ACTA ARITHMETICA
132.4 (2008)

Congruences for Stirling numbers and Eulerian numbers

by

HUI-QIN CAO and HAO PAN (Nanjing)

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

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

We also set $\binom{x}{k} = 0$ for any negative integer k.

Let p be a prime, and let $n > 0$ and r be integers. In 1913, A. Fleck (cf. [3, p. 274]) discovered that

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

where $\lfloor\cdot\rfloor$ is the floor function. In 1977, C. S. Weisman [14] extended Fleck's congruence to prime power moduli in the following way:

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

where α is a positive integer and $n \geq p^{\alpha-1}$.

In 2005, in his lecture notes on Fontaine's rings, D. Wan got another extension of Fleck's congruence:

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

where $l \in \mathbb{N} = \{0, 1, 2, \ldots\}$ and $n > lp$. Later, by a combinatorial approach, Z. W. Sun [7] established a common generalization of Weisman's and Wan's extensions of Fleck's congruence:

2000 *Mathematics Subject Classification*: Primary 11A07; Secondary 05A15, 11B65, 11B73.

Key words and phrases: Stirling number, Eulerian number, congruence.

$$\operatorname{ord}_p\Big(\sum_{k\equiv r\,(\mathrm{mod}\,p^\beta)}\binom{n}{k}(-1)^k\binom{\lfloor (k-r)/p^\alpha\rfloor}{l}\Big) \geq \Big\lfloor \frac{n-p^{\alpha-1}-l}{p^{\alpha-1}(p-1)}\Big\rfloor-(l-1)\alpha-\beta \tag{1.4}$$

provided that $\alpha,\beta\in\mathbb{N}$, $\alpha\geq\beta$ and $n\geq p^{\alpha-1}$, where $\operatorname{ord}_p(a)=\sup\{i\in\mathbb{N}: p^i\mid a\}$ is the p-adic order of $a\in\mathbb{Z}$.

In fact, with the help of the ψ-operator in Fontaine's theory of (ϕ,Γ)-modules, (1.3) and (1.4) can be improved as follows [13]:

$$\operatorname{ord}_p\Big(\sum_{k\equiv r\,(\mathrm{mod}\,p^\alpha)}\binom{n}{k}(-1)^k\binom{(k-r)/p^\alpha}{l}\Big) \geq \Big\lfloor \frac{n-p^{\alpha-1}-lp^\alpha}{p^{\alpha-1}(p-1)}\Big\rfloor. \tag{1.5}$$

A combinatorial proof of (1.5) is given in [11]. On the other hand, motivated by algebraic topology, D. M. Davis and Z. W. Sun [2, 10] showed that

$$\operatorname{ord}_p\Big(\sum_{k\equiv r\,(\mathrm{mod}\,p^\alpha)}\binom{n}{k}(-1)^k\binom{(k-r)/p^\alpha}{l}\Big) \geq \operatorname{ord}_p\Big(\Big\lfloor\frac{n}{p^\alpha}\Big\rfloor!\Big) \tag{1.6}$$

and

$$\operatorname{ord}_p\Big(\sum_{k\equiv r\,(\mathrm{mod}\,p^\alpha)}\binom{n}{k}(-1)^k\binom{(k-r)/p^\alpha}{l}\Big) \geq \operatorname{ord}_p\Big(\Big\lfloor\frac{n}{p^{\alpha-1}}\Big\rfloor!\Big)-l-\operatorname{ord}_p(l!). \tag{1.7}$$

Notice that (1.6) and (1.7) cannot be deduced from (1.5) though they have the similar flavor. For the further developments on (1.5) and (1.6), the reader is referred to [8, 11, 12, 9].

In the present paper, we shall investigate some Fleck–Weisman and Davis–Sun type congruences for other number arrays. The *Stirling number $s(n,k)$ of the first kind* is the number of permutations of $\{1,\dots,n\}$ which contain exactly k permutation cycles. $s(n,k)$ $(0\leq k\leq n)$ can be given by

$$x(x+1)\cdots(x+n-1)=\sum_{k=0}^{n}s(n,k)x^k.$$

Similarly, the *Stirling number $S(n,k)$ of the second kind* is the number of ways to partition a set of cardinality n into k nonempty subsets. It is well known that

$$x^n=\sum_{k=0}^{n}S(n,k)k!\binom{x}{k}$$

for $n\in\mathbb{N}$. In particular, we set $s(0,0)=S(0,0)=1$ and $s(n,k)=S(n,k)=0$ whenever $k>n$.

