Acta Arith. 126(2007), no. 4, 387–398.

COMBINATORIAL CONGRUENCES AND STIRLING NUMBERS

Zhi-Wei Sun (Nanjing)

Abstract. In this paper we obtain some sophisticated combinatorial congruences involving binomial coefficients and confirm two conjectures of the author and Davis. They are closely related to our investigation of the periodicity of the sequence $\sum_{j=0}^{l}\binom{l}{j}S(j,m)a^{l-j}$ $(l=m,m+1,\ldots)$ modulo a prime p, where a and $m>0$ are integers, and those $S(j,m)$ are Stirling numbers of the second kind. We also give a new extension of Glaisher's congruence by showing that $(p-1)p^{\lfloor \log_p m\rfloor}$ is a period of the sequence $\sum_{j\equiv r\,(\mathrm{mod}\ p-1)}\binom{l}{j}S(j,m)$ $(l=m,m+1,\ldots)$ modulo p.

1. Introduction

In a recent paper of the author and D. M. Davis [SD] originally motivated by the study of homotopy exponents of the special unitary group $\mathrm{SU}(n)$, the following sophisticated theorem was established.

Theorem 1.0 (Sun and Davis). *Let p be a prime, and let $\alpha,n\in\mathbb{N}=\{0,1,\ldots\}$ and $r\in\mathbb{Z}$. Then, for any $f(x)\in\mathbb{Z}[x]$, we have*

$$\begin{aligned}&\mathrm{ord}_p\bigg(\sum_{k\equiv r\,(\mathrm{mod}\ p^{\alpha})}(-1)^k\binom{n}{k}f\left(\frac{k-r}{p^{\alpha}}\right)\bigg)\\ \geqslant&\,\mathrm{ord}_p\left(\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\right)-\deg f+\tau_p(\{r\}_{p^{\alpha-1}},\{n-r\}_{p^{\alpha-1}}),\end{aligned}\tag{1.0}$$

where $\mathrm{ord}_p(a)=\sup\{m\in\mathbb{N}:p^m\mid a\}$ is the p-adic order of $a\in\mathbb{Z}$, $\{a\}_{p^{\alpha-1}}$ stands for the least nonnegative residue of a modulo $p^{\alpha-1}$ (and this is regarded as 0 if $\alpha=0$), and for $a,b\in\mathbb{N}$ we use $\tau_p(a,b)$ to denote the number of carries occurring in the addition of a and b in base p.

Let p be a prime. By a well-known fact in number theory (cf. [IR, p. 26]),

$$\mathrm{ord}_p(n!)=\sum_{i=1}^{\infty}\left\lfloor\frac{n}{p^i}\right\rfloor\qquad\text{for every } n=0,1,2,\ldots.$$

2000 *Mathematics Subject Classification.* Primary 11B65; Secondary 05A10, 11A07, 11B73.

Supported by the National Science Fund for Distinguished Young Scholars (Grant No. 10425103) and a Key Program of NSF (Grant No. 10331020) in China.

A useful theorem of E. Kummer asserts that if $a, b \in \mathbb{N}$ then

$$\mathrm{ord}_p\binom{a+b}{a} = \sum_{i=1}^{\infty}\left(\left\lfloor\frac{a+b}{p^i}\right\rfloor - \left\lfloor\frac{a}{p^i}\right\rfloor - \left\lfloor\frac{b}{p^i}\right\rfloor\right) = \tau_p(a,b).$$

In this paper we will apply Theorem 1.0 to deduce three theorems on combinatorial congruences or Stirling numbers of the second kind.

For $l, m \in \mathbb{N}$ with $l + m > 0$, the Stirling number $S(l,m)$ of the second kind denotes the number of ways to partition a set of cardinality l into m nonempty subsets; in addition, we define $S(0,0)$ to be 1. It is well known that

$$x^l = \sum_{j=0}^{l} S(l,j)(x)_j \quad \text{for } l = 0, 1, 2, \dots ,$$

where $(x)_j = \prod_{0\leqslant i<j}(x-i)$ and an empty product has the value 1 (thus $(x)_0 = 1$).

Here is our first theorem.

