg)\\ \geqslant&\operatorname{ord}_p\left(\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\right)-l-\operatorname{ord}_p(l!)+\tau_p(\{r\}_{p^{\alpha-1}},\{n-r\}_{p^{\alpha-1}}).\end{aligned}\tag{1.4}$$

Remark 1.2. This theorem has topological background. In the case $p=\alpha=r=2$ and $f(x)=\binom{x}{l}$, it first arose as a conjecture of the second author in his study of algebraic topology.

Let $[x^n]F(x)$ denote the coefficient of x^n in the power series expansion of $F(x)$. Theorem 1.1 also has the following equivalent form.

Theorem 1.3. *Let p be a prime, and let $\alpha,l,n,r\in\mathbb{N}$. If $r>n-(l+1)p^\alpha$, then*

$$\begin{aligned}&\operatorname{ord}_p\left([x^r]\frac{(1-x)^n}{(1-x^{p^\alpha})^{l+1}}\right)\\ \geqslant&\operatorname{ord}_p\left(\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\right)-l-\operatorname{ord}_p(l!)+\tau_p(\{r\}_{p^{\alpha-1}},\{n-r\}_{p^{\alpha-1}}).\end{aligned}\tag{1.5}$$

Proof. Let $r>n-(l+1)m$ where $m=p^\alpha$. Observe that

$$\begin{aligned}[x^r]\frac{(1-x)^n}{(1-x^m)^{l+1}}=&\sum_{k=0}^{r}\binom{n}{k}(-1)^k[x^{r-k}](1-x^m)^{-l-1}\\ =&\sum_{k=0}^{r}\binom{n}{k}(-1)^k[x^{r-k}]\sum_{j\geqslant0}\binom{l+j}{l}(x^m)^j\\ =&\sum_{\substack{0\leqslant k\leqslant r\\ k\equiv r\,(\mathrm{mod}\ m)}}\binom{n}{k}(-1)^k\binom{l-(k-r)/m}{l}.\end{aligned}$$

If $r < k \leqslant n$ and $k \equiv r \pmod m$, then $0 < (k-r)/m \leqslant (n-r)/m < l+1$ and hence $\binom{l-(k-r)/m}{l} = 0$. Therefore

$$[x^r]\frac{(1-x)^n}{(1-x^m)^{l+1}} = \sum_{\substack{0\leqslant k\leqslant n\\ k\equiv r(\mathrm{mod}\ m)}} \binom{n}{k}(-1)^k\binom{l-(k-r)/m}{l},$$
$$=(-1)^l\sum_{k\equiv r'\ (\mathrm{mod}\ m)}\binom{n}{k}(-1)^k\binom{(k-r')/m}{l},$$

where $r' = r+m$. Applying Theorem 1.1 or 1.2 we immediately get the inequality (1.5). □

Here is another equivalent version of Theorem 1.1.

Theorem 1.4. *Let p be a prime and α be a nonnegative integer. Let $f(x) \in \mathbb{Z}_p[x]$ with $\deg f = l \in \mathbb{N}$. Then, there is a sequence $\{a_k\}_{k\in\mathbb{N}}$ of p-adic integers such that for any $n \in \mathbb{N}$ we have*

$$\begin{aligned}&\sum_{k=0}^{n}\binom{n}{k}(-1)^k\left\lfloor\frac{k}{p^{\alpha-1}}\right\rfloor!\binom{\{r\}_{p^{\alpha-1}}+\{k-r\}_{p^{\alpha-1}}}{\{r\}_{p^{\alpha-1}}}a_k\\ &=\begin{cases}p^l f(\frac{n-r}{p^\alpha}) & \text{if } n\equiv r \pmod{p^\alpha},\\ 0 & \text{otherwise.}\end{cases}\end{aligned}\tag{1.6}$$

Proof. The binomial inversion formula (see, e.g., [GKP]) states that $\sum_{k=0}^{n}\binom{n}{k}(-1)^k b_k = d_n$ for all $n\in\mathbb{N}$, if and only if $\sum_{k=0}^{n}\binom{n}{k}(-1)^k d_k = b_n$ for all $n\in\mathbb{N}$. Thus the desired result has the following equivalent form: There exists a sequence $\{a_n\}_{n\in\mathbb{N}}$ of p-adic integers such that for all $n\in\mathbb{N}$ we have

$$\begin{aligned}&\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\binom{\{r\}_{p^{\alpha-1}}+\{n-r\}_{p^{\alpha-1}}}{\{r\}_{p^{\alpha-1}}}a_n\\ &=\sum_{k\equiv r\ (\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k p^l f\left(\frac{k-r}{p^\alpha}\right).\end{aligned}$$

This is essentially what Theorem 1.1 says. □

A famous theorem of E. Lucas states that if p is a prime and n, r, s, t are nonnegative integers with $s, t < p$ then

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

Now we present our following analogue of Lucas' theorem.

Theorem 1.5. *Let p be a prime and $\alpha \geqslant 2$ be an integer. Then, for any $l, n \in \mathbb{N}$ and $r \in \mathbb{Z}$, we have the congruence*

$$T_{l,\alpha+1}^{(p)}(n,r) \equiv (-1)^{\{r\}_p} \binom{\{n\}_p}{\{r\}_p} T_{l,\alpha}^{(p)}\left(\left\lfloor \frac{n}{p} \right\rfloor, \left\lfloor \frac{r}{p} \right\rfloor\right) \pmod{p}, \tag{1.7}$$

where

$$T_{l,\alpha}^{(p)}(n,r) := \frac{l!p^l}{\lfloor n/p^{\alpha-1} \rfloor!} \sum_{k \equiv r \pmod{p^\alpha}} \binom{n}{k} (-1)^k \binom{(k-r)/p^\alpha}{l}.$$

Remark 1.3. Theorem 1.2 guarantees that $T_{l,\alpha}^{(p)}(n,r) \in \mathbb{Z}_p$ (and our proof of Theorem 1.2 given later is based on analysis of this T). Theorem 1.5 provides further information on $T_{l,\alpha}^{(p)}(n,r)$ modulo p.

Since $f(x) = l!\binom{x}{l} - x^l \in \mathbb{Z}[x]$ has degree smaller than l, we have

$$T_{l,\alpha}^{(p)}(n,r) \equiv \frac{p^l}{\lfloor n/p^{\alpha-1} \rfloor!} \sum_{k \equiv r \pmod{p^\alpha}} \binom{n}{k} (-1)^k \left(\frac{k-r}{p^\alpha}\right)^l \pmod{p}$$

by Theorem 1.1. Thus, Theorem 1.5 has the following equivalent version.

Theorem 1.6. *Let p be any prime, and and let $l, n \in \mathbb{N}$, $r, s, t \in \mathbb{Z}$ and $0 \leqslant s, t < p$. Then, for every $\alpha = 2, 3, \ldots$, we have*

$$\begin{aligned} &\frac{1}{\lfloor n/p^{\alpha-1} \rfloor!} \sum_{k \equiv r \pmod{p^\alpha}} \binom{pn+s}{pk+t} (-1)^{pk} \left(\frac{k-r}{p^{\alpha-1}}\right)^l \\ \equiv &\frac{1}{\lfloor n/p^{\alpha-1} \rfloor!} \sum_{k \equiv r \pmod{p^\alpha}} \binom{n}{k}\binom{s}{t} (-1)^k \left(\frac{k-r}{p^{\alpha-1}}\right)^l \pmod{p}. \end{aligned} \tag{1.8}$$

Remark 1.4. Theorem 1.6 is a vast generalization of Lucas' theorem. Given a prime p and nonnegative integers n, r, s, t with $r \leqslant n$ and $s, t < p$, if we apply (1.8) with $\alpha > \log_p(\max\{n, p\})$ and $l = 0$ then we obtain Lucas' congruence $\binom{pn+s}{pr+t} \equiv \binom{n}{r}\binom{s}{t} \pmod{p}$. We conjecture that (1.8) (or its equivalent form (1.7)) also holds with $\alpha = 1$.

Let $p > 3$ be a prime. A well-known theorem of Wolstenholme asserts that $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$, i.e., $\binom{2p}{p} \equiv 2 \pmod{p^3}$. In 1952 W. Ljunggren (cf. [G]) generalized this as follows: $\binom{pn}{pr} \equiv \binom{n}{r} \pmod{p^3}$ for any $n, r \in \mathbb{N}$. Our following conjecture extends Ljunggren's result greatly.

Conjecture 1.1. *Let p be an odd prime, and let $\alpha \in \mathbb{Z}^+$, $n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then, for all $l \in \mathbb{N}$ we have*

$$T^{(p)}_{l,\alpha+1}(pn, pr) - T^{(p)}_{l,\alpha}(n, r) \equiv \begin{cases} 0 \pmod{p^3} & \text{if } p > 3, \\ 0 \pmod{p^2} & \text{if } p = 3. \end{cases}$$

Equivalently, for any $f(x) \in \mathbb{Z}_p[x]$ we have

$$\frac{1}{\lfloor n/p^{\alpha-1} \rfloor !} \sum_{k \equiv r \pmod{p^\alpha}} \left(\binom{pn}{pk} - \binom{n}{k} \right) (-1)^k f\left(\frac{k-r}{p^{\alpha-1}} \right) \equiv \begin{cases} 0 \pmod{p^3} & \text{if } p > 3, \\ 0 \pmod{p^2} & \text{if } p = 3. \end{cases}$$

Remark 1.5. The reason for the equivalence of the two parts in Conjecture 1.1 is as follows: For any $l \in \mathbb{N}$ we have

$$p^l x^l = \sum_{j=0}^{l} S(l,j) p^{l-j} j! p^j \binom{x}{j} \text{ and } l! p^l \binom{x}{l} = \sum_{j=0}^{l} (-1)^{l-j} s(l,j) p^{l-j} (p^j x^j),$$

where $s(l, j)$ $(0 \leqslant j \leqslant l)$ are Stirling numbers of the first kind.

The proof of Theorem 1.5 involves our following refinement of Weisman's result.

Theorem 1.7. *Let p be any prime, and let $\alpha, n \in \mathbb{N}$, $\alpha \geqslant 2$, $r, s, t \in \mathbb{Z}$ and $0 \leqslant s, t < p^{\alpha-2}$. Then*

$$\begin{aligned} &p^{-\left\lfloor \frac{p^{\alpha-2} n + s - p^{\alpha-1}}{\varphi(p^\alpha)} \right\rfloor} \sum_{k \equiv p^{\alpha-2} r + t \pmod{p^\alpha}} \binom{p^{\alpha-2} n + s}{k} (-1)^k \\ &\equiv (-1)^t \binom{s}{t} \left(p^{-\left\lfloor \frac{n-p}{\varphi(p^2)} \right\rfloor} \sum_{k \equiv r \pmod{p^2}} \binom{n}{k} (-1)^k \right) \pmod{p}. \end{aligned} \tag{1.9}$$

Here is a consequence of this theorem.