Another important array of numbers related to permutations is formed by the so-called Eulerian numbers. For an arbitrary permutation $\pi = a_1 \cdots a_n$ of $\{1, \ldots, n\}$, we say that an element $i \in \{1, \ldots, n-1\}$ is an *ascent* of π if $a_i < a_{i+1}$. The *Eulerian number* $\left\langle {n \atop k} \right\rangle$ is the number of permutations of $\{1, \ldots, n\}$ having exactly k ascents. (Another commonly used notation is $A(n,k)$ (sometimes $A_{n,k}$) with $A(n,k) = \left\langle {n \atop k-1} \right\rangle$.) Clearly $\left\langle {n \atop 0} \right\rangle = 1$ and $\left\langle {n \atop k} \right\rangle = 0$ for every $k > n-1$. We also set $\left\langle {n \atop k} \right\rangle = 0$ when $k < 0$. It is easy to check that the Eulerian numbers satisfy the recurrence relation

$$\left\langle {n \atop k} \right\rangle = (k+1)\left\langle {n-1 \atop k} \right\rangle + (n-k)\left\langle {n-1 \atop k-1} \right\rangle.$$

The Stirling numbers of the first and second kind and the Eulerian numbers play important roles in enumerative combinatorics (cf. [4, pp. 257–272] and [5, pp. 123–127]). Many arithmetic properties of these numbers are listed in [6, Chapter 5]. A little surprisingly, the Eulerian numbers satisfy a congruence mixing (1.5) and (1.7) in some way.

Theorem 1.1. *Let p be a prime. Let $n > 0$ and r be integers. Then for any positive integer α and $l \in \mathbb{N}$, we have*

$$\operatorname{ord}_p\Big(\sum_{k \equiv r \,(\operatorname{mod} p^\alpha)} \left\langle {n \atop k} \right\rangle \binom{(k-r)/p^\alpha}{l}\Big) \geq \operatorname{ord}_p\Big(\Big\lfloor \frac{n}{p^{\alpha-1}} \Big\rfloor !\Big) - l - \Big\lceil \frac{1+l}{p-1} \Big\rceil, \tag{1.8}$$

where $\lceil \cdot \rceil$ is the ceiling function. Moreover, if a is an integer with $a \equiv 1 \pmod{p}$, then

$$\sum_{k \equiv r \,(\operatorname{mod} p^\alpha)} \left\langle {n \atop k} \right\rangle a^k \equiv 0 \pmod{p^{\operatorname{ord}_p(\lfloor n/p^{\alpha-1} \rfloor !)-1}} \tag{1.9}$$

provided that $n \geq p^\alpha$.

The results on Stirling numbers are a little complicated. We have the following Davis–Sun type congruence:

Theorem 1.2. *Let p be a prime and n, m be positive integers. For arbitrary integers a and r,*

$$\operatorname{ord}_p\Big(\sum_{k \equiv r \,(\operatorname{mod} p-1)} s(n,k) S(k,m) a^k\Big) \geq \operatorname{ord}_p(n!) - \operatorname{ord}_p(m!). \tag{1.10}$$

Moreover, if $f(x)$ is a polynomial with integral coefficients, then

$$\operatorname{ord}_p\Big(\sum_{k \equiv r \,(\operatorname{mod} p-1)} s(n,k) f(k) a^k\Big) \geq \operatorname{ord}_p(n!) - \log_p \binom{n}{l}, \tag{1.11}$$

where $l = \min\{\deg f, \lfloor n/p \rfloor\}$ and $\log_p x = \log x / \log p$.

Also, we have the following Weisman type congruence.

THEOREM 1.3. *Let p be a prime and n, m be positive integers. For any integers a, r and $\alpha \geq 1$,*

$$\operatorname{ord}_p\Big(\sum_{k\equiv r\,(\mathrm{mod}\,p^\alpha(p-1))} s(n,k)S(k,m)a^k\Big) \geq \left\lfloor \frac{n-p^\alpha}{p^\alpha(p-1)} \right\rfloor - \operatorname{ord}_p(m!). \tag{1.12}$$

Combining Theorems 1.2 and 1.3, we immediately deduce

COROLLARY 1.1.

$$\operatorname{ord}_p\Big(\sum_{k\equiv r\,(\mathrm{mod}\,\varphi(p^\alpha))} s(n,k)a^k\Big) \geq \begin{cases} \operatorname{ord}_p(n!) & \text{if } \alpha = 1,\\ \lfloor (n-p^{\alpha-1})/\varphi(p^\alpha)\rfloor & \text{if } \alpha \geq 2, \end{cases} \tag{1.13}$$

where φ denotes the Euler totient function.

The proofs of Theorems 1.1–1.3 will be given in the next sections.

2. Congruences for Eulerian numbers: $k \equiv r \pmod{p^\alpha}$. In this section, we shall prove Theorem 1.1. The following lemma gives a weak (but non-trivial) lower bound for the p-adic order of $S(n,k)$.