Theorem 1.1. *Let p be any prime. Let $a \in \mathbb{Z}$, $l, l', m \in \mathbb{Z}^+ = \{1, 2, \dots\}$, $l' \geqslant l > m/p$ and*

$$l' \equiv l \ \left(\mathrm{mod}\ (p-1)p^{\lfloor \log_p m\rfloor - \delta_p(a,m)}\right), \tag{1.1}$$

where

$$\delta_p(a,m) = \begin{cases} 1 & \text{if } a \in p\mathbb{Z} \text{ and } \log_p m \in \mathbb{Z}^+, \\ 0 & \text{otherwise.} \end{cases} \tag{1.2}$$

Then we have

$$\sum_{j=0}^{l'}\binom{l'}{j}S(j,m)a^{l'-j} \equiv \sum_{j=0}^{l}\binom{l}{j}S(j,m)a^{l-j} \ (\mathrm{mod}\ p). \tag{1.3}$$

Corollary 1.1. *Let p be a prime, and let $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then, for $k = m + (p-1)p^{\lfloor \log_p m\rfloor - \delta_p(a,m)}q$ with $q \in \mathbb{N}$, we have*

$$\sum_{j=0}^{k}\binom{k}{j}S(j,m)a^{k-j} \equiv 1 \ (\mathrm{mod}\ p).$$

Proof. Just apply Theorem 1.1 with $l = m$ and $l' = k$. □

Remark 1.1. Note that if p is a prime and m is a positive integer then $m - (p-1)p^{\lfloor \log_p m\rfloor} < m/p$.

The following result was first obtained by L. Carlitz [C] in 1955. (See also A. Nijenhuis and H. S. Wilf [NW], and Y. H. H. Kwong [K].)

Corollary 1.2. *Let p be any prime. Suppose that $\alpha, m \in \mathbb{N}$, $m \geqslant p$ and $p^\alpha < m \leqslant p^{\alpha+1}$. Then $p^\alpha(p-1)$ is a period of the sequence $\{S(l,m)\}_{l\geqslant m}$ modulo p.*

Proof. It suffices to apply Theorem 1.1 with $a = 0$. □

The sum $\sum_{k\equiv r\,(\mathrm{mod}\ m)}\binom{n}{k}$ with $m \in \mathbb{Z}^+$, $n \in \mathbb{N}$ and $r \in \mathbb{Z}$ has been investigated intensively, see [S] for some historical background and related congruences. In 1899 J.W.L. Glaisher (cf. [D, p. 271] and [ST]) proved that

$$\sum_{j\equiv r\,(\mathrm{mod}\ p-1)}\binom{l'}{j} \equiv \sum_{j\equiv r\,(\mathrm{mod}\ p-1)}\binom{l}{j} \pmod p$$

whenever p is a prime, $r \in \mathbb{Z}$, $l', l \in \mathbb{Z}^+$ and $l' \equiv l \pmod{p-1}$. Clearly Glaisher's congruence is our following result in the case $m = 1$.

Corollary 1.3. *Let p be a prime, $m \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$. For any $l', l \in \mathbb{Z}^+$ with $l' \geqslant l > m/p$ and*

$$l' \equiv l \ \left(\mathrm{mod}\ (p-1)p^{\lfloor \log_p m\rfloor}\right),$$

we have

$$\sum_{j\equiv r\,(\mathrm{mod}\ p-1)}\binom{l'}{j}S(j,m) \equiv \sum_{j\equiv r\,(\mathrm{mod}\ p-1)}\binom{l}{j}S(j,m) \pmod p. \tag{1.4}$$

Our second theorem is slightly stronger than Conjecture 1.3 of the author and Davis [SD] which was proved in [SD] when $p = 2$ and $r = 0$.

Theorem 1.2. *Let p be a prime, and let $\alpha, l, n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Set $r_* = \{r\}_{p^\alpha}$, $n_* = r_* + \{n-r\}_{p^\alpha}$ and*

$$m = \frac{n-n_*}{p^\alpha} = \left\lfloor \frac{r}{p^\alpha}\right\rfloor + \left\lfloor\frac{n-r}{p^\alpha}\right\rfloor. \tag{1.5}$$

Suppose that $l \geqslant m > 0$ and

$$l \equiv m \ \left(\mathrm{mod}\ (p-1)p^{\lfloor \log_p m\rfloor - \delta_p(\lfloor r/p^\alpha\rfloor, m)}\right), \tag{1.6}$$

where the notation $\delta_p(a,m)$ is given by (1.2). Then we have

$$\frac{1}{\lfloor n/p^\alpha\rfloor!\binom{n_*}{r_*}}\sum_{k\equiv r\,(\mathrm{mod}\ p^\alpha)}(-1)^k\binom{n}{k}\left(\frac{k-r}{p^\alpha}\right)^l \equiv (-1)^{l+r_*} \pmod p. \tag{1.7}$$

Remark 1.2. Theorem 1.2 implies that the inequality in Theorem 5.1 of [DS] is sharp for infinitely many values of l provided that $n \geqslant 2p^\alpha - 1$.