Corollary 1.2. *Let $\alpha \in \mathbb{Z}^+$, $n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then*

$$2^{-\left\lfloor \frac{n-2^{\alpha-1}}{\varphi(2^\alpha)} \right\rfloor} \sum_{k \equiv r \pmod{2^\alpha}} \binom{n}{k} \equiv 1 \pmod{2},$$

if and only if $\alpha = 1 \leqslant n$, or

$$\alpha \geqslant 2 \ \ \& \ \binom{\{n\}_{2^{\alpha-2}}}{\{r\}_{2^{\alpha-2}}} \equiv 1 \pmod{2}$$

and

$$n_* > 2 \ \& \ n_* \not\equiv 2r_* + 2 \pmod{4} \quad \text{or} \quad n_* = 2 \ \& \ 2 \mid r_*,$$

where $n_* = \lfloor n/2^{\alpha-2} \rfloor$ and $r_* = \lfloor r/2^{\alpha-2} \rfloor$.

As a complement to Theorem 1.7, we have the following conjecture.

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*

$$\begin{aligned} &p^{-\lfloor \frac{pn+s-p}{\varphi(p^2)} \rfloor} \sum_{k \equiv pr+t \pmod{p^2}} \binom{pn+s}{k}(-1)^k \\ \equiv &(-1)^t \binom{s}{t} p^{-\lfloor \frac{n-1}{p-1} \rfloor} \sum_{k \equiv r \pmod{p}} \binom{n}{k}(-1)^k \pmod{p} \end{aligned}$$

for every $t = 0, \ldots, p-1$. When $s \neq p-1$, $p \nmid n$ and $p-1 \mid n-1$, the least nonnegative residue of

$$p^{-\lfloor \frac{pn+s-p}{\varphi(p^2)} \rfloor} \sum_{k \equiv pr+t \pmod{p^2}} \binom{pn+s}{k}(-1)^k$$

modulo p does not depend on r for $t = s+1, \ldots, p-1$, and these residues form a permutation of $1, \ldots, p-1$ if $s = 0$.

Conjecture 5.2 of [DS] stated that the bound in the inequality (1.2) is attained if $f(x) = x^l$ and l satisfies a certain congruence equation. In the following result, we prove this conjecture when $p = 2$ and $r = 0$.

Theorem 1.8. *Let $\alpha \in \mathbb{N}$, $n \geqslant 2^\alpha$, $l \geqslant \lfloor n/2^\alpha \rfloor$ and*

$$l \equiv \left\lfloor \frac{n}{2^\alpha} \right\rfloor \left(\bmod\ 2^{\lfloor \log_2(n/2^\alpha) \rfloor} \right).$$

Then

$$\operatorname{ord}_2\Bigg(\sum_{k \equiv 0 \pmod{2^\alpha}} \binom{n}{k}(-1)^k \left(\frac{k}{2^\alpha}\right)^l \Bigg) = \operatorname{ord}_2\left(\left\lfloor \frac{n}{2^\alpha} \right\rfloor ! \right). \tag{1.10}$$

Remark 1.6. Theorem 1.8 in the case $\alpha = 0$ essentially asserts that if $n \in \mathbb{Z}^+$ and $q \in \mathbb{N}$ then $S(n + 2^{\lfloor \log_2 n \rfloor} q, n)$ is odd. This is because $\sum_{k=0}^{n} \binom{n}{k}(-1)^k k^l = (-1)^n n! S(l, n)$ for $l \in \mathbb{N}$ (cf. [LW, pp. 125–126]).

The following conjecture is a refinement of [DS, Conjecture 5.2].

Conjecture 1.3. *Let p be a prime, and $\alpha \geqslant 0$ and r be integers. Let $n \geqslant 2p^\alpha - 1$, $l \geqslant \lfloor n/p^\alpha \rfloor$ and*

$$l \equiv \left\lfloor \frac{r}{p^\alpha} \right\rfloor + \left\lfloor \frac{n-r}{p^\alpha} \right\rfloor \left(\bmod\ (p-1)p^{\lfloor \log_p(n/p^\alpha) \rfloor} \right).$$

Then

$$\frac{1}{\lfloor n/p^\alpha \rfloor ! \binom{n_*}{r_*}} \sum_{k \equiv r \pmod{p^\alpha}} \binom{n}{k}(-1)^k \left(\frac{k-r}{p^\alpha}\right)^l \equiv \pm 1 \pmod{p},$$

where $r_* = \{r\}_{p^\alpha}$ *and* $n_* = r_* + \{n-r\}_{p^\alpha}$. *When* $0 \leqslant r < p$ *the sign* $\pm$ *can be made explicitly by taking the value* $(-1)^{l+r}$.

For convenience, throughout this paper we use $[\![A]\!]$ to denote the characteristic function of an assertion A, i.e., $[\![A]\!]$ takes 1 or 0 according to whether A holds or not. For $m, n \in \mathbb{N}$ the Kronecker symbol $\delta_{m,n}$ stands for $[\![m = n]\!]$.

The next section is devoted to the proof of an equivalent version of Theorems 1.1–1.4. In Section 3 we will prove Theorem 1.7 and Corollary 1.2, and in Section 4 we establish Theorems 1.5 and 1.8.

2. Proof of Theorem 1.2

In this section we prove the following equivalent version of Theorem 1.2.

Theorem 2.1. *Let* p *be a prime, and let* $\alpha, l, n \in \mathbb{N}$. *Then, for all* $r \in \mathbb{Z}$, *we have*

$$\mathrm{ord}_p(T_l(n,r)) \geqslant \tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}), \tag{2.1}$$

where $T_l(n,r)$ *stands for* $T^{(p)}_{l,\alpha}(n,r)$ *given in Theorem 1.5.*

Lemma 2.1. *Theorem 2.1 holds in the case* $\alpha = 0$.

Proof. Clearly $\tau_p(\{r\}_{p^{-1}}, \{n-r\}_{p^{-1}}) = \tau_p(0,0) = 0$. Provided $\alpha = 0$ we have

$$T_l(n,r) = \frac{l!p^l}{\lfloor n/p^{-1}\rfloor!}\sum_{k=0}^{n}\binom{n}{k}(-1)^k\binom{k-r}{l} = \frac{l!p^l}{(pn)!}(-1)^n\binom{-r}{l-n},$$

where we have applied a known identity (cf. [GKP, (5.24)]) in the last step. If $l < n$, then $T_l(n,r) = 0 \in \mathbb{Z}_p$. When $l \geqslant n$, we also have $T_l(n,r) \in \mathbb{Z}_p$ because $\mathrm{ord}_p((pn)!) = n + \mathrm{ord}_p(n!) \leqslant l + \mathrm{ord}_p(l!)$. This ends the proof. □

For convenience, below we let p be a fixed prime and α be a positive integer.

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

$$T_l(n-1,r) - T_l(n-1,r-1) = \begin{cases} T_l(n,r) & \text{if } p^{\alpha-1} \nmid n, \\ \frac{n}{p^{\alpha-1}}T_l(n,r) & \text{otherwise.} \end{cases} \tag{2.2}$$

When $l > 0$, *we also have*

$$\begin{aligned} &T_l(n,r) + \frac{r}{p^{\alpha-1}}T_{l-1}(n,r+p^\alpha) \\ =&\begin{cases} -T_{l-1}(n-1,r+p^\alpha-1) & \text{if } p^{\alpha-1} \mid n, \\ -\frac{n}{p^{\alpha-1}}T_{l-1}(n-1,r+p^\alpha-1) & \text{otherwise.} \end{cases} \end{aligned} \tag{2.3}$$

Proof. Clearly

$$\begin{aligned}
&\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k\binom{(k-r)/p^\alpha}{l}\\
&\quad+\sum_{k\equiv r-1\,(\mathrm{mod}\ p^\alpha)}\binom{n-1}{k}(-1)^k\binom{(k-(r-1))/p^\alpha}{l}\\
=&\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k\binom{(k-r)/p^\alpha}{l}\\
&\quad-\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n-1}{k-1}(-1)^k\binom{(k-r)/p^\alpha}{l}\\
=&\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n-1}{k}(-1)^k\binom{(k-r)/p^\alpha}{l}.
\end{aligned}$$

Therefore

$$\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\,T_l(n,r)+\left\lfloor\frac{n-1}{p^{\alpha-1}}\right\rfloor!\,T_l(n-1,r-1)=\left\lfloor\frac{n-1}{p^{\alpha-1}}\right\rfloor!\,T_l(n-1,r)$$

and hence (2.2) follows.

Now let $l>0$. Note that

$$\begin{aligned}
&\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\frac{T_l(n,r)}{(l-1)!p^{l-1}}\\
=&lp\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k\frac{(k-r)/p^\alpha}{l}\binom{(k-r)/p^\alpha-1}{l-1}\\
=&\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k\left(\frac{k}{p^{\alpha-1}}-\frac{r}{p^{\alpha-1}}\right)\binom{(k-r-p^\alpha)/p^\alpha}{l-1}.
\end{aligned}$$

Using the identity $\binom{n}{k}k=n\binom{n-1}{k-1}$, we find that

$$\begin{aligned}
&\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\frac{T_l(n,r)}{(l-1)!p^{l-1}}\\
=&\frac{n}{p^{\alpha-1}}\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n-1}{k-1}(-1)^k\binom{(k-r-p^\alpha)/p^\alpha}{l-1}\\
&\quad-\frac{r}{p^{\alpha-1}}\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k\binom{(k-r-p^\alpha)/p^\alpha}{l-1}\\
=&\frac{n}{p^{\alpha-1}}\sum_{k\equiv r-1\,(\mathrm{mod}\ p^\alpha)}\binom{n-1}{k}(-1)^{k+1}\binom{(k-(r-1)-p^\alpha)/p^\alpha}{l-1}\\
&\quad-\frac{r}{p^{\alpha-1}}\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k\binom{(k-r-p^\alpha)/p^\alpha}{l-1}.
\end{aligned}$$

So we have

$$\left\lfloor \frac{n}{p^{\alpha-1}} \right\rfloor! \, T_l(n,r) = -\frac{n}{p^{\alpha-1}} \left\lfloor \frac{n-1}{p^{\alpha-1}} \right\rfloor! \, T_{l-1}(n-1, r+p^\alpha-1) - \frac{r}{p^{\alpha-1}} \left\lfloor \frac{n}{p^{\alpha-1}} \right\rfloor! \, T_{l-1}(n, r+p^\alpha),$$

which is equivalent to (2.3). □

Remark 2.1. Lemma 2.2 is not sufficient for an induction proof of Theorem 2.1; in fact we immediately encounter difficulty when $p^{\alpha-1} \mid n$ and $p^{\alpha-1} \nmid r$.