LEMMA 2.1. *Let p be a prime and let $n, k \in \mathbb{N}$. Then for any positive integer α,*

$$\operatorname{ord}_p(k!S(n,k)) \geq \operatorname{ord}_p\left(\left\lfloor \frac{n}{p^{\alpha-1}} \right\rfloor !\right) - \left\lfloor \frac{n-k}{p^{\alpha-1}(p-1)} \right\rfloor. \tag{2.1}$$

Proof. We use induction on n. There is nothing to do when $n = 0$. Below we assume that $n \geq 1$ and (2.1) is valid for smaller values of n. Obviously (2.1) holds for $k = 0$ since

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

Suppose that $k \geq 1$. It is known (cf. [1, p. 209]) that

$$k!S(n,k) = \sum_{i=k-1}^{n-1} \binom{n}{i} (k-1)!S(i,k-1) \quad (k \geq 1). \tag{2.2}$$

Observe that

$$\begin{aligned}\operatorname{ord}_p\left(\binom{n}{i}\right) &= \sum_{j=1}^{\infty}\left(\left\lfloor\frac{n}{p^j}\right\rfloor - \left\lfloor\frac{n-i}{p^j}\right\rfloor - \left\lfloor\frac{i}{p^j}\right\rfloor\right)\\ &\geq \sum_{j=\alpha}^{\infty}\left(\left\lfloor\frac{n}{p^j}\right\rfloor - \left\lfloor\frac{n-i}{p^j}\right\rfloor - \left\lfloor\frac{i}{p^j}\right\rfloor\right)\\ &= \operatorname{ord}_p\left(\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\right) - \operatorname{ord}_p\left(\left\lfloor\frac{n-i}{p^{\alpha-1}}\right\rfloor!\right) - \operatorname{ord}_p\left(\left\lfloor\frac{i}{p^{\alpha-1}}\right\rfloor!\right).\end{aligned}$$

By the induction hypothesis, for $k-1 \leq i \leq n-1$ we have

$$\begin{aligned}&\operatorname{ord}_p\left(\binom{n}{i}(k-1)!S(i,k-1)\right)\\ &\quad\geq \operatorname{ord}_p\left(\binom{n}{i}\right) + \operatorname{ord}_p\left(\left\lfloor\frac{i}{p^{\alpha-1}}\right\rfloor!\right) - \left\lfloor\frac{i-(k-1)}{p^{\alpha-1}(p-1)}\right\rfloor\\ &\quad\geq \operatorname{ord}_p\left(\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\right) - \operatorname{ord}_p\left(\left\lfloor\frac{n-i}{p^{\alpha-1}}\right\rfloor!\right) - \left\lfloor\frac{i-k+1}{p^{\alpha-1}(p-1)}\right\rfloor\\ &\quad\geq \operatorname{ord}_p\left(\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\right) - \left\lfloor\frac{n-i-1}{p^{\alpha-1}(p-1)}\right\rfloor - \left\lfloor\frac{i-k+1}{p^{\alpha-1}(p-1)}\right\rfloor\\ &\quad\geq \operatorname{ord}_p\left(\left\lfloor\frac{n}{p^{\alpha-1}}\right\rfloor!\right) - \left\lfloor\frac{n-k}{p^{\alpha-1}(p-1)}\right\rfloor. \ \blacksquare\end{aligned}$$

LEMMA 2.2. *Let n be a positive integer. Then for any polynomial $f(x) \in \mathbb{Q}[x]$ we have*

$$\sum_k \left\langle {n \atop k} \right\rangle f(k)x^k = \sum_m m!S(n,m)\sum_{i=0}^{n-m}\binom{n-m}{i}(-1)^{n-m-i}f(i)x^i. \tag{2.3}$$

Proof. It is sufficient to prove (2.3) for $f(x) = x^l$, $l \in \mathbb{N}$. In the case $l = 0$, (2.3) reduces to

$$\begin{aligned}\sum_k \left\langle {n \atop k} \right\rangle x^k &= \sum_m m!S(n,m)\sum_{i=0}^{n-m}\binom{n-m}{i}(-1)^{n-m-i}x^i \\ &= \sum_m m!S(n,m)(x-1)^{n-m},\end{aligned} \tag{2.4}$$

which is true (cf. [4, p. 269]). Now assume that $l > 0$ and (2.3) holds for $l-1$, that is,

$$\sum_k \left\langle {n \atop k} \right\rangle k^{l-1}x^k = \sum_m m!S(n,m)\sum_{i=0}^{n-m}\binom{n-m}{i}(-1)^{n-m-i}i^{l-1}x^i.$$

Taking derivatives of both sides of the above equation with respect to x, we get

$$\sum_k \left\langle {n \atop k} \right\rangle k^l x^{k-1} = \sum_m m!S(n,m) \sum_{i=1}^{n-m} \binom{n-m}{i} (-1)^{n-m-i} i^l x^{i-1}. \ \blacksquare$$