Our third theorem confirms Conjecture 1.1 of [SD].

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

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

where

$$a_p = \begin{cases} 1 & \text{if } p = 2,\\ 2 & \text{if } p = 3,\\ 3 & \text{if } p > 3.\end{cases} \tag{1.9}$$

Remark 1.3. Let p be a prime, $\alpha, n \in \mathbb{N}$ and $r \in \mathbb{Z}$. When $p^\alpha > n$ and $l = 0 \leqslant r \leqslant n$, (1.8) reduces to Ljunggren's congruence $\binom{pn}{pr} \equiv \binom{n}{r} \pmod{p^{a_p}}$ (cf. [G]) which is an extension of the Wolstenholme congruence $\binom{2p}{p} \equiv 2 \pmod{p^{a_p}}$ (i.e., $\binom{2p-1}{p-1} \equiv 1 \pmod{p^{a_p}}$). Note also that (1.8) holds for every $l \in \mathbb{N}$ if and only if we have

$$\binom{pn}{pr}_{f,\,p^{\alpha+1}} \equiv \binom{n}{r}_{f,\,p^\alpha} \pmod{p^{a_p}} \tag{1.10}$$

for all $f(x) \in \mathbb{Z}[x]$, where

$$\binom{n}{r}_{f,\,p^\alpha} = \frac{p^{\deg f}}{\lfloor n/p^{\alpha-1}\rfloor!}\sum_{k\equiv r \,(\mathrm{mod}\ p^\alpha)}(-1)^k\binom{n}{k} f\left(\frac{k-r}{p^\alpha}\right) \in \mathbb{Z}_p. \tag{1.11}$$

(As usual, $\mathbb{Z}_p$ denotes the ring of p-adic integers.)

Concerning the right-hand side of the congruence (1.8), a Lucas-type congruence modulo p was established in [SD] for $\alpha > 1$ (and in [SW] for $\alpha = 1$). See also [SW] for some other congruences of Lucas' type related to combinatorial sums involving binomial coefficients.

In the next section we are going to prove Theorem 1.1 and Corollary 1.3. On the basis of Theorem 1.1 we will deduce Theorem 1.2 in Section 3. Section 4 is devoted to our proof of Theorem 1.3.

2. Proofs of Theorem 1.1 and Corollary 1.3

Proof of Theorem 1.1. By a well-known property of Stirling numbers of the second kind (cf. [LW, pp. 125–126]),

$$\begin{aligned}\sum_{j=0}^{l}\binom{l}{j}a^{l-j}S(j,m) =&\sum_{j=0}^{l}\binom{l}{j}a^{l-j}\frac{1}{m!}\sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k}k^j\\ =&\frac{1}{m!}\sum_{k=0}^{m}(-1)^{m-k}\binom{m}{k}(a+k)^l = (-1)^m\sum_{r=0}^{p-1}S_r(l),\end{aligned}$$

where

$$S_r(l) = \frac{1}{m!} \sum_{k\equiv r \,(\mathrm{mod}\ p)} (-1)^k \binom{m}{k} (a+k)^l. \tag{2.1}$$

Let $r \in \{0, \dots, p-1\}$. Observe that

$$\begin{aligned} S_r(l) =& \frac{1}{m!} \sum_{k\equiv r \,(\mathrm{mod}\ p)} (-1)^k \binom{m}{k} \sum_{j=0}^{l} \binom{l}{j} p^j \left(\frac{k-r}{p}\right)^j (a+r)^{l-j} \\ =& \sum_{j=0}^{l} \binom{l}{j} (a+r)^{l-j} \frac{p^j}{m!} \sum_{k\equiv r \,(\mathrm{mod}\ p)} (-1)^k \binom{m}{k} \left(\frac{k-r}{p}\right)^j . \end{aligned}$$

By Theorem 1.0, for any $j \in \mathbb{N}$ we have

$$\sigma_r(j) := \frac{p^j}{m!} \sum_{k\equiv r \,(\mathrm{mod}\ p)} (-1)^k \binom{m}{k} \left(\frac{k-r}{p}\right)_j \in \mathbb{Z}_p \tag{2.2}$$

and

$$\frac{p^j}{m!} \sum_{k\equiv r \,(\mathrm{mod}\ p)} (-1)^k \binom{m}{k} \left(\left(\frac{k-r}{p}\right)^j - \left(\frac{k-r}{p}\right)_j \right) \equiv 0 \pmod{p}$$

since the degree of $f_j(x) = x^j - (x)_j \in \mathbb{Z}[x]$ is smaller than j. Therefore,

$$S_r(l) \equiv \sum_{j=0}^{l} \binom{l}{j} (a+r)^{l-j} \sigma_r(j) \pmod{p}. \tag{2.3}$$