Lemma 2.3. *Let $d, m \in \mathbb{Z}^+$, $n \in \mathbb{N}$ and $r \in \mathbb{Z}$, and let $f(x)$ be a function from $\mathbb{Z}$ to the complex field. Then we have*

$$\sum_{k \equiv r \,(\mathrm{mod}\ d)} \binom{n}{k} (-1)^k f\left(\left\lfloor \frac{k-r}{m} \right\rfloor \right) = \sum_{j=0}^{n} \binom{n}{j} \Bigg(\sum_{i \equiv r \,(\mathrm{mod}\ d)} \binom{j}{i} (-1)^i \Bigg) \sum_{i=0}^{m-1} \sigma_{ij}, \tag{2.4}$$

where

$$\sigma_{ij} = \sum_{k \equiv r+i-j \,(\mathrm{mod}\ m)} \binom{n-j}{k} (-1)^k f\left(\frac{k-(r+i-j)}{m} \right). \tag{2.5}$$

Proof. Let ζ be a primitive dth root of unity. Given $0 \leqslant j \leqslant n$, we have

$$\begin{aligned} \sum_{i \equiv r \,(\mathrm{mod}\ d)} \binom{j}{i} (-1)^i &= \sum_{i=0}^{j} \binom{j}{i} \frac{(-1)^i}{d} \sum_{s=0}^{d-1} \zeta^{(i-r)s} \\ &= \frac{1}{d} \sum_{s=0}^{d-1} \zeta^{-rs} \sum_{i=0}^{j} \binom{j}{i} (-\zeta^s)^i \\ &= \frac{1}{d} \sum_{s=0}^{d-1} \zeta^{-rs} (1-\zeta^s)^j. \end{aligned}$$

Also,

$$\begin{aligned} \sum_{i=0}^{m-1} \sigma_{ij} &= \sum_{i=0}^{m-1} \sum_{k-(r-j) \equiv i \,(\mathrm{mod}\ m)} \binom{n-j}{k} (-1)^k f\left(\frac{k-(r-j)-i}{m} \right) \\ &= \sum_{i=0}^{m-1} \sum_{k-(r-j) \equiv i \,(\mathrm{mod}\ m)} \binom{n-j}{k} (-1)^k f\left(\left\lfloor \frac{k-(r-j)}{m} \right\rfloor \right) \\ &= \sum_{k=0}^{n-j} \binom{n-j}{k} (-1)^k f\left(\left\lfloor \frac{k+j-r}{m} \right\rfloor \right). \end{aligned}$$

Therefore

$$\begin{aligned}
&\sum_{j=0}^{n}\binom{n}{j}\Big(\sum_{i\equiv r\,(\mathrm{mod}\ d)}\binom{j}{i}(-1)^i\Big)\sum_{i=0}^{m-1}\sigma_{ij}\\
=&\sum_{j=0}^{n}\binom{n}{j}\frac{1}{d}\sum_{s=0}^{d-1}\zeta^{-rs}(1-\zeta^s)^j\sum_{k=j}^{n}\binom{n-j}{k-j}(-1)^{k-j}f\left(\left\lfloor\frac{k-r}{m}\right\rfloor\right)\\
=&\frac{1}{d}\sum_{s=0}^{d-1}\zeta^{-rs}\sum_{k=0}^{n}\binom{n}{k}(-1)^k f\left(\left\lfloor\frac{k-r}{m}\right\rfloor\right)\sum_{j=0}^{k}\binom{k}{j}(\zeta^s-1)^j\\
=&\sum_{k=0}^{n}\binom{n}{k}(-1)^k f\left(\left\lfloor\frac{k-r}{m}\right\rfloor\right)\frac{1}{d}\sum_{s=0}^{d-1}\zeta^{(k-r)s}\\
=&\sum_{k\equiv r\,(\mathrm{mod}\ d)}\binom{n}{k}(-1)^k f\left(\left\lfloor\frac{k-r}{m}\right\rfloor\right).
\end{aligned}$$

This proves (2.4). □

Lemma 2.4. *Let $l,n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Then*

$$T_l(n,r)=\sum_{i=0}^{p^\alpha-1}\sum_{j=0}^{n}c_\alpha(n,j)T_0(j,r)T_l(n-j,\,r+i-j),\tag{2.6}$$

where

$$c_\alpha(n,j):=\binom{n}{j}\frac{\lfloor j/p^{\alpha-1}\rfloor!\lfloor(n-j)/p^{\alpha-1}\rfloor!}{\lfloor n/p^{\alpha-1}\rfloor!}.\tag{2.7}$$

Proof. It suffices to apply Lemma 2.3 with $d=m=p^\alpha$ and $f(x)=\binom{x}{l}$. □

Lemma 2.5. *We have $c_\alpha(n,j)\in\mathbb{Z}_p$ for all $j=0,\ldots,n$.*

Proof. Clearly

$$\begin{aligned}
\mathrm{ord}_p(c_\alpha(n,j))=&\mathrm{ord}_p(n!)-\mathrm{ord}_p\left(\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\right)\\
&-\left(\mathrm{ord}_p(j!)-\mathrm{ord}_p\left(\left\lfloor\frac{j}{p^{\alpha-1}}\right\rfloor!\right)\right)\\
&-\left(\mathrm{ord}_p((n-j)!)-\mathrm{ord}_p\left(\left\lfloor\frac{n-j}{p^{\alpha-1}}\right\rfloor!\right)\right)\\
=&\sum_{0<s<\alpha}\left(\left\lfloor\frac{n}{p^s}\right\rfloor-\left\lfloor\frac{j}{p^s}\right\rfloor-\left\lfloor\frac{n-j}{p^s}\right\rfloor\right)\geqslant 0.
\end{aligned}$$

This concludes the proof. □

Proof of Theorem 2.1. Lemma 2.1 indicates that Theorem 2.1 holds when $\alpha = 0$. Below we let $\alpha > 0$.

Step I. Use induction on $l+n$ to show that $T_l(n,r) \in \mathbb{Z}_p$ for any $r \in \mathbb{Z}$.

The case $l = n = 0$ is trivial since $T_0(0,r) \in \mathbb{Z}$.

Now let $l+n > 0$, and assume that $T_{l_*}(n_*, r_*) \in \mathbb{Z}_p$ whenever $l_*, n_* \in \mathbb{N}$, $l_* + n_* < l + n$ and $r_* \in \mathbb{Z}$.

`Case 1`. $l = 0$. By Weisman's result mentioned in the first section (see also, [S05]),

$$\operatorname{ord}_p\bigg(\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k\bigg) \geqslant \left\lfloor \frac{n-p^{\alpha-1}}{\varphi(p^\alpha)}\right\rfloor = \left\lfloor \frac{n/p^{\alpha-1}-1}{p-1}\right\rfloor = \left\lfloor \frac{n_0-1}{p-1}\right\rfloor$$

where $n_0 = \lfloor n/p^{\alpha-1}\rfloor$. If $n_0 > 0$, then $\operatorname{ord}_p(n_0!) \leqslant \lfloor (n_0-1)/(p-1)\rfloor$ (as mentioned in the first section), hence

$$T_0(n,r) = \frac{1}{n_0!}\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k \in \mathbb{Z}_p.$$

Clearly this also holds when $n_0 = 0$.

`Case 2`. $l > 0$ and $p^\alpha \nmid r$. In this case, $T_0(0,r)$ vanishes. Thus, by Lemmas 2.4–2.5 and the induction hypothesis, we have

$$T_l(n,r) = \sum_{i=0}^{p^\alpha-1}\sum_{0<j\leqslant n} c_\alpha(n,j)T_0(j,r)T_l(n-j,\ r+i-j) \in \mathbb{Z}_p. \tag{2.8}$$

`Case 3`. $l > 0$ and $p^\alpha \mid r$. If $p^{\alpha-1} \nmid n$,

$$T_l(n,r) = T_l(n-1,r) - T_l(n-1,r-1) \in \mathbb{Z}_p$$

by (2.2) and the induction hypothesis. If $p^{\alpha-1} \mid n$ and $n \neq 0$, then

$$T_l(n,r) = -\frac{r}{p^{\alpha-1}}T_{l-1}(n,r+p^\alpha) - T_{l-1}(n-1,r+p^\alpha-1) \in \mathbb{Z}_p \tag{2.9}$$

by (2.3) and the induction hypothesis. Note also that $T_l(0,r) \in \mathbb{Z}_p$.

In view of the above, we have finished the first step.

Step II. Use induction on n to prove (2.1) for any $r \in \mathbb{Z}$.

If $p^\alpha \nmid r$, then $T_l(0,r) = 0$; if $p^\alpha \mid r$ then $\tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}) = 0$. So (2.1) holds when $n = 0$.

Now let $n > 0$ and $\tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}) \neq 0$. Then both $\mathrm{ord}_p(r)$ and $\mathrm{ord}_p(n-r)$ are smaller than $\alpha - 1$. Assume that (2.1) with n replaced by $n-1$ holds for all $r \in \mathbb{Z}$. For $r' = n - r - (l-1)p^\alpha$, we have

$$\begin{aligned}\tau_p\left(\{r'\}_{p^{\alpha-1}}, \{n-r'\}_{p^{\alpha-1}}\right) =&\tau_p\left(\{n-r\}_{p^{\alpha-1}}, \{r\}_{p^{\alpha-1}}\right)\\ =&\tau_p\left(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}\right)\end{aligned}$$

and

$$\begin{aligned}T_l(n,r') =&\frac{l!p^l}{\lfloor n/p^{\alpha-1}\rfloor!}\sum_{k\equiv r' \ (\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k\binom{(n-r'-(n-k))/p^\alpha}{l}\\ =&\frac{l!p^l}{\lfloor n/p^{\alpha-1}\rfloor!}\sum_{k\equiv n-r' \ (\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^{n-k}\binom{(n-r'-k)/p^\alpha}{l}\\ =&\frac{(-1)^{l+n}l!p^l}{\lfloor n/p^{\alpha-1}\rfloor!}\sum_{k\equiv r \ (\mathrm{mod}\ p^\alpha)}\binom{n}{k}(-1)^k\binom{(k-(n-r'))/p^\alpha+l-1}{l}\\ =&(-1)^{l+n}T_l(n,r);\end{aligned}$$

also, $\mathrm{ord}_p(r') = \mathrm{ord}_p(n-r) = \mathrm{ord}_p(n)$ if $\mathrm{ord}_p(r) > \mathrm{ord}_p(n)$. Thus, without loss of generality, below we simply let $\mathrm{ord}_p(r) \leqslant \mathrm{ord}_p(n)$.

In view of Lemma 2.2,

$$T_{l+1}(n, r-p^\alpha) + \frac{r-p^\alpha}{p^{\alpha-1}}T_l(n,r) = \begin{cases} -T_l(n-1,r-1) & \text{if } p^{\alpha-1} \mid n,\\ -\frac{n}{p^{\alpha-1}}T_l(n-1,r-1) & \text{otherwise.}\end{cases}$$

As $T_{l+1}(n, r-p^\alpha) \in \mathbb{Z}_p$, and

$$\mathrm{ord}_p(T_l(n-1,r-1)) \geqslant \tau_p(\{r-1\}_{p^{\alpha-1}}, \{n-1-(r-1)\}_{p^{\alpha-1}}) \geqslant 0$$

by the induction hypothesis, we have

$$\begin{aligned}\mathrm{ord}_p(rT_l(n,r)) &\geqslant \min\{\alpha-1, \mathrm{ord}_p(nT_l(n-1,r-1))\}\\ &\geqslant \min\{\alpha-1, \mathrm{ord}_p(n) + \tau_p(\{r-1\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}})\}.\end{aligned}$$

By the definition of τ_p,

$$\tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}) \leqslant \alpha - 1 - \mathrm{ord}_p(r)$$

and also

$$\tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}) \leqslant \tau_p(\{r-1\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}) + \mathrm{ord}_p(n) - \mathrm{ord}_p(r).$$

(Note that $\{r\}_{p^{\alpha-1}} + \{n-r\}_{p^{\alpha-1}} \equiv n \pmod{p^{\alpha-1}}$.) So, (2.1) follows from the above.