Proof of (1.8). Let ζ be a primitive p^αth root of the unity. Then

$$\begin{aligned}\sum_{k \equiv r \,(\mathrm{mod}\, p^\alpha)} \left\langle {n \atop k} \right\rangle \binom{(k-r)/p^\alpha}{l} &= \sum_k \left\langle {n \atop k} \right\rangle \binom{(k-r)/p^\alpha}{l} \frac{1}{p^\alpha} \sum_{j=0}^{p^\alpha-1} \zeta^{j(k-r)} \\ &= \frac{1}{p^\alpha} \sum_{j=0}^{p^\alpha-1} \zeta^{-jr} \sum_k \left\langle {n \atop k} \right\rangle \binom{(k-r)/p^\alpha}{l} \zeta^{jk}.\end{aligned}$$

Note that $\binom{(x-r)/p^\alpha}{l}$ is a polynomial in x with rational coefficients of degree l. By Lemma 2.2, we have

$$\begin{aligned}&\sum_{k \equiv r \,(\mathrm{mod}\, p^\alpha)} \left\langle {n \atop k} \right\rangle \binom{(k-r)/p^\alpha}{l} \\ &= \frac{1}{p^\alpha} \sum_{j=0}^{p^\alpha-1} \zeta^{-jr} \sum_m m!S(n,m) \sum_{i=0}^{n-m} \binom{n-m}{i} (-1)^{n-m-i} \binom{(i-r)/p^\alpha}{l} \zeta^{ji} \\ &= \sum_{m=0}^{n} m!S(n,m) \sum_{i=0}^{n-m} \binom{n-m}{i} (-1)^{n-m-i} \binom{(i-r)/p^\alpha}{l} \frac{1}{p^\alpha} \sum_{j=0}^{p^\alpha-1} \zeta^{j(i-r)} \\ &= \sum_{m=0}^{n} m!S(n,m) \sum_{i \equiv r \,(\mathrm{mod}\, p^\alpha)} \binom{n-m}{i} (-1)^{n-m-i} \binom{(i-r)/p^\alpha}{l}.\end{aligned}$$

Applying Lemma 2.1 and (1.5), for every $0 \le m \le n$ we have

$$\begin{aligned}&\mathrm{ord}_p \left(m!S(n,m) \sum_{i \equiv r \,(\mathrm{mod}\, p^\alpha)} \binom{n-m}{i} (-1)^{n-m-i} \binom{(i-r)/p^\alpha}{l} \right) \\ &\qquad \ge \mathrm{ord}_p \left(\left\lfloor \frac{n}{p^{\alpha-1}} \right\rfloor ! \right) - \left\lfloor \frac{n-m}{p^{\alpha-1}(p-1)} \right\rfloor + \left\lfloor \frac{n-m-p^{\alpha-1}-lp^\alpha}{p^{\alpha-1}(p-1)} \right\rfloor \\ &\qquad \ge \mathrm{ord}_p \left(\left\lfloor \frac{n}{p^{\alpha-1}} \right\rfloor ! \right) - \left\lceil \frac{p^{\alpha-1}+lp^\alpha}{p^{\alpha-1}(p-1)} \right\rceil \\ &\qquad = \mathrm{ord}_p \left(\left\lfloor \frac{n}{p^{\alpha-1}} \right\rfloor ! \right) - l - \left\lceil \frac{1+l}{p-1} \right\rceil. \ \blacksquare\end{aligned}$$

Proof of (1.9). Let ζ be a primitive p^αth root of the unity. Using (2.4) we have

$$\begin{aligned}\sum_{k\equiv r\,(\mathrm{mod}\,p^\alpha)}\left\langle{n\atop k}\right\rangle a^k &= \sum_k \left\langle{n\atop k}\right\rangle a^k \frac{1}{p^\alpha}\sum_{j=0}^{p^\alpha-1}\zeta^{j(k-r)} = \frac{1}{p^\alpha}\sum_{j=0}^{p^\alpha-1}\zeta^{-jr}\sum_k\left\langle{n\atop k}\right\rangle(a\zeta^j)^k \\ &= \frac{1}{p^\alpha}\sum_{j=0}^{p^\alpha-1}\zeta^{-jr}\sum_m m!S(n,m)(a\zeta^j-1)^{n-m} \\ &= \frac{1}{p^\alpha}\sum_{j=0}^{p^\alpha-1}\zeta^{-jr}\sum_{m=0}^{n} m!S(n,m)\sum_{i=0}^{n-m}\binom{n-m}{i}(-1)^{n-m-i}a^i\zeta^{ji} \\ &= \sum_{m=0}^{n} m!S(n,m)(-1)^{n-m}\sum_{i=0}^{n-m}\binom{n-m}{i}(-a)^i\frac{1}{p^\alpha}\sum_{j=0}^{p^\alpha-1}\zeta^{j(i-r)} \\ &= \sum_{m=0}^{n} m!S(n,m)(-1)^{n-m}\sum_{i\equiv r\,(\mathrm{mod}\,p^\alpha)}\binom{n-m}{i}(-a)^i.\end{aligned}$$