In view of the above, it suffices to show that

$$\binom{l'}{j} (a+r)^{l'-j} \sigma_r(j) \equiv \binom{l}{j} (a+r)^{l-j} \sigma_r(j) \pmod{p} \tag{2.4}$$

for every $j = 0, 1, \dots$.

Below we assume $j \in \mathbb{N}$ and $\sigma_r(j) \neq 0$. Then $((k-r)/p)_j \neq 0$ for some $0 \leqslant k \leqslant m$ with $k \equiv r \,(\mathrm{mod}\ p)$, hence $m - r \geqslant k - r \geqslant pj$ and $j \leqslant m/p < l \leqslant l'$. If $p \mid a + r$, then

$$(a+r)^{l'-j} \equiv 0 \equiv (a+r)^{l-j} \pmod{p}.$$

When $p \nmid a + r$, as $l' \equiv l \pmod{p-1}$ we have

$$(a+r)^{l'-j} \equiv (a+r)^{l-j} \pmod{p}$$

by Fermat's little theorem. So it remains to show $\binom{l'}{j} \equiv \binom{l}{j} \pmod p$ in the case $p \nmid a+r$.

Let $\alpha = \lfloor \log_p m \rfloor$. Then $p^\alpha \leqslant m < p^{\alpha+1}$ and $\delta = \delta_p(a,m) \leqslant \alpha$. Write $l = p^{\alpha-\delta}q_0 + l_0$ with $q_0 \in \mathbb{N}$ and $0 \leqslant l_0 < p^{\alpha-\delta}$. For some $q \in \mathbb{N}$ we have $l' = l + (p-1)p^{\alpha-\delta}q = p^{\alpha-\delta}((p-1)q + q_0) + l_0$. Recall that $j \leqslant (m-r)/p < p^\alpha$. Suppose $a+r \not\equiv 0 \pmod p$. If $\delta = 1$, then $j < m/p = p^{\alpha-1}$ because $m = p^\alpha$ and $r \neq \{-a\}_p = 0$. Thus $j < p^{\alpha-\delta}$. With help of the Chu-Vandermonde convolution identity (cf. [GKP, (5.27)]),

$$\begin{aligned}\binom{l}{j} - \binom{l_0}{j} &= \sum_{0<i\leqslant j} \binom{p^{\alpha-\delta}q_0}{i}\binom{l_0}{j-i} \\ &= \sum_{0<i\leqslant j} \frac{p^{\alpha-\delta}}{i} q_0 \binom{p^{\alpha-\delta}q_0 - 1}{i-1}\binom{l_0}{j-i} \equiv 0 \pmod p.\end{aligned}$$

Similarly, $\binom{l'}{j} \equiv \binom{l_0}{j} \pmod p$ as desired. We are done. □

Proof of Corollary 1.3. Let g be a primitive root modulo p. For any integer h, if $p-1 \mid h$ then $\sum_{a=1}^{p-1} a^h \equiv p-1 \equiv -1 \pmod p$ by Fermat's little theorem; if $p-1 \nmid h$ then $g^h \not\equiv 1 \pmod p$ and hence $\sum_{a=1}^{p-1} a^h \equiv 0 \pmod p$ since

$$(g^h - 1)\sum_{a=1}^{p-1} a^h = \sum_{a=1}^{p-1}(ag)^h - \sum_{a=1}^{p-1} a^h \equiv 0 \pmod p.$$

In view of the above,

$$\begin{aligned}&\sum_{a=1}^{p-1} a^{r-l} \sum_{j=0}^{l} \binom{l}{j} S(j,m) a^{l-j} \\ =& \sum_{j=0}^{l} \binom{l}{j} S(j,m) \sum_{a=1}^{p-1} a^{r-j} \\ \equiv& -\sum_{j\equiv r \pmod{p-1}} \binom{l}{j} S(j,m) \pmod p.\end{aligned}$$

Similarly,

$$\sum_{a=1}^{p-1} a^{r-l'} \sum_{j=0}^{l'} \binom{l'}{j} S(j,m) a^{l'-j} \equiv -\sum_{j\equiv r \pmod{p-1}} \binom{l'}{j} S(j,m) \pmod p.$$