The proof of Theorem 2.1 is now complete. □

3. Proofs of Theorems 1.7 and Corollary 1.2

To prove Theorem 1.7 and Corollary 1.2, we need to establish an auxiliary theorem first.

Lemma 3.1. *Let $m \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$ be relatively prime. Then, for any $n \in \mathbb{Z}^+$, we have*

$$\frac{1}{n}\sum_{k=0}^{n-1}\frac{1}{km+r} \equiv \frac{1}{r} + \frac{m}{2}[\![2 \mid n]\!] \pmod{m}. \tag{3.1}$$

Proof. We use induction on n.

If n is relatively prime to m (e.g., $n = 1$), then 2 cannot divide both m and n, hence

$$\frac{1}{n}\sum_{k=0}^{n-1}\frac{1}{km+r} \equiv \frac{1}{n}\sum_{k=0}^{n-1}\frac{1}{r} \equiv \frac{1}{r} + \frac{m}{2}[\![2 \mid n]\!] \pmod{m}.$$

Now suppose that p is a common prime divisor of m and n, and set $n_0 = n/p$. Then

$$\sum_{k=0}^{n-1}\frac{1}{km+r} = \sum_{i=0}^{n_0-1}\sum_{j=0}^{p-1}\frac{1}{(i+jn_0)m+r} = \sum_{i=0}^{n_0-1}\sum_{j=0}^{p-1}\frac{1}{im+jmn_0+r}.$$

For any $i = 0, \ldots, n_0 - 1$, clearly

$$\begin{aligned}
&\frac{1}{n}\sum_{j=0}^{p-1}\left(\frac{1}{im+jmn_0+r} - \frac{1}{im+r}\right)\\
=&\frac{1}{n}\sum_{j=0}^{p-1}\frac{-jmn/p}{(im+jmn_0+r)(im+r)}\\
\equiv& -\sum_{j=0}^{p-1}\frac{jm/p}{r^2} = -\frac{p-1}{2}\cdot\frac{m}{r^2} \equiv \delta_{p,2}\frac{m}{2} \pmod{m}.
\end{aligned}$$

Therefore

$$\begin{aligned}
\frac{1}{n}\sum_{k=0}^{n-1}\frac{1}{km+r} \equiv& \sum_{i=0}^{n_0-1}\left(\frac{1}{n}\sum_{j=0}^{p-1}\frac{1}{im+r} + \delta_{p,2}\frac{m}{2}\right)\\
\equiv&\frac{1}{n_0}\sum_{i=0}^{n_0-1}\frac{1}{im+r} + \delta_{p,2}\frac{m}{2}\cdot\frac{n}{2} \pmod{m}.
\end{aligned}$$

Note that $n_0 < n$. If

$$\frac{1}{n_0}\sum_{i=0}^{n_0-1}\frac{1}{im+r} \equiv \frac{1}{r} + \frac{m}{2}[\![2 \mid n_0]\!] \pmod{m},$$

then (3.1) holds by the above, because

$$\delta_{p,2}\frac{m}{2}\cdot\frac{n}{2} + \frac{m}{2}[\![2 \mid n_0]\!] \equiv \delta_{p,2}\frac{m}{2}([\![4 \mid n-2]\!] + [\![4 \mid n]\!]) \equiv \frac{m}{2}[\![2 \mid n]\!] \pmod{m}.$$

This concludes the induction proof. □

Remark 3.1. Lemma 3.1 can be further extended by considering the arithmetic mean $\frac{1}{n}\sum_{k=0}^{n-1}(km+r)^l$ modulo m via the same method.

Lemma 3.2. *Let p be a prime, and let $k \in \mathbb{N}$ and $n \in \mathbb{Z}^+$. If p is odd, then*

$$\binom{pn}{pk} \equiv \binom{n}{k} \left(\mathrm{mod}\ p^{2\mathrm{ord}_p(n)+2}\right). \tag{3.2}$$

For $p = 2$ we have

$$\binom{2n}{2k} \equiv (-1)^k\binom{n}{k} \left(\mathrm{mod}\ 2^{2\mathrm{ord}_2(n)+1}\right). \tag{3.3}$$

Proof. The case $k = 0$ or $k \geqslant n$ is trivial. Below we let $0 < k < n$.

By a result of Jacobsthal (see, e.g., [G]), if $p > 3$, then

$$\binom{pn}{pk}\Big/\binom{n}{k} = 1 + p^3nk(n-k)q$$

for some $q \in \mathbb{Z}_p$, and hence

$$\begin{aligned}\binom{pn}{pk} - \binom{n}{k} =&\binom{n}{k}p^3nk(n-k)q = p^3n^2\binom{n-1}{k-1}(n-k)q\\ \equiv&0 \left(\mathrm{mod}\ p^{3+2\mathrm{ord}_p(n)}\right).\end{aligned}$$

Now we handle the case $p = 3$. Observe that

$$\begin{aligned}\binom{3n}{3k}\Big/\binom{n}{k} =&\frac{(3n-1)(3n-2)}{1\cdot 2} \times \frac{(3n-4)(3n-5)}{4\cdot 5}\\ &\times\cdots\times\frac{(3n-(3k-2))(3n-(3k-1))}{(3k-2)(3k-1)}\end{aligned}$$

and

$$(3n-(3i+1))(3n-(3i+2)) = 9n^2 - 9n(2i+1) + (3i+1)(3i+2)$$

for any $i \in \mathbb{Z}$. So we have

$$\binom{3n}{3k}\Big/\binom{n}{k} = \prod_{i=0}^{k-1}\left(1 + 9n\frac{n-2i-1}{(3i+1)(3i+2)}\right)$$
$$\equiv 1 + 9n\sum_{i=0}^{k-1}\frac{n-2i-1}{(3i+1)(3i+2)} \pmod{(3^{2+\mathrm{ord}_3(n)})^2}.$$

Clearly

$$\sum_{i=0}^{k-1}\frac{n-2i-1}{(3i+1)(3i+2)} = \sum_{i=0}^{k-1}\left(\frac{n-2i-1}{3i+1} - \frac{n-2i-1}{3i+2}\right)$$
$$= \sum_{i=0}^{k-1}\left(\frac{n-2i-1}{3i+1} - \frac{n-2(k-1-i)-1}{3(k-1-i)+2}\right)$$

and hence

$$\frac{1}{k}\sum_{i=0}^{k-1}\frac{n-2i-1}{(3i+1)(3i+2)}$$
$$= \frac{1}{k}\sum_{i=0}^{k-1}\left(\frac{n-(2i+1)}{3i+1} - \frac{n+(2i+1)-2k}{3k-(3i+1)}\right)$$
$$= \frac{1}{k}\sum_{i=0}^{k-1}\frac{3k(n-(2i+1)) + 2k(3i+1) - 2n(3i+1)}{(3i+1)(3k-3i-1)}$$
$$= \sum_{i=0}^{k-1}\frac{3n-1}{(3i+1)(3k-3i-1)} - \frac{2n}{k}\sum_{i=0}^{k-1}\frac{1}{3(k-1-i)+2}$$
$$\equiv \sum_{i=0}^{k-1}\frac{-1}{-1} - 2n \times \frac{1}{2} = k - n \pmod{3},$$

where we have applied Lemma 3.1 with $m = 3$ to get the last congruence. Therefore

$$\binom{3n}{3k} \equiv \binom{n}{k} + 9n\frac{n}{k}\binom{n-1}{k-1}\sum_{i=0}^{k-1}\frac{n-2i-1}{(3i+1)(3i+2)} \pmod{3^{2\mathrm{ord}_3(n)+4}}$$
$$\equiv \binom{n}{k} + 9n^2\binom{n-1}{k-1}(k-n) \pmod{3^{2\mathrm{ord}_3(n)+3}}$$
$$\equiv \binom{n}{k} \pmod{3^{2\mathrm{ord}_3(n)+2}}.$$

Finally we consider the case $p=2$. Observe that

$$\frac{\binom{2n}{2k}}{\binom{n}{k}}=\prod_{j=0}^{k-1}\frac{2n-(2j+1)}{2j+1}=(-1)^k\prod_{j=0}^{k-1}\left(1-\frac{2n}{2j+1}\right)$$
$$\equiv(-1)^k\left(1-2n\sum_{j=0}^{k-1}\frac{1}{2j+1}\right)\ \left(\mathrm{mod}\ (2^{\mathrm{ord}_2(n)+1})^2\right).$$

This, together with Lemma 3.1 in the case $m=2$, yields that

$$\binom{2n}{2k}\equiv(-1)^k\left(\binom{n}{k}-\frac{2n^2}{k}\binom{n-1}{k-1}\sum_{j=0}^{k-1}\frac{1}{2j+1}\right)\ \left(\mathrm{mod}\ 2^{2\mathrm{ord}_2(n)+2}\right)$$
$$\equiv(-1)^k\binom{n}{k}-(-1)^k2n^2\binom{n-1}{k-1}(1+[\![2\mid k]\!])\ \left(\mathrm{mod}\ 2^{2\mathrm{ord}_2(n)+2}\right)$$
$$\equiv(-1)^k\binom{n}{k}\ \left(\mathrm{mod}\ 2^{2\mathrm{ord}_2(n)+1}\right).$$

We are done. □

If p is a prime, and $\alpha,n\in\mathbb{N}$ and $r\in\mathbb{Z}$, then

$$\mathrm{ord}_p\Bigg(\sum_{k\equiv r\ (\mathrm{mod}\ p^\alpha)}\binom{p^{\alpha-1}n}{k}(-1)^k\Bigg)\geqslant\left\lfloor\frac{p^{\alpha-1}n-p^{\alpha-1}}{\varphi(p^\alpha)}\right\rfloor=\left\lfloor\frac{n-1}{p-1}\right\rfloor$$

by Weisman's result, and hence

$$S_\alpha^{(p)}(n,r):=p^{-\lfloor\frac{n-1}{p-1}\rfloor}\sum_{k\equiv r\ (\mathrm{mod}\ p^\alpha)}\binom{p^{\alpha-1}n}{k}(-1)^k \tag{3.4}$$

is an integer.

Theorem 3.1. *Let p be a prime. Then, for each $\alpha=2,3,\ldots,$ whenever $n\in\mathbb{N}$ and $r\in\mathbb{Z}$ we have*

$$S_\alpha^{(p)}(n,r)\equiv\begin{cases}S_{\alpha-1}^{(p)}(n,r/p)\ (\mathrm{mod}\ p^{(2-\delta_{p,2})(\alpha-2)}) & \text{if } p\mid r,\\ 0\ (\mathrm{mod}\ p^{\alpha-2}) & \text{otherwise,}\end{cases} \tag{3.5}$$

where $S_\alpha^{(p)}(n,r)$ is defined by (3.4).