In view of Lemma 2.1 and (1.8) in [7],

$$\begin{aligned}&\mathrm{ord}_p\bigg(m!S(n,m)\sum_{i\equiv r\,(\mathrm{mod}\,p^\alpha)}\binom{n-m}{i}(-a)^i\bigg) \\ &\qquad\ge \mathrm{ord}_p\bigg(\bigg\lfloor\frac{n}{p^{\alpha-1}}\bigg\rfloor!\bigg)-\bigg\lfloor\frac{n-m}{p^{\alpha-1}(p-1)}\bigg\rfloor+\bigg\lfloor\frac{n-m-p^{\alpha-1}}{p^{\alpha-1}(p-1)}\bigg\rfloor \\ &\qquad\ge \mathrm{ord}_p\bigg(\bigg\lfloor\frac{n}{p^{\alpha-1}}\bigg\rfloor!\bigg)-1 \quad \text{for every } 0\le m\le n. \ \blacksquare\end{aligned}$$

3. Congruences for Stirling numbers: $k\equiv r \pmod{p-1}$**.** In this section, we shall prove Theorem 1.2. For a prime p, we let $\mathbb{Z}_p$ and $\mathbb{Q}_p$ denote the ring of p-adic integers and the field of p-adic numbers respectively.

Lemma 3.1. *Let p be a prime. For any $n\in\mathbb{N}$ and $x\in\mathbb{Z}_p$, $\binom{x}{n}$ is p-integral.*

Proof. We may choose $x'\in\mathbb{N}$ such that

$$x\equiv x' \pmod{p^{\mathrm{ord}_p(n!)+1}}.$$

Then

$$\begin{aligned}\binom{x}{n} &= \frac{x(x-1)\cdots(x-n+1)}{n!} \\ &\equiv \frac{x'(x'-1)\cdots(x'-n+1)}{n!} = \binom{x'}{n} \pmod{p}.\end{aligned}$$

This shows that $\binom{x}{n}\in\mathbb{Z}_p$ since $\binom{x'}{n}\in\mathbb{Z}$. ∎

Proof of (1.10). Let ω be the Teichmüller character of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. As an application of Hensel's lemma, we know that

$$\omega(a) \in \mathbb{Z}_p, \qquad a = 1, \dots, p-1,$$

are exactly all $(p-1)$th roots of unity in $\mathbb{Q}_p$. Moreover, $\omega(g)$ is a primitive $(p-1)$th root of unity if and only if g is a primitive root modulo p. Let $\varpi \in \mathbb{Z}_p$ be an arbitrary primitive $(p-1)$th root of unity in $\mathbb{Q}_p$. Then

$$\begin{aligned}\sum_{k \equiv r \,(\mathrm{mod}\, p-1)} s(n,k)S(k,m)a^k &= \sum_{k=0}^{n} s(n,k)S(k,m)a^k \cdot \frac{1}{p-1}\sum_{j=1}^{p-1} \varpi^{j(k-r)} \\ &= \frac{1}{p-1}\sum_{j=1}^{p-1} \varpi^{-jr} \sum_k s(n,k)S(k,m)(a\varpi^j)^k.\end{aligned}$$

It is known that

$$m!S(k,m) = \sum_{i=0}^{m} \binom{m}{i}(-1)^{m-i} i^k,$$

so

$$\begin{aligned}&\sum_{k \equiv r \,(\mathrm{mod}\, p-1)} s(n,k)S(k,m)a^k \\ &\quad = \frac{1}{p-1}\sum_{j=1}^{p-1} \varpi^{-jr} \sum_k s(n,k)\bigg(\frac{1}{m!}\sum_{i=0}^{m}\binom{m}{i}(-1)^{m-i}i^k\bigg)(a\varpi^j)^k \\ &\quad = \frac{1}{m!(p-1)}\sum_{j=1}^{p-1} \varpi^{-jr} \sum_{i=0}^{m}\binom{m}{i}(-1)^{m-i}\sum_k s(n,k)(ai\varpi^j)^k \\ &\quad = \frac{n!}{m!(p-1)}\sum_{j=1}^{p-1} \varpi^{-jr} \sum_{i=0}^{m}\binom{m}{i}(-1)^{m-i}\binom{ai\varpi^j + n - 1}{n}.\end{aligned}$$