Since $l' \equiv l \pmod{p-1}$, $a^{r-l'} \equiv a^{r-l} \pmod p$ for all $a = 1, \ldots, p-1$. Thus, applying Theorem 1.1 we immediately obtain (1.4) from the above. □

3. Proof of Theorem 1.2

At first we make some useful observations. Clearly

$$m \leqslant \frac{n-r_*}{p^\alpha} = \frac{n-r}{p^\alpha} + \left\lfloor \frac{r}{p^\alpha} \right\rfloor < 1 + \left\lfloor \frac{n-r}{p^\alpha} \right\rfloor + \left\lfloor \frac{r}{p^\alpha} \right\rfloor = m+1.$$

Since

$$\tau_p(\{r\}_{p^\alpha}, \{n-r\}_{p^\alpha}) - \tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}) = \begin{cases} 1 & \text{if } n_* \geqslant p^\alpha, \\ 0 & \text{otherwise,} \end{cases}$$

we also have

$$\mathrm{ord}_p \binom{n_*}{r_*} - \tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}) = \left\lfloor \frac{n_*}{p^\alpha} \right\rfloor = \left\lfloor \frac{n}{p^\alpha} \right\rfloor - m. \tag{3.1}$$

Let $a = -\lfloor r/p^\alpha \rfloor$, $k \in \{0, \ldots, n\}$ and $k \equiv r \pmod{p^\alpha}$. Then

$$\begin{aligned} \left(\frac{k-r}{p^\alpha}\right)^l &= \left(\frac{k-r_*}{p^\alpha} + a\right)^l = \sum_{j=0}^{l} \binom{l}{j} a^{l-j} \left(\frac{k-r_*}{p^\alpha}\right)^j \\ &= \sum_{j=0}^{l} \binom{l}{j} a^{l-j} \sum_{i=0}^{j} S(j,i) \left(\frac{k-r_*}{p^\alpha}\right)_i \\ &= \sum_{j=0}^{l} \binom{l}{j} a^{l-j} \sum_{i=0}^{m} S(j,i) \left(\frac{k-r_*}{p^\alpha}\right)_i, \end{aligned}$$

because for $i \geqslant m+1$ we have $i > (n-r_*)/p^\alpha \geqslant (k-r_*)/p^\alpha$ and hence $((k-r_*)/p^\alpha)_i = 0$.

Observe that

$$\mathrm{ord}_p\left(\left\lfloor \frac{n}{p^{\alpha-1}} \right\rfloor ! \right) = \left\lfloor \frac{n}{p^\alpha} \right\rfloor + \sum_{s>\alpha} \left\lfloor \frac{n}{p^s} \right\rfloor = \left\lfloor \frac{n}{p^\alpha} \right\rfloor + \mathrm{ord}_p\left(\left\lfloor \frac{n}{p^\alpha} \right\rfloor ! \right).$$

If $i \in \{0, \ldots, m-1\}$, then by Theorem 1.0 and (3.1) we have

$$\begin{aligned} &\mathrm{ord}_p\Bigg(\sum_{k \equiv r_* \pmod{p^\alpha}} (-1)^k \binom{n}{k} \left(\frac{k-r_*}{p^\alpha}\right)_i \Bigg) \\ \geqslant &\mathrm{ord}_p\left(\left\lfloor \frac{n}{p^{\alpha-1}} \right\rfloor ! \right) - i + \tau_p(\{r_*\}_{p^{\alpha-1}}, \{n-r_*\}_{p^{\alpha-1}}) \\ > &\mathrm{ord}_p\left(\left\lfloor \frac{n}{p^\alpha} \right\rfloor ! \right) + \left\lfloor \frac{n}{p^\alpha} \right\rfloor - m + \tau_p(\{r\}_{p^{\alpha-1}}, \{n-r\}_{p^{\alpha-1}}) \\ = &\mathrm{ord}_p\left(\left\lfloor \frac{n}{p^\alpha} \right\rfloor ! \binom{n_*}{r_*} \right). \end{aligned}$$