Proof. We use induction on α and write $S_\alpha(n,r)$ for $S_\alpha^{(p)}(n,r)$.

When $\alpha=2$ we need do nothing.

Now let $\alpha>2$ and assume the desired result for $\alpha-1$. We use induction on n to prove that (3.5) holds for any $r\in\mathbb{Z}$.

First we consider the case $n<p$. Note that $\lfloor (n-1)/(p-1)\rfloor=-1$ and $p^{\alpha-1}n<p^\alpha$. Thus

$$S_\alpha(n,r)=p\binom{p^{\alpha-1}n}{\{r\}_{p^\alpha}}(-1)^{\{r\}_{p^\alpha}}.$$

If $p\nmid r$, then

$$\binom{p^{\alpha-1}n}{\{r\}_{p^\alpha}}=\frac{p^{\alpha-1}n}{\{r\}_{p^\alpha}}\binom{p^{\alpha-1}n-1}{\{r\}_{p^\alpha}-1}\equiv 0 \pmod{p^{\alpha-1}}$$

and hence $S_\alpha(n,r)\equiv 0 \pmod{p^\alpha}$. When $p\mid r$, by Lemma 3.2 we have

$$\begin{aligned}&(-1)^{\{r\}_{p^\alpha}-\{r/p\}_{p^{\alpha-1}}}\binom{p^{\alpha-2}n}{\{r/p\}_{p^{\alpha-1}}}\\ =&(-1)^{(p-1)\{r\}_{p^\alpha}/p}\binom{p^{\alpha-2}n}{\{r\}_{p^\alpha}/p}\equiv\binom{p^{\alpha-1}n}{\{r\}_{p^\alpha}}\ \left(\mathrm{mod}\ p^{2(\alpha-2)+1}\right),\end{aligned}$$

thus $S_\alpha(n,r)\equiv S_{\alpha-1}(n,r/p) \pmod{p^{2(\alpha-1)}}$.

Below we let $n\geqslant p$, and assume that (3.5) is valid for all $r\in\mathbb{Z}$ if we replace n in (3.5) by a smaller nonnegative integer. Set $n'=n-(p-1)\geqslant 1$. Then, by Vandermonde's identity $\binom{x+y}{k}=\sum_{j\in\mathbb{N}}\binom{x}{j}\binom{y}{k-j}$ (cf. [GKP]), we have

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

If $0\leqslant j\leqslant\varphi(p^\alpha)$ and $p\nmid j$, then

$$\frac{1}{p}\binom{\varphi(p^\alpha)}{j}=\frac{p^{\alpha-1}(p-1)}{pj}\binom{\varphi(p^\alpha)-1}{j-1}\equiv 0 \pmod{p^{\alpha-2}},$$

and also $S_\alpha(n',r-j)\equiv 0 \pmod{p^{\alpha-2}}$ (by the induction hypothesis) providing $p\mid r$. Thus

$$S_\alpha(n,r)\equiv\sum_{j=0}^{\varphi(p^{\alpha-1})}\frac{(-1)^{pj}}{p}\binom{\varphi(p^\alpha)}{pj}S_\alpha(n',r-pj)\ \left(\mathrm{mod}\ p^{(1+[\![p|r]\!])(\alpha-2)}\right).$$

Note that when $j\not\equiv 0 \pmod{p^{\alpha-2}}$ we have

$$\frac{1}{p}\binom{\varphi(p^\alpha)}{pj}=\frac{p^{\alpha-1}(p-1)}{p^2j}\binom{\varphi(p^\alpha)-1}{pj-1}\in\mathbb{Z}_p.$$

`Case I.` $p\nmid r$. By the induction hypothesis, $p^{\alpha-2}\mid S_\alpha(n',r-pj)$ for all $j\in\mathbb{Z}$. Thus, by the above,

$$S_\alpha(n,r)\equiv\sum_{j=0}^{p-1}\frac{(-1)^{p^{\alpha-1}j}}{p}\binom{\varphi(p^\alpha)}{p^{\alpha-1}j}S_\alpha(n',r-p^{\alpha-1}j)\ (\mathrm{mod}\ p^{\alpha-2}).$$

In view of Lucas' theorem,

$$\binom{p^{\alpha-1}(p-1)}{p^{\alpha-1}j}\equiv\binom{p^{\alpha-2}(p-1)}{p^{\alpha-2}j}\equiv\cdots\equiv\binom{p-1}{j}\equiv(-1)^j\ (\mathrm{mod}\ p)$$

for every $j=0,\dots,p-1$. Note also that $(-1)^j\equiv1\ (\mathrm{mod}\ 2)$. So we have

$$S_\alpha(n,r)\equiv\frac{1}{p}\sum_{j=0}^{p-1}S_\alpha(n',r-p^{\alpha-1}j)\ \ (\mathrm{mod}\ p^{\alpha-2}).$$

Observe that

$$\begin{aligned}&\sum_{j=0}^{p-1}S_\alpha(n',r-p^{\alpha-1}j)\\ =&p^{-\lfloor\frac{n'-1}{p-1}\rfloor}\sum_{k\equiv r\,(\mathrm{mod}\ p^{\alpha-1})}\binom{p^{\alpha-2}pn'}{k}(-1)^k\\ =&p^{-\lfloor\frac{n'-1}{p-1}\rfloor}p^{\lfloor\frac{pn'-1}{p-1}\rfloor}S_{\alpha-1}(pn',r)=p^{n'}S_{\alpha-1}(pn',r).\end{aligned}$$

Therefore

$$S_\alpha(n,r)\equiv p^{n'-1}S_{\alpha-1}(pn',r)\ \ \left(\mathrm{mod}\ p^{\alpha-2}\right).$$

By the induction hypothesis for $\alpha-1$, we have $p^{\alpha-3}\mid S_{\alpha-1}(pn',r)$, hence $S_\alpha(n,r)\equiv0\ (\mathrm{mod}\ p^{\alpha-2})$ if $n'>1$. In the case $n'=1$, we need to show that $S_{\alpha-1}(p,r)\equiv0\ (\mathrm{mod}\ p^{\alpha-2})$. In fact,

$$\begin{aligned}S_{\alpha-1}(p,r)=&p^{-\lfloor\frac{p-1}{p-1}\rfloor}\sum_{k\equiv r\,(\mathrm{mod}\ p^{\alpha-1})}\binom{p^{\alpha-2}p}{k}(-1)^k\\ =&\sum_{k\equiv r\,(\mathrm{mod}\ p^{\alpha-1})}\frac{p^{\alpha-2}}{k}\binom{p^{\alpha-1}-1}{k-1}(-1)^k\equiv0\ (\mathrm{mod}\ p^{\alpha-2}).\end{aligned}$$

(Note that if $k\equiv r\ (\mathrm{mod}\ p^{\alpha-1})$ then $p\nmid k$ since $p\nmid r$.)

`Case II`. $p \mid r$. In this case,

$$\begin{aligned}
&S_\alpha(n,r) - S_{\alpha-1}\left(n, \frac{r}{p}\right) \\
\equiv &\sum_{j=0}^{\varphi(p^{\alpha-1})} \frac{(-1)^{pj}}{p} \binom{\varphi(p^\alpha)}{pj} S_\alpha(n', r-pj) \\
&- \sum_{j=0}^{\varphi(p^{\alpha-1})} \frac{(-1)^j}{p} \binom{\varphi(p^{\alpha-1})}{j} S_{\alpha-1}\left(n', \frac{r}{p} - j\right) \ \left(\mathrm{mod}\ p^{2(\alpha-2)}\right).
\end{aligned}$$

By Lemma 3.2,

$$\binom{p^{\alpha-1}(p-1)}{pj} \equiv (-1)^{(p-1)j} \binom{p^{\alpha-2}(p-1)}{j} \ \left(\mathrm{mod}\ p^{(2-\delta_{p,2})(\alpha-2)+2}\right).$$

Thus $S_\alpha(n,r) - S_{\alpha-1}(n, r/p)$ is congruent to

$$\sum_{j=0}^{\varphi(p^{\alpha-1})} \frac{(-1)^j}{p} \binom{\varphi(p^{\alpha-1})}{j} \left(S_\alpha(n', r-pj) - S_{\alpha-1}\left(n', \frac{r}{p} - j\right)\right)$$

modulo $p^{(2-\delta_{p,2})(\alpha-2)}$. If $p^{\alpha-2} \nmid j$, then

$$\frac{1}{p}\binom{\varphi(p^{\alpha-1})}{j} = \frac{p^{\alpha-2}(p-1)}{pj} \binom{\varphi(p^{\alpha-1})-1}{j-1} \in \mathbb{Z}_p.$$

Since $S_\alpha(n', r-pj) \equiv S_{\alpha-1}(n', r/p-j) \ (\mathrm{mod}\ p^{(2-\delta_{p,2})(\alpha-2)})$ by the induction hypothesis, and $-1 \equiv 1 \ (\mathrm{mod}\ 2)$, we have

$$\begin{aligned}
&S_\alpha(n,r) - S_{\alpha-1}\left(n, \frac{r}{p}\right) \\
\equiv &\sum_{j=0}^{p-1} \frac{(-1)^j}{p} \binom{\varphi(p^{\alpha-1})}{p^{\alpha-2}j} \left(S_\alpha(n', r-p^{\alpha-1}j) - S_{\alpha-1}\left(n', \frac{r}{p} - p^{\alpha-2}j\right)\right) \\
\equiv &\sum_{j=0}^{p-1} \frac{S_\alpha(n', r-p^{\alpha-1}j) - S_{\alpha-1}(n', r/p - p^{\alpha-2}j)}{p} \ \left(\mathrm{mod}\ p^{(2-\delta_{p,2})(\alpha-2)}\right),
\end{aligned}$$

where we have used the fact that $\binom{p^{\alpha-2}(p-1)}{p^{\alpha-2}j} \equiv \binom{p-1}{j} \equiv (-1)^j \ (\mathrm{mod}\ p)$ for $0 \leqslant j \leqslant p-1$. As in Case I,

$$\sum_{j=0}^{p-1} S_\alpha(n', r-p^{\alpha-1}j) = p^{n'} S_{\alpha-1}(pn', r)$$

and

$$S_{\alpha-1}\left(n', \frac{r}{p} - p^{\alpha-2}j\right) = p^{n'} S_{\alpha-2}\left(pn', \frac{r}{p}\right).$$

Thus

$$\begin{aligned}&S_\alpha(n,r) - S_{\alpha-1}\left(n, \frac{r}{p}\right)\\ \equiv &p^{n'-1}\left(S_{\alpha-1}(pn',r) - S_{\alpha-2}\left(pn', \frac{r}{p}\right)\right) \ \left(\mathrm{mod}\ p^{(2-\delta_{p,2})(\alpha-2)}\right).\end{aligned}$$

By the induction hypothesis for $\alpha-1$, $S_{\alpha-1}(pn',r)$ and $S_{\alpha-2}(pn',r/p)$ are congruent modulo $p^{(2-\delta_{p,2})(\alpha-3)}$. Therefore, if $n'>2$ then

$$S_\alpha(n,r) \equiv S_{\alpha-1}\left(n, \frac{r}{p}\right) \ \left(\mathrm{mod}\ p^{(2-\delta_{p,2})(\alpha-2)}\right).$$

When $n' \in \{1,2\}$, we have $n'-1-\lfloor (pn'-1)/(p-1)\rfloor \geqslant -2$ and also

$$\begin{aligned}&\sum_{k\equiv r\ (\mathrm{mod}\ p^{\alpha-1})} \binom{p^{\alpha-1}n'}{k}(-1)^k - \sum_{k\equiv r/p\ (\mathrm{mod}\ p^{\alpha-2})} \binom{p^{\alpha-2}n'}{k}(-1)^k\\ =&\sum_{k\equiv r/p\ (\mathrm{mod}\ p^{\alpha-2})}\left(\binom{p^{\alpha-1}n'}{pk}(-1)^{pk} - \binom{p^{\alpha-2}n'}{k}(-1)^k\right).\end{aligned}$$

By Lemma 3.2, the last sum is a multiple of

$$p^{2(\alpha-2)+2-\delta_{p,2}} = p^{(2-\delta_{p,2})(\alpha-2)} p^{2+\delta_{p,2}(\alpha-3)}.$$

So we also have the desired result in the case $n' \leqslant 2$.