Thus applying Lemma 3.1, it is derived that

$$\mathrm{ord}_p\bigg(\sum_{k \equiv r \,(\mathrm{mod}\, p-1)} s(n,k)S(k,m)a^k\bigg) \ge \mathrm{ord}_p(n!/m!) = \mathrm{ord}_p(n!) - \mathrm{ord}_p(m!). \ \blacksquare$$

LEMMA 3.2. *Let n and l be positive integers. Then*

$$(n-i)\binom{i}{l-1} \le \binom{n}{l} \qquad \textit{for each integer } 0 \le i \le n.$$

Proof. Clearly, the desired result is true if $n < l$. Below we assume that $n \ge l$. It is easy to check that

$$(n-i)\binom{i}{l-1} \ge (n-i+1)\binom{i-1}{l-1} \ \Leftrightarrow\ i \le \frac{(l-1)(n+1)}{l}.$$

Hence

$$
\begin{aligned}
(n-i)\binom{i}{l-1} &\le (n-\lfloor (l-1)(n+1)/l\rfloor)\binom{\lfloor (l-1)(n+1)/l\rfloor}{l-1}\\
&= \left\lceil \frac{n-l+1}{l}\right\rceil \binom{n-\lceil (n-l+1)/l\rceil}{l-1}\\
&\le \frac{n}{l}\binom{n-1}{l-1}=\binom{n}{l}. \ \blacksquare
\end{aligned}
$$

Proof of (1.11). We use induction on $\deg f$. The case $\deg f = 0$ follows from (1.10) by setting $m = 1$. Below we assume that $\deg f > 0$ and (1.11) holds for smaller values of $\deg f$. It is known (cf. [1, p. 215]) that

$$ks(n,k) = \sum_{i=k-1}^{n-1} \binom{n}{i}(n-i-1)!s(i,k-1) \quad (k \ge 1). \tag{3.1}$$

Write $f(x) = xf_1(x) + c$ with $\deg f_1 = \deg f - 1$. Then

$$
\begin{aligned}
&\sum_{k\equiv r \,(\mathrm{mod}\, p-1)} s(n,k)f(k)a^k\\
&= \sum_{k\equiv r \,(\mathrm{mod}\, p-1)} f_1(k)a^k \sum_{i=k-1}^{n-1}\binom{n}{i}(n-i-1)!s(i,k-1)\\
&\quad + c\sum_{k\equiv r \,(\mathrm{mod}\, p-1)} s(n,k)a^k\\
&= \sum_{i=0}^{n-1}\frac{n!}{i!(n-i)}\sum_{k\equiv r \,(\mathrm{mod}\, p-1)} s(i,k-1)f_1(k)a^k + c\sum_{k\equiv r \,(\mathrm{mod}\, p-1)} s(n,k)a^k\\
&= \sum_{i=0}^{n-1}\frac{n!a}{i!(n-i)}\sum_{k\equiv r-1 \,(\mathrm{mod}\, p-1)} s(i,k)f_1(k+1)a^k + c\sum_{k\equiv r \,(\mathrm{mod}\, p-1)} s(n,k)a^k.
\end{aligned}
$$

When $i = 0$,

$$
\begin{aligned}
&\mathrm{ord}_p\left(\frac{an!}{0!(n-0)}\sum_{k\equiv r-1 \,(\mathrm{mod}\, p-1)} s(0,k)f_1(k+1)a^k\right)\\
&\qquad \ge \mathrm{ord}_p(n!) - \mathrm{ord}_p(n)\\
&\qquad \ge \begin{cases} 0 = \mathrm{ord}_p(n!) - \log_p\binom{n}{0} & \text{if } n < p,\\ \mathrm{ord}_p(n!) - \log_p n \ge \mathrm{ord}_p(n!) - \log_p\binom{n}{l} & \text{otherwise.}\end{cases}
\end{aligned}
$$

For every $0 < i \le n-1$, by the induction hypothesis,

$$\begin{aligned}\operatorname{ord}_p\biggl(\frac{n!a}{i!(n-i)}\sum_{k\equiv r-1\,(\mathrm{mod}\,p-1)} s(i,k)f_1(k+1)a^k\biggr)\\ &\ge \operatorname{ord}_p(n!)-\operatorname{ord}_p(i!)-\operatorname{ord}_p(n-i)+\operatorname{ord}_p(i!)-\log_p\binom{i}{l'}\\ &= \operatorname{ord}_p(n!)-\operatorname{ord}_p(n-i)-\log_p\binom{i}{l'},\end{aligned}$$

where $l' = \min\{\deg f - 1, \lfloor i/p\rfloor\}$. It suffices to show that

$$\operatorname{ord}_p(n-i)+\log_p\binom{i}{l'} \le \log_p\binom{n}{l}.$$

When $i > n-p$, clearly $l-1 \le l' \le l$ and $\operatorname{ord}_p(n-i) = 0$. Hence

$$\binom{i}{l'} \le \max\biggl\{\binom{n-1}{l-1},\binom{n-1}{l}\biggr\} \le \binom{n}{l}.$$