Therefore,

$$\begin{aligned}&\frac{1}{\lfloor n/p^\alpha\rfloor!\binom{n_*}{r_*}}\sum_{k\equiv r\ (\mathrm{mod}\ p^\alpha)}(-1)^k\binom{n}{k}\left(\frac{k-r}{p^\alpha}\right)^l\\ \equiv&\sum_{j=0}^l\binom{l}{j}\frac{S(j,m)a^{l-j}}{\lfloor n/p^\alpha\rfloor!\binom{n_*}{r_*}}\sum_{k\equiv r\ (\mathrm{mod}\ p^\alpha)}(-1)^k\binom{n}{k}\left(\frac{k-r_*}{p^\alpha}\right)_m\ (\mathrm{mod}\ p).\end{aligned}$$

In light of Corollary 1.1, it remains to show that $S\equiv(-1)^{l+r_*}\ (\mathrm{mod}\ p)$, where

$$S=\frac{1}{\lfloor n/p^\alpha\rfloor!\binom{n_*}{r_*}}\sum_{k\equiv r_*\ (\mathrm{mod}\ p^\alpha)}(-1)^k\binom{n}{k}\left(\frac{k-r_*}{p^\alpha}\right)_m. \tag{3.2}$$

If $k\in\{0,\ldots,n\}$, $k\equiv r_*\ (\mathrm{mod}\ p^\alpha)$ and $((k-r_*)/p^\alpha)_m\neq0$, then

$$m\leqslant\frac{k-r_*}{p^\alpha}\leqslant\frac{n-r_*}{p^\alpha}<m+1$$

and hence $k=mp^\alpha+r_*$. So

$$S=\frac{(-1)^{mp^\alpha+r_*}}{\lfloor n/p^\alpha\rfloor!\binom{n_*}{r_*}}\binom{n}{mp^\alpha+r_*}(m)_m=\frac{(-1)^{mp^\alpha+r_*}m!}{(m+\lfloor n_*/p^\alpha\rfloor)!}\times\frac{\binom{mp^\alpha+n_*}{mp^\alpha+r_*}}{\binom{n_*}{r_*}}.$$

Clearly

$$\begin{aligned}\frac{\binom{mp^\alpha+n_*}{mp^\alpha+r_*}}{\binom{n_*}{r_*}}&=\frac{(mp^\alpha+n_*)!/(mp^\alpha+r_*)!}{n_*!/r_*!}\\&=\prod_{0<i\leqslant n_*}\left(1+m\frac{p^\alpha}{i}\right)\Big/\prod_{0<j\leqslant r_*}\left(1+m\frac{p^\alpha}{j}\right).\end{aligned}$$

Thus, if $n_*<p^\alpha$ then

$$\frac{\binom{mp^\alpha+n_*}{mp^\alpha+r_*}}{\binom{n_*}{r_*}}\equiv1\ (\mathrm{mod}\ p);$$

if $n_*\geqslant p^\alpha$ then $\lfloor n_*/p^\alpha\rfloor=1$ and

$$\frac{\binom{mp^\alpha+n_*}{mp^\alpha+r_*}}{(m+1)\binom{n_*}{r_*}}=\prod_{\substack{0<i\leqslant n_*\\ i\neq p^\alpha}}\left(1+m\frac{p^\alpha}{i}\right)\Big/\prod_{0<j\leqslant r_*}\left(1+m\frac{p^\alpha}{j}\right)\equiv1\ (\mathrm{mod}\ p).$$

Therefore,

$$S\equiv(-1)^{mp^\alpha+r_*}\equiv(-1)^{m+r_*}\equiv(-1)^{l+r_*}\pmod p.$$

This concludes the proof of Theorem 1.2.

4. Proof of Theorem 1.3

For $i,k\in\mathbb{N}$ let $\delta_{i,k}$ be the Kronecker symbol which takes 1 or 0 according to whether $i=k$ or not. Since

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

we have

$$\begin{aligned}&(-1)^{(p-1)r}\sum_{k\equiv r\,(\mathrm{mod}\ p^{\alpha})}(-1)^k\binom{pn}{pk}\left(\frac{k-r}{p^{\alpha-1}}\right)^l\\
=&\sum_{k\equiv r\,(\mathrm{mod}\ p^{\alpha})}(-1)^{pk}\binom{pn}{pk}\left(\frac{k-r}{p^{\alpha-1}}\right)^l\\
=&\sum_{k=0}^{n}(-1)^{pk}\binom{pn}{pk}\sum_{i\equiv r\,(\mathrm{mod}\ p^{\alpha})}\left(\frac{i-r}{p^{\alpha-1}}\right)^l\delta_{i,k}\\
=&\sum_{k=0}^{n}(-1)^{pk}\binom{pn}{pk}\sum_{i\equiv r\,(\mathrm{mod}\ p^{\alpha})}\left(\frac{i-r}{p^{\alpha-1}}\right)^l\sum_{j\geqslant i}(-1)^{j-i}\binom{k}{j}\binom{j}{i}\\
=&\sum_{j=0}^{n}(-1)^jC_{n,j}\sum_{i\equiv r\,(\mathrm{mod}\ p^{\alpha})}(-1)^i\binom{j}{i}\left(\frac{i-r}{p^{\alpha-1}}\right)^l,\end{aligned}$$