The induction proof of Theorem 3.1 is now complete. □

We believe that (3.5) in the case $p \mid r$ can be improved slightly. Here is our conjecture.

Conjecture 3.1. *Let p be an odd prime, and let $\alpha \geqslant 2$ be an integer. If $n\in\mathbb{N}$ and $r\in\mathbb{Z}$, then*

$$S_\alpha^{(p)}(n,pr) \equiv S_{\alpha-1}^{(p)}(n,r) \pmod{p^{2\alpha-2-\delta_{p,3}}}.$$

Now we give a useful consequence of Theorem 3.1.

Corollary 3.1. *Let p be a prime, and let $\alpha,\beta,n\in\mathbb{N}$ with $\alpha-\beta\geqslant 2$. Given $r\in\mathbb{Z}$ we have*

$$S_\alpha^{(p)}(n,p^\beta r) \equiv S_{\alpha-\beta}^{(p)}(n,r) \ \left(\mathrm{mod}\ p^{(2-\delta_{p,2})(\alpha-\beta-1)}\right). \tag{3.6}$$

Provided $r \not\equiv 0 \pmod p$ *we also have*

$$S_\alpha^{(p)}(n, p^\beta r) \equiv 0 \pmod{p^{\alpha-\beta-2}}. \tag{3.7}$$

Proof. By Theorem 3.1, if $0 \leqslant j < \beta$ then

$$S_{\alpha-j}^{(p)}(n, p^{\beta-j}r) \equiv S_{\alpha-j-1}^{(p)}(n, p^{\beta-j-1}r) \pmod{p^{(2-\delta_{p,2})(\alpha-j-2)}}.$$

So (3.6) follows.

If $p \nmid r$, then $S_{\alpha-\beta}^{(p)}(n, r) \equiv 0 \pmod{p^{\alpha-\beta-2}}$ by Theorem 3.1, combining this with (3.6) we immediately obtain (3.7). □

Proof of Theorem 1.7. Write $n = pn_0 + s_0$ with $n_0, s_0 \in \mathbb{N}$ and $s_0 < p$. Then

$$\left\lfloor \frac{p^{\alpha-2}n + s - p^{\alpha-1}}{\varphi(p^\alpha)} \right\rfloor = \left\lfloor \frac{n + s/p^{\alpha-2} - p}{\varphi(p^2)} \right\rfloor = \left\lfloor \frac{n-p}{\varphi(p^2)} \right\rfloor$$
$$= \left\lfloor \frac{n/p - 1}{p-1} \right\rfloor = \left\lfloor \frac{n_0 - 1}{p-1} \right\rfloor.$$

By Vandermonde's identity,

$$\sum_{k \equiv p^{\alpha-2}r+t \,(\mathrm{mod}\ p^\alpha)} \binom{p^{\alpha-2}n+s}{k}(-1)^k$$
$$= \sum_{k \equiv p^{\alpha-2}r+t \,(\mathrm{mod}\ p^\alpha)} \sum_{j \in \mathbb{N}} \binom{p^{\alpha-2}s_0+s}{j}\binom{p^{\alpha-1}n_0}{k-j}(-1)^k$$
$$= \sum_{j \in \mathbb{N}} \binom{p^{\alpha-2}s_0+s}{j}(-1)^j \sum_{k \equiv p^{\alpha-2}r+t-j \,(\mathrm{mod}\ p^\alpha)} \binom{p^{\alpha-1}n_0}{k}(-1)^k.$$

In light of Corollary 3.1, for any $r' \in \mathbb{Z}$ we have

$$S_\alpha(n_0, r') \equiv \begin{cases} S_2(n_0, r'/p^{\alpha-2}) \pmod{p^{2-\delta_{p,2}}} & \text{if } r' \equiv 0 \pmod{p^{\alpha-2}}, \\ 0 \pmod p & \text{if } \mathrm{ord}_p(r') < \alpha - 2. \end{cases}$$

Thus

$$p^{-\lfloor \frac{n_0-1}{p-1} \rfloor} \sum_{k \equiv p^{\alpha-2}r+t \,(\mathrm{mod}\ p^\alpha)} \binom{p^{\alpha-2}n+s}{k}(-1)^k$$
$$\equiv \sum_{i \in \mathbb{N}} \binom{p^{\alpha-2}s_0+s}{p^{\alpha-2}i+t}(-1)^{p^{\alpha-2}i+t} p^{-\lfloor \frac{n_0-1}{p-1} \rfloor} \sum_{k \equiv r-i \,(\mathrm{mod}\ p^2)} \binom{pn_0}{k}(-1)^k$$
$$\equiv \sum_{i \in \mathbb{N}} \binom{s_0}{i}\binom{s}{t}(-1)^{i+t} p^{-\lfloor \frac{n_0-1}{p-1} \rfloor} \sum_{k \equiv r-i \,(\mathrm{mod}\ p^2)} \binom{pn_0}{k}(-1)^k \pmod p$$

where we have applied Lucas' theorem in the last step. (Note that $s = t = 0$ if $\alpha = 2$, also $-1 \equiv 1 \pmod 2$.) Since

$$\begin{aligned}&\sum_{i=0}^{s_0}\binom{s_0}{i}(-1)^i\sum_{k\equiv r-i\,(\mathrm{mod}\ p^2)}\binom{pn_0}{k}(-1)^k\\ =&\sum_{i=0}^{s_0}\binom{s_0}{i}\sum_{k\equiv r\,(\mathrm{mod}\ p^2)}\binom{pn_0}{k-i}(-1)^k\\ =&\sum_{k\equiv r\,(\mathrm{mod}\ p^2)}\binom{pn_0+s_0}{k}(-1)^k=\sum_{k\equiv r\,(\mathrm{mod}\ p^2)}\binom{n}{k}(-1)^k,\end{aligned}$$

the desired result follows from the above. □

Proof of Corollary 1.2. The case $\alpha = 1$ is easy, because $\sum_{k\equiv r\,(\mathrm{mod}\ 2)}\binom{n}{k} = 2^{n-1}$ if $n > 0$.

Now let $\alpha \geqslant 2$ and write $n = 2^{\alpha-2}n_* + s$ and $r = 2^{\alpha-2}r_* + t$ where $0 \leqslant s, t < 2^{\alpha-2}$. Then $s = \{n\}_{2^{\alpha-2}}$ and $t = \{r\}_{2^{\alpha-2}}$. By Theorem 1.7,

$$\begin{aligned}&2^{-\lfloor\frac{n-2^{\alpha-1}}{\varphi(2^\alpha)}\rfloor}\sum_{k\equiv r\,(\mathrm{mod}\ 2^\alpha)}\binom{n}{k}(-1)^k\equiv 1 \pmod 2\\ \iff&\binom{s}{t}\equiv 2^{-\lfloor\frac{n_*-2}{\varphi(4)}\rfloor}\sum_{k\equiv r_*\,(\mathrm{mod}\ 4)}\binom{n_*}{k}(-1)^k\equiv 1 \pmod 2.\end{aligned}$$

In the case $n_* \equiv 1 \pmod 2$, by [S02, (3.3)] we have

$$\begin{aligned}&2\sum_{\substack{0<k<n_*\\ 4\mid k-r_*}}\binom{n_*}{k}-\left(2^{n_*-1}-1\right)\\ =&(-1)^{\frac{r_*(n_*-r_*)}{2}}\left((-1)^{\frac{n_*^2-1}{8}}2^{\frac{n_*-1}{2}}-1\right),\end{aligned}$$

thus

$$\begin{aligned}2\sum_{k\equiv r_*\,(\mathrm{mod}\ 4)}\binom{n_*}{k}=&2([\![4\mid r_*]\!]+[\![4\mid n_*-r_*]\!])+2^{n_*-1}-1\\ &+(-1)^{\frac{r_*(n_*-r_*)}{2}}\left((-1)^{\frac{n_*^2-1}{8}}2^{\frac{n_*-1}{2}}-1\right)\\ =&2^{n_*-1}+(-1)^{\frac{r_*(n_*-r_*)}{2}+\frac{n_*^2-1}{8}}2^{\frac{n_*-1}{2}}\end{aligned}$$

and hence

$$2^{-\lfloor\frac{n_*}{2}\rfloor+1}\sum_{k\equiv r_*\,(\mathrm{mod}\ 4)}\binom{n_*}{k}\equiv 1 \pmod 2 \iff n_*>1.$$

When $n_* \equiv 0 \pmod 2$, if $n_* > 0$ then by the above we have

$$\begin{aligned}
&2\sum_{k\equiv r_* \pmod 4}\binom{n_*}{k}\\
=&2\sum_{k\equiv r_* \pmod 4}\binom{n_*-1}{k}+2\sum_{k\equiv r_*-1 \pmod 4}\binom{n_*-1}{k}\\
=&2^{(n_*-1)-1}+(-1)^{\frac{r_*(n_*-1-r_*)}{2}+\frac{(n_*-1)^2-1}{8}}2^{\frac{(n_*-1)-1}{2}}\\
&+2^{(n_*-1)-1}+(-1)^{\frac{(r_*-1)(n_*-1-(r_*-1))}{2}+\frac{(n_*-1)^2-1}{8}}2^{\frac{(n_*-1)-1}{2}}\\
=&2^{n_*-1}+(-1)^{\binom{n_*/2}{2}}2^{n_*/2-1}\left((-1)^{\frac{r_*(n_*-1-r_*)}{2}}+(-1)^{\frac{(r_*-1)(n_*-r_*)}{2}}\right)\\
=&2^{n_*-1}+(-1)^{\binom{n_*/2}{2}+\lfloor\frac{r_*}{2}\rfloor}\left(1+(-1)^{\frac{n_*}{2}+r_*}\right)2^{n_*/2-1},
\end{aligned}$$

therefore

$$\begin{aligned}
&2^{-\lfloor\frac{n_*}{2}\rfloor+1}\sum_{k\equiv r_* \pmod 4}\binom{n_*}{k}\equiv 1 \pmod 2\\
\iff& n_*>2\ \&\ \frac{n_*}{2}\equiv r_* \pmod 2,\ \text{or } n_*=2\ \&\ 2\mid r_*.
\end{aligned}$$

Combining the above we obtain the desired result. □

4. Proofs of Theorems 1.5 and 1.8

Let us prove Theorem 1.5 first.