Below we assume that $i \le n-p$. Then $\lfloor i/p\rfloor+1 \le \lfloor n/p\rfloor$. If $\deg f-1 \le \lfloor i/p\rfloor$, then applying Lemma 3.2 we obtain

$$(n-i)\binom{i}{l'} = (n-i)\binom{i}{\deg f-1} \le \binom{n}{\deg f} = \binom{n}{l}$$

since $\deg f \le \lfloor n/p\rfloor$ now. Also, when $\lfloor i/p\rfloor < \deg f - 1$, we have

$$(n-i)\binom{i}{l'} = (n-i)\binom{i}{\lfloor i/p\rfloor} \le \binom{n}{\lfloor i/p\rfloor+1} \le \binom{n}{l}$$

since $\lfloor i/p\rfloor + 1 \le \min\{\deg f, \lfloor n/p\rfloor\} = l$. In each of the above two cases, we obtain

$$\operatorname{ord}_p(n-i)+\log_p\binom{i}{l'} \le \log_p(n-i)+\log_p\binom{i}{l'} \le \log_p\binom{n}{l}. \quad\blacksquare$$

4. Congruences for Stirling numbers: $k \equiv r \pmod{p^\alpha(p-1)}$. In this section, we shall prove Theorem 1.3. Define

$$C_{d,r}(n,m,a) = \sum_{k\equiv r\,(\mathrm{mod}\,d)} s(n,k)S(k,m)a^k.$$

Let ζ_d be a primitive dth root of the unity. Then

$$(4.1)\quad C_{d,r}(n,m,a)$$
$$= \sum_k s(n,k)a^k\Big(\frac{1}{m!}\sum_{i=0}^m\binom{m}{i}(-1)^{m-i}i^k\Big)\Big(\frac{1}{d}\sum_{j=0}^{d-1}\zeta_d^{j(k-r)}\Big)$$
$$= \frac{1}{m!d}\sum_{j=0}^{d-1}\zeta_d^{-jr}\sum_{i=0}^m\binom{m}{i}(-1)^{m-i}\sum_k s(n,k)(ai\zeta_d^j)^k$$
$$= \frac{(-1)^n}{m!d}\sum_{i=0}^m\binom{m}{i}(-1)^{m-i}\sum_{j=0}^{d-1}\zeta_d^{-jr}(-ai\zeta_d^j)_n,$$

where

$$(x)_0 = 1 \quad\text{and}\quad (x)_k = x(x-1)\cdots(x-k+1)\quad\text{for } k=1,2,\ldots.$$

LEMMA 4.1. *Let p be a prime and α be a positive integer. Then for any $1 \le k \le p^\alpha(p-1)$, we have*

$$(4.2)\qquad s(p^\alpha(p-1),k) \equiv \begin{cases} 1 \pmod p & \text{if } k\equiv 0 \pmod{p^{\alpha-1}(p-1)},\\ 0 \pmod p & \text{otherwise.}\end{cases}$$

Proof. Let x be a variable. Apparently

$$x(x+1)\cdots(x+p-1) \equiv x^p - x \pmod p.$$

Thus

$$\sum_{k=0}^{p^\alpha(p-1)} s(p^\alpha(p-1),k)x^k = x(x+1)\cdots(x+p^\alpha(p-1)-1)$$
$$\equiv (x(x+1)\cdots(x+p-1))^{p^{\alpha-1}(p-1)} \equiv (x^p-x)^{p^{\alpha-1}(p-1)}$$
$$= \sum_{j=0}^{p^{\alpha-1}(p-1)}\binom{p^{\alpha-1}(p-1)}{j}(-1)^j x^{p^\alpha(p-1)-(p-1)j} \pmod p.$$

By the Lucas congruence, we know that for $0 \le j \le p^{\alpha-1}(p-1)$,

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

Hence

$$\sum_{k=0}^{p^\alpha(p-1)} s(p^\alpha(p-1),k)x^k \equiv \sum_{j=0}^{p-1}\binom{p-1}{j}(-1)^j x^{p^\alpha(p-1)-p^{\alpha-1}(p-1)j}$$
$$\equiv \sum_{j=0}^{p-1} x^{p^{\alpha-1}(p-1)(p-j)} = \sum_{j=1}^{p} x^{p^{\alpha-1}(p-1)j} \pmod p,$$

which is evidently equivalent to (4.2). ∎

Proof of Theorem 1.3. Since

$$s(n+1,k) = ns(n,k)+s(n,k-1) \quad \text{and} \quad S(n+1,k) = kS(n,k)+S(n,k-1),$$