where

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

As $C_{n,n}=(-1)^{pn}$, by the above

$$\begin{aligned}&(-1)^{(p-1)r}\sum_{k\equiv r\,(\mathrm{mod}\ p^{\alpha})}(-1)^k\binom{pn}{pk}\left(\frac{k-r}{p^{\alpha-1}}\right)^l\\
&-(-1)^{(p-1)n}\sum_{i\equiv r\,(\mathrm{mod}\ p^{\alpha})}(-1)^i\binom{n}{i}\left(\frac{i-r}{p^{\alpha-1}}\right)^l\\
=&\sum_{0\leqslant j<n}(-1)^jC_{n,j}\sum_{i\equiv r\,(\mathrm{mod}\ p^{\alpha})}(-1)^i\binom{j}{i}\left(\frac{i-r}{p^{\alpha-1}}\right)^l.\end{aligned}$$

Note that $(-1)^{(p-1)n}\equiv(-1)^{(p-1)r}\ (\mathrm{mod}\ p^{a_p})$. In view of Theorem 1.0,

$$\mathrm{ord}_p\bigg(\sum_{i\equiv r\,(\mathrm{mod}\ p^{\alpha})}(-1)^i\binom{j}{i}\left(\frac{i-r}{p^{\alpha-1}}\right)^l\bigg)\geqslant\mathrm{ord}_p\bigg(\left\lfloor\frac{j}{p^{\alpha-1}}\right\rfloor!\bigg)=\sum_{s=\alpha}^{\infty}\left\lfloor\frac{j}{p^s}\right\rfloor.$$

So it suffices to show that

$$\operatorname{ord}_p(C_{n,j}) \geqslant a_p+\operatorname{ord}_p\bigg(\Big\lfloor\frac{n}{p^{\alpha-1}}\Big\rfloor!\bigg)-\sum_{s=\alpha}^{\infty}\Big\lfloor\frac{j}{p^s}\Big\rfloor = a_p+\sum_{s=\alpha}^{\infty}\bigg(\Big\lfloor\frac{n}{p^s}\Big\rfloor-\Big\lfloor\frac{j}{p^s}\Big\rfloor\bigg)$$

for any $j\in\mathbb{N}$ with $j<n$.

Fix a nonnegative integer $j<n$. In light of Theorem 1.0,

$$\operatorname{ord}_p(j!C_{n,j}) \geqslant \operatorname{ord}_p\bigg(\Big\lfloor\frac{pn}{p^{1-1}}\Big\rfloor!\bigg)-j=\sum_{s=0}^{\infty}\Big\lfloor\frac{n}{p^s}\Big\rfloor-j.$$

By Lemma 3.2 of [SD] and its proof, $C_{n,j}$ is congruent to

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{k}{j}=(-1)^j\binom{n}{j}\sum_{k\geqslant j}(-1)^{k-j}\binom{n-j}{k-j}=0$$

modulo $p^{2\operatorname{ord}_p(n)+a_p}$. In the case $p>3$, by Jacobsthal's result (cf. [G]), if $k\in\{1,\ldots,n\}$, then

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

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

$$\binom{pn}{pk}-\binom{n}{k}=\binom{n}{k}p^3nk(n-k)q_k=p^3n^2(n-1)\binom{n-2}{k-1}q_k.$$

So we also have $\operatorname{ord}_p(C_{n,j})\geqslant\operatorname{ord}_p(n-1)+3$ when $p>3$. These facts will be used in the following discussion.

Case 1. $n-j\geqslant a_p$.