Proof of Theorem 1.5. For convenience, we set $T_{l,\alpha}(n,r) := T_{l,\alpha}^{(p)}(n,r)$.

We point out that the case $n = 0$ is easy, because

$$T_{0,\alpha+1}(0,r)=[\![p^{\alpha+1}\mid r]\!]\binom{-r/p^{\alpha+1}}{l}=(-1)^{\{r\}_p}\binom{0}{\{r\}_p}T_{0,\alpha}\left(0,\left\lfloor\frac{r}{p}\right\rfloor\right).$$

Below we use induction on $l+n$ to prove the desired result.

If $l+n=0$, then $n=0$ and hence we are done.

Now let $n>0$, and assume that

$$T_{l_*,\alpha+1}(n_*,r_*)\equiv(-1)^{\{r_*\}_p}\binom{\{n_*\}_p}{\{r_*\}_p}T_{l_*,\alpha}\left(\left\lfloor\frac{n_*}{p}\right\rfloor,\left\lfloor\frac{r_*}{p}\right\rfloor\right)\pmod p$$

whenever $l_*, n_* \in \mathbb{N}$, $l_*+n_* < l+n$ and $r_* \in \mathbb{Z}$. Write $n = pn_0 + s$ and $r = pr_0 + t$, where $n_0, r_0 \in \mathbb{Z}$ and $s, t \in \{0, \dots, p-1\}$.

Case 1. $p^\alpha \nmid n$. By Lemma 2.2 and the induction hypothesis, if $s \neq 0$ then

$$\begin{aligned}T_{l,\alpha+1}(n,r) =&T_{l,\alpha+1}(pn_0+s-1,pr_0+t)\\ &-T_{l,\alpha+1}(pn_0+s-1,pr_0+t-1)\\ \equiv&(-1)^t\binom{s-1}{t}T_{l,\alpha}(n_0,r_0)\\ &-\begin{cases}(-1)^{t-1}\binom{s-1}{t-1}T_{l,\alpha}(n_0,r_0) & \text{if } t>0,\\ (-1)^{p-1}\binom{s-1}{p-1}T_{l,\alpha}(n_0,r_0-1) & \text{if } t=0,\end{cases}\\ \equiv&(-1)^t\binom{s-1}{t}T_{l,\alpha}(n_0,r_0)+(-1)^t\binom{s-1}{t-1}T_{l,\alpha}(n_0,r_0)\\ \equiv&(-1)^t\binom{s}{t}T_{l,\alpha}(n_0,r_0)\pmod p.\end{aligned}$$

Similarly, provided $s=0$ we have

$$\begin{aligned}T_{l,\alpha+1}(n,r) =&T_{l,\alpha+1}(p(n_0-1)+p-1,pr_0+t)\\ &-T_{l,\alpha+1}(p(n_0-1)+p-1,pr_0+t-1)\\ \equiv&(-1)^t\binom{p-1}{t}T_{l,\alpha}(n_0-1,r_0)\\ &-\begin{cases}(-1)^{t-1}\binom{p-1}{t-1}T_{l,\alpha}(n_0-1,r_0)\pmod p & \text{if } t>0,\\ (-1)^{p-1}\binom{p-1}{p-1}T_{l,\alpha}(n_0-1,r_0-1)\pmod p & \text{if } t=0.\end{cases}\end{aligned}$$

Thus, if $0<t<p$ then

$$T_{l,\alpha+1}(n,r)\equiv(-1)^t\binom{p}{t}T_{l,\alpha}(n_0-1,r_0)\equiv 0\pmod p$$

and hence $T_{l,\alpha+1}(n,r)\equiv(-1)^t\binom{0}{t}T_{l,\alpha}(n_0,r_0)\pmod p$; if $t=0$ then

$$T_{l,\alpha+1}(n,r)\equiv T_{l,\alpha}(n_0-1,r_0)-T_{l,\alpha}(n_0-1,r_0-1)\equiv T_{l,\alpha}(n_0,r_0)\pmod p$$

with the help of Lemma 2.2.

Case 2. $p^\alpha \mid n$ and $p^\alpha \nmid r$. In this case,

$$\operatorname{ord}_p(T_{l,\alpha+1}(n,r))\geqslant\tau_p(\{r\}_{p^\alpha},\{n-r\}_{p^\alpha})>0$$

by Theorem 2.1. If $p\nmid r$ (i.e., $t>0$) then $\binom{\{n\}_p}{\{r\}_p}=\binom{0}{t}=0$; if $p\mid r$ then

$$\begin{aligned}\operatorname{ord}_p(T_{l,\alpha}(n_0,r_0))\geqslant&\tau_p(\{r_0\}_{p^{\alpha-1}},\{n_0-r_0\}_{p^{\alpha-1}})\\ =&\tau_p(p\{r_0\}_{p^{\alpha-1}},p\{n_0-r_0\}_{p^{\alpha-1}})=\tau_p(\{r\}_{p^\alpha},\{n-r\}_{p^\alpha}).\end{aligned}$$

So we have

$$T_{l,\alpha+1}(n,r) \equiv 0 \equiv (-1)^{\{r\}_p}\binom{\{n\}_p}{\{r\}_p}T_{l,\alpha}(n_0,r_0) \pmod p.$$

`Case 3`. $n \equiv r \equiv 0 \pmod{p^\alpha}$. When $l = 0$, by Theorem 3.1 we have

$$\begin{aligned}T_{0,\alpha+1}(n,r) =& \frac{p^{\lfloor\frac{n/p^\alpha-1}{p-1}\rfloor}}{(n/p^\alpha)!}S^{(p)}_{\alpha+1}\left(\frac{n}{p^\alpha},r\right)\\ \equiv&\frac{p^{\lfloor\frac{n_0/p^{\alpha-1}-1}{p-1}\rfloor}}{(n_0/p^{\alpha-1})!}S^{(p)}_{\alpha}\left(\frac{n_0}{p^{\alpha-1}},\frac{r}{p}\right) = T_{0,\alpha}(n_0,r_0) \ \left(\bmod\ p^{(2-\delta_{p,2})(\alpha-1)}\right).\end{aligned}$$

In view of Lemma 2.2 and the induction hypothesis, if $l > 0$ then

$$\begin{aligned}T_{l,\alpha+1}(n,r) =& -\frac{r}{p^\alpha}T_{l-1,\alpha+1}(n,r+p^{\alpha+1}) - T_{l-1,\alpha+1}(n-1,r+p^{\alpha+1}-1)\\ =& -\frac{r_0}{p^{\alpha-1}}T_{l-1,\alpha+1}(pn_0,p(r_0+p^\alpha))\\ &- T_{l-1,\alpha+1}(p(n_0-1)+p-1,p(r_0+p^\alpha-1)+p-1)\\ \equiv& -\frac{r_0}{p^{\alpha-1}}T_{l-1,\alpha}(n_0,r_0+p^\alpha)\\ &-(-1)^{p-1}\binom{p-1}{p-1}T_{l-1,\alpha}(n_0-1,r_0+p^\alpha-1)\\ \equiv&T_{l,\alpha}(n_0,r_0) \pmod p.\end{aligned}$$

Combining the above we have completed the induction proof. □

To establish Theorem 1.8 we need some auxiliary results.

Lemma 4.1. *Let p be a prime, and let $n = p^\beta(pq+r)$ with $\beta, q, r \in \mathbb{N}$ and $\{-q\}_{p-1} < r < p$. Then*

$$\mathrm{ord}_p(n!) = \left\lfloor\frac{n-1}{p-1}\right\rfloor \iff q = 0.$$

Proof. For $s = \{-q\}_{p-1}$ we clearly have $pq + s \equiv 0 \pmod{p-1}$. Observe that

$$\begin{aligned}\left\lfloor\frac{n-1}{p-1}\right\rfloor =&\frac{p^\beta-1}{p-1}(pq+r) + \left\lfloor\frac{pq+r-1}{p-1}\right\rfloor\\ =&\frac{p^\beta-1}{p-1}(pq+r) + \frac{pq+s}{p-1}.\end{aligned}$$

Also,

$$\begin{aligned}\operatorname{ord}_p(n!) =& \sum_{0<i\leqslant\beta}\frac{p^\beta(pq+r)}{p^i}+\sum_{i=1}^{\infty}\left\lfloor\frac{p^\beta(pq+r)}{p^{\beta+i}}\right\rfloor\\ =&(pq+r)\sum_{0<i\leqslant\beta}p^{\beta-i}+\operatorname{ord}_p((pq+r)!)\\ =&\frac{p^\beta-1}{p-1}(pq+r)+\operatorname{ord}_p((pq)!).\end{aligned}$$

In the case $q=0$, we have $s=0$ and hence

$$\left\lfloor\frac{n-1}{p-1}\right\rfloor=\frac{p^\beta-1}{p-1}r=\operatorname{ord}_p(n!)$$

by the above.

Now let $q>0$. Then

$$\operatorname{ord}_p((pq)!)=\sum_{i=1}^{\infty}\left\lfloor\frac{pq}{p^i}\right\rfloor<\sum_{i=1}^{\infty}\frac{pq}{p^i}=\frac{q}{1-p^{-1}}=\frac{pq}{p-1}\leqslant\frac{pq+s}{p-1}$$

and therefore $\operatorname{ord}_p(n!)<\lfloor(n-1)/(p-1)\rfloor$. This ends the proof. □

Remark 4.1. By Lemma 4.1, if p is a prime and n is a positive integer with $\operatorname{ord}_p(n)=\lfloor\log_p n\rfloor$, then $\operatorname{ord}_p(n!)=\lfloor(n-1)/(p-1)\rfloor$.

Using Lemma 4.1 and Corollary 1.2, we can deduce the following lemma.