In this case,

$$\begin{aligned}\operatorname{ord}_p(C_{n,j}) \geqslant&\sum_{s=0}^{\infty}\Big\lfloor\frac{n}{p^s}\Big\rfloor-j-\operatorname{ord}_p(j!)=\sum_{s=0}^{\infty}\bigg(\Big\lfloor\frac{n}{p^s}\Big\rfloor-\Big\lfloor\frac{j}{p^s}\Big\rfloor\bigg)\\ =&n-j+\sum_{s=1}^{\infty}\bigg(\Big\lfloor\frac{n}{p^s}\Big\rfloor-\Big\lfloor\frac{j}{p^s}\Big\rfloor\bigg)\\ \geqslant&a_p+\sum_{s=\alpha}^{\infty}\bigg(\Big\lfloor\frac{n}{p^s}\Big\rfloor-\Big\lfloor\frac{j}{p^s}\Big\rfloor\bigg).\end{aligned}$$

Case 2. $0<n-j<a_p\leqslant 3$, and $p\mid n$ or $j\neq n-2$.

If $\beta = \mathrm{ord}_p(n) > 0$, then $n - j < a_p < p \leqslant p^\beta$ and hence

$$\left\lfloor \frac{n}{p^{\beta+1}} \right\rfloor = \left\lfloor \frac{n/p^\beta}{p} \right\rfloor = \left\lfloor \frac{n/p^\beta - 1}{p} \right\rfloor = \left\lfloor \frac{\lfloor j/p^\beta \rfloor}{p} \right\rfloor = \left\lfloor \frac{j}{p^{\beta+1}} \right\rfloor,$$

therefore

$$\begin{aligned}\sum_{s=\alpha}^{\infty}\left(\left\lfloor \frac{n}{p^s} \right\rfloor - \left\lfloor \frac{j}{p^s} \right\rfloor \right) &= \sum_{\alpha \leqslant s \leqslant \beta} \left(\frac{n}{p^s} - \left\lfloor \frac{j}{p^s} \right\rfloor \right) \\ &\leqslant \sum_{\alpha \leqslant s \leqslant \beta} 1 < 2\beta = 2\mathrm{ord}_p(n) \leqslant \mathrm{ord}_p(C_{n,j}) - a_p.\end{aligned}$$

When $\beta = \mathrm{ord}_p(n) = 0$ (i.e., $p \nmid n$) and $j = n - 1$, we have

$$\sum_{s=\alpha}^{\infty}\left(\left\lfloor \frac{n}{p^s} \right\rfloor - \left\lfloor \frac{j}{p^s} \right\rfloor \right) = 0 = 2\mathrm{ord}_p(n) \leqslant \mathrm{ord}_p(C_{n,j}) - a_p.$$

Case 3. $n - j = 2 < a_p$ and $p \nmid n$.
In this case, $a_p = 3 < p$ and

$$\begin{aligned}\mathrm{ord}_p(C_{n,j}) - a_p \geqslant& \mathrm{ord}_p(n-1) \geqslant \sum_{\alpha \leqslant s \leqslant \mathrm{ord}_p(n-1)} \left(\frac{n-1}{p^s} - \left\lfloor \frac{n-2}{p^s} \right\rfloor \right) \\ =& \sum_{s=\alpha}^{\infty}\left(\left\lfloor \frac{n-1}{p^s} \right\rfloor - \left\lfloor \frac{n-2}{p^s} \right\rfloor \right) = \sum_{s=\alpha}^{\infty}\left(\left\lfloor \frac{n}{p^s} \right\rfloor - \left\lfloor \frac{j}{p^s} \right\rfloor \right).\end{aligned}$$

Combining the above we have completed the proof of Theorem 1.3.

References

[C] L. Carlitz, *Congruences for generalized Bell and Stirling numbers*, Duke Math. J. **22** (1955), 193–205.

[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.

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

[GKP] R. 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.

[K] Y. H. H. Kwong, *Minimum periods of* $S(n,k)$ *modulo* M, Fibonacci Quart. **27** (1989), 217–221.

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

[NW] A. Nijenhuis and H. S. Wilf, *Periodicities of partition functions and Stirling numbers modulo p*, J. Number Theory **25** (1987), 308–312.

[S] 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.

[SD] Z. W. Sun and D. M. Davis, *Combinatorial congruences modulo prime powers*, Trans. Amer. Math. Soc., to appear. http://arxiv.org/abs/math.NT/0508087.

[ST] Z. W. Sun and R. Tauraso, *Congruences for sums of binomial coefficients*, J. Number Theory, to appear. http://arxiv.org/abs/math.NT/0502187.

[SW] Z. W. Sun and D. Wan, *Lucas-type congruences for cyclotomic ψ-coefficients*, Int. J. Number Theory, to appear. http://arxiv.org/abs/math.NT/0512012.

Department of Mathematics
Nanjing University
Nanjing 210093
People's Republic of China
zwsun@nju.edu.cn
http://math.nju.edu.cn/~zwsun