Lemma 4.2. *Let $\alpha\in\mathbb{N}$, $n\in\mathbb{Z}^+$, $r\in\mathbb{Z}$ and $n\equiv r\equiv 0 \pmod{2^\alpha}$. Then*

$$T_{0,\alpha+1}^{(2)}(n,r)\equiv 1 \pmod 2 \iff n \textit{ is a power of } 2.$$

Proof. Clearly

$$T_{0,\alpha+1}^{(2)}(n,r)=\frac{(-1)^r2^{n/2^\alpha-1}}{(n/2^\alpha)!}2^{-\left\lfloor\frac{n-2^\alpha}{\varphi(2^{\alpha+1})}\right\rfloor}\sum_{k\equiv r\ (\mathrm{mod}\ 2^{\alpha+1})}\binom{n}{k}.$$

By Lemma 4.1 in the case $p=2$,

$$\operatorname{ord}_2\left(\frac{n}{2^\alpha}!\right)=2^{n/2^\alpha-1}\iff\frac{n}{2^\alpha}\text{ is a power of 2.}$$

If $\alpha=0$, then

$$2^{-\left\lfloor\frac{n-2^\alpha}{\varphi(2^{\alpha+1})}\right\rfloor}\sum_{k\equiv r\ (\mathrm{mod}\ 2^{\alpha+1})}\binom{n}{k}=2^{-(n-1)}\sum_{k\equiv r\ (\mathrm{mod}\ 2)}\binom{n}{k}=1.$$

Now we let $\alpha > 0$. Note that both $n_* = n/2^{\alpha-1}$ and $r_* = r/2^{\alpha-1}$ are even. Also, $\{n\}_{2^{\alpha-1}} = \{r\}_{2^{\alpha-1}} = 0$. Thus, Corollary 1.2 implies that

$$2^{-\left\lfloor \frac{n-2^{\alpha}}{\varphi(2^{\alpha+1})} \right\rfloor} \sum_{k\equiv r \pmod{2^{\alpha+1}}} \binom{n}{k} \equiv 1 \pmod 2$$
$$\iff n_* = 2 \quad \text{or} \quad n_* \equiv 2r_* \equiv 0 \pmod 4.$$

Combining the above we find that $T^{(2)}_{0,\alpha+1}(n,r) \equiv 1 \pmod 2$ if and only if n is a power of 2. This concludes the proof. □

The following result plays a major role in our proof of Theorem 1.8.

Theorem 4.1. *Let $\alpha, c, d, e \in \mathbb{N}$ and $0 \leqslant d < 2^e$. Then*

$$T^{(2)}_{l,\alpha+1}(2^{\alpha}(2^e + d), 2^{\alpha}c) \equiv \delta_{l,d} \pmod 2 \quad \text{for all } l = 0, \ldots, d. \tag{4.1}$$

Proof. By Lemma 4.2, if $n \in \mathbb{Z}^+$, $r \in \mathbb{Z}$ and $n \equiv r \equiv 0 \pmod{2^{\beta}}$ with $\beta = 1$, then $T^{(2)}_{0,\beta+1}(n,r) \equiv T^{(2)}_{0,\beta}(n/2, r/2) \pmod 2$. Thus, by modifying the proof of Theorem 1.5 (just the third case) slightly, we get a modified version of (1.7) with $p = 2$ and α replaced by $\beta = 1$. This, together with Theorem 1.5, shows that if $l \in \mathbb{N}$ and $\alpha > 0$ then

$$\begin{aligned} T^{(2)}_{l,\alpha+1}(2^{\alpha}(2^e + d), 2^{\alpha}c) \equiv& T^{(2)}_{l,\alpha}(2^{\alpha-1}(2^e + d), 2^{\alpha-1}c) \\ &\equiv \cdots \equiv T^{(2)}_{l,1}(2^e + d, c) \pmod 2. \end{aligned}$$

So, it suffices to show the following claim:

`Claim`. *If $l \in \mathbb{N}$, $n \in \mathbb{Z}^+$ and $d_n := n - 2^{\lfloor \log_2 n \rfloor} \geqslant l$, then*

$$T_l(n,r) := T^{(2)}_{l,1}(n,r) \equiv \delta_{l,d_n} \pmod 2 \quad \text{for all } r \in \mathbb{Z}.$$

We use induction on l to show the claim.

As $n \in \mathbb{Z}^+$ is a power of two if and only if $d_n = 0$, in the case $l = 0$ the claim follows from Lemma 4.2.

Now let $l \in \mathbb{Z}^+$ and assume the claim for $l-1$. Let $n \in \mathbb{Z}^+$ with $d_n \geqslant l$. Clearly $d_1 = 0 < l$ and hence $n > 1$. By Lemma 2.2,

$$T_l(n,r) = -rT_{l-1}(n, r+2) - T_{l-1}(n-1, r+1).$$

Since $d_{n-1} = d_n - 1 \geqslant l - 1$, by the induction hypothesis we have

$$T_{l-1}(n, r+2) \equiv \delta_{l-1,d_n} \pmod 2 \quad \text{and} \quad T_{l-1}(n-1, r+1) \equiv \delta_{l-1,d_n-1} \pmod 2.$$

Therefore

$$T_l(n,r) \equiv -r\delta_{l-1,d_n} - \delta_{l-1,d_n-1} \equiv \delta_{l,d_n} \pmod 2.$$

This concludes the induction step, and we are done. □

Proof of Theorem 1.8. Write $n = 2^\alpha(2^e+d)+c$ with $c,d,e \in \mathbb{N}$, $c < 2^\alpha$ and $d < 2^e$. Clearly $n_0 := 2^e + d = \lfloor n/2^\alpha \rfloor$. Since $2^e \leqslant n/2^\alpha < n_0 + 1 \leqslant 2^{e+1}$, we also have $e = \lfloor \log_2(n/2^\alpha) \rfloor$. By Vandermonde's identity,

$$\begin{aligned}&\sum_{k\equiv 0 \pmod{2^\alpha}} \binom{n}{k}(-1)^k\left(\frac{k}{2^\alpha}\right)^l \\ =&\sum_{k\equiv 0 \pmod{2^\alpha}}\sum_{j=0}^{c}\binom{c}{j}\binom{2^\alpha n_0}{k-j}(-1)^k\left(\frac{k}{2^\alpha}\right)^l \\ =&\sum_{j=0}^{c}\binom{c}{j}(-1)^j\sum_{k\equiv -j \pmod{2^\alpha}}\binom{2^\alpha n_0}{k}(-1)^k\left(\frac{k+j}{2^\alpha}\right)^l.\end{aligned}$$

(Note that signs are not omitted because α might be zero.) If $0 < j \leqslant c < 2^\alpha$, then

$$\begin{aligned}&\operatorname{ord}_2\bigg(\sum_{k\equiv -j \pmod{2^\alpha}}\binom{2^\alpha n_0}{k}(-1)^k\left(\frac{k+j}{2^\alpha}\right)^l\bigg) \\ &\geqslant \operatorname{ord}_2(n_0!) + \tau_2(2^\alpha - j, j) > \operatorname{ord}_2(n_0!)\end{aligned}$$

by the inequality (1.2). So, we need to show that

$$\sum_{k\equiv 0 \pmod{2^\alpha}}\binom{2^\alpha n_0}{k}(-1)^k\left(\frac{k}{2^\alpha}\right)^l = \sum_{k\in\mathbb{N}}\binom{2^\alpha n_0}{2^\alpha k}(-1)^{2^\alpha k}k^l$$

has the same 2-adic order as $n_0!$. If k is even, then $\operatorname{ord}_2(k^l) \geqslant l \geqslant n_0 > \operatorname{ord}_2(n_0!)$. Thus, it remains to prove that $\operatorname{ord}_2(\Sigma) = \operatorname{ord}_2(n_0!)$, where

$$\Sigma = \sum_{2\nmid k}\binom{2^\alpha n_0}{2^\alpha k}k^l = \sum_{j\in\mathbb{N}}\binom{2^\alpha n_0}{2^\alpha(2j+1)}(2j+1)^l.$$

Observe that

$$(2j+1)^l = \sum_{s=0}^{l}\binom{l}{s}2^s j^s = \sum_{s=0}^{l}\binom{l}{s}2^s\sum_{t=0}^{s}S(s,t)\ t!\binom{j}{t}$$

and hence

$$\begin{aligned}\frac{\Sigma}{n_0!} &= \sum_{0\leqslant t\leqslant s\leqslant l}\binom{l}{s}2^s S(s,t)\frac{t!}{n_0!}\sum_{j\in\mathbb{N}}\binom{2^\alpha n_0}{2^{\alpha+1}j+2^\alpha}\binom{j}{t}\\ &= \sum_{0\leqslant t\leqslant s\leqslant l}\binom{l}{s}2^{s-t}S(s,t)(-1)^{2^\alpha}T^{(2)}_{t,\alpha+1}(2^\alpha n_0,2^\alpha)\\ &\equiv\sum_{t=0}^{l}\binom{l}{t}T^{(2)}_{t,\alpha+1}(2^\alpha n_0,2^\alpha)\ (\mathrm{mod}\ 2).\end{aligned}$$

Now we analyze the parity of $\binom{l}{t}T^{(2)}_{t,\alpha+1}(2^\alpha n_0,2^\alpha)$ for each $0\leqslant t\leqslant l$. As $l\geqslant n_0$ and $l\equiv n_0\ (\mathrm{mod}\ 2^e)$, we can write $l=n_0+2^e q=2^e(q+1)+d$ with $q\in\mathbb{N}$. Note that

$$\binom{l}{d}=\prod_{0<r<d}\left(1+\frac{2^e}{r}(q+1)\right)\equiv 1\ (\mathrm{mod}\ 2).$$

Also, if $0\leqslant t\leqslant d$ then $T^{(2)}_{t,\alpha+1}(2^\alpha n_0,2^\alpha)\equiv\delta_{t,d}\ (\mathrm{mod}\ 2)$ by Theorem 4.1. When $d<t\leqslant l$ and $T^{(2)}_{t,\alpha+1}(2^\alpha n_0,2^\alpha)\neq 0$, we have $2^\alpha n_0\geqslant 2^{\alpha+1}t+2^\alpha$, hence $d<t<n_0/2<2^e$ and thus

$$\begin{aligned}\mathrm{ord}_2\binom{l}{t} &= \sum_{i=1}^{\infty}\left(\left\lfloor\frac{l}{2^i}\right\rfloor-\left\lfloor\frac{t}{2^i}\right\rfloor-\left\lfloor\frac{l-t}{2^i}\right\rfloor\right)\\ &\geqslant\left\lfloor\frac{l}{2^e}\right\rfloor-\left\lfloor\frac{t}{2^e}\right\rfloor-\left\lfloor\frac{l-t}{2^e}\right\rfloor=(q+1)-0-q>0.\end{aligned}$$

Combining the above we find that

$$\frac{\Sigma}{n_0!}\equiv\sum_{t=0}^{l}\binom{l}{t}T^{(2)}_{t,\alpha+1}(2^\alpha n_0,2^\alpha)\equiv 1\ (\mathrm{mod}\ 2).$$

So $\mathrm{ord}_2(\Sigma)=\mathrm{ord}_2(n_0!)$ as required. □

Acknowledgment. The joint paper was written during the first author's visit to the University of California at Irvine. He would like to thank Prof. D. Wan for the invitation.

References

[DS] D. M. Davis and Z. W. Sun, *A number-theoretic approach to homotopy exponents of* SU(n), 2005, submitted, `http://arxiv.org/abs/math.AT/0508083`.

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

[GKP] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, New York, 1989.

[G] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers,* in: Organic mathematics (Burnaby, BC, 1995), 253–276, CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Graduate texts in math.; 84), 2nd ed., Springer, New York, 1990.

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

[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] Z. W. Sun, *General congruences for Bernoulli polynomials*, Discrete Math. **262** (2003), 253–276.

[S05] Z. W. Sun, *Polynomial extension of Fleck's congruence*, preprint, 2005, on-line version: `http://arxiv.org/abs/math.NT/0507008`.

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