we have

$$\begin{aligned}
&\sum_{k\equiv r\,(\mathrm{mod}\,d)} s(n+1,k)S(k,m)a^k \\
&\qquad = n\sum_{k\equiv r\,(\mathrm{mod}\,d)} s(n,k)S(k,m)a^k + \sum_{k\equiv r\,(\mathrm{mod}\,d)} s(n,k-1)S(k,m)a^k \\
&\qquad = n\sum_{k\equiv r\,(\mathrm{mod}\,d)} s(n,k)S(k,m)a^k \\
&\qquad\quad + \sum_{k\equiv r-1\,(\mathrm{mod}\,d)} s(n,k)(mS(k,m)+S(k,m-1))a^{k+1},
\end{aligned}$$

that is,

$$\begin{aligned}
&C_{d,r}(n+1,m,a) \\
&\qquad = nC_{d,r}(n,m,a) + amC_{d,r-1}(n,m,a) + aC_{d,r-1}(n,m-1,a).
\end{aligned}$$

Also observe that

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

Without loss of generality, we may assume that p^α divides n. We reason by induction on n. Clearly the case $n < p^{\alpha+1}$ is trivial. Let ζ be a primitive $p^\alpha(p-1)$th root of unity. Then in view of (4.1),

$$\begin{aligned}
&(-1)^n m! p^\alpha(p-1) C_{p^\alpha(p-1),r}(n+p^\alpha(p-1),m,a) \\
&= \sum_{i=0}^{m}\binom{m}{i}(-1)^{m-i}\sum_{j=1}^{p^\alpha(p-1)} \zeta^{-jr}(-ai\zeta^j)_n(-ai\zeta^j-n)_{p^\alpha(p-1)} \\
&= \sum_{i=0}^{m}\binom{m}{i}(-1)^{m-i}\sum_{j=1}^{p^\alpha(p-1)} \zeta^{-jr}(-ai\zeta^j)_n \sum_{k=0}^{p^\alpha(p-1)} s(p^\alpha(p-1),k)(ai\zeta^j+n)^k \\
&= \sum_{i=0}^{m}\binom{m}{i}(-1)^{m-i}\sum_{j=1}^{p^\alpha(p-1)} \zeta^{-jr}(-ai\zeta^j)_n \\
&\quad \times \sum_{k=0}^{p^\alpha(p-1)} s(p^\alpha(p-1),k)\sum_{l=0}^{k}\binom{k}{l}(ai\zeta^j)^l n^{k-l}.
\end{aligned}$$

Applying Lemma 4.1, we have

$$
\begin{aligned}
&m!C_{p^\alpha(p-1),r}(n+p^\alpha(p-1),m,a)\\
&\quad=\sum_{i=0}^{m}\binom{m}{i}(-1)^{m-i}\sum_{k=0}^{p^\alpha(p-1)}s(p^\alpha(p-1),k)\\
&\qquad\times\sum_{l=0}^{k}\binom{k}{l}(ai)^l n^{k-l}\cdot\frac{\sum_{j=1}^{p^\alpha(p-1)}\zeta^{j(l-r)}(-ai\zeta^j)_n}{(-1)^n p^\alpha(p-1)}\\
&\quad=\sum_{i=0}^{m}\binom{m}{i}(-1)^{m-i}\sum_{k=0}^{p^\alpha(p-1)}s(p^\alpha(p-1),k)\\
&\qquad\times\sum_{l=0}^{k}\binom{k}{l}(ai)^l n^{k-l}C_{p^\alpha(p-1),r-l}(n,1,ai)\\
&\quad\equiv\sum_{i=0}^{m}\binom{m}{i}(-1)^{m-i}\sum_{k=1}^{p}(ai)^{kp^{\alpha-1}(p-1)}C_{p^\alpha(p-1),r-kp^{\alpha-1}(p-1)}(n,1,ai)\\
&\qquad\qquad\pmod{p^{\lfloor\frac{n-p^\alpha}{p^\alpha(p-1)}\rfloor+1}},
\end{aligned}
$$

since $p^\alpha \mid n$ and

$$C_{p^\alpha(p-1),r-l}(n,1,ai)\equiv 0 \pmod{p^{\lfloor\frac{n-p^\alpha}{p^\alpha(p-1)}\rfloor}}$$

by the induction hypothesis on n. When $p\mid a$, clearly

$$m!C_{p^\alpha(p-1),r}(n+p^\alpha(p-1),m,a)\equiv 0 \pmod{p^{\lfloor\frac{n-p^\alpha}{p^\alpha(p-1)}\rfloor+1}}.$$

If $p\nmid a$,

$$
\begin{aligned}
&m!C_{p^\alpha(p-1),r}(n+p^\alpha(p-1),m,a)\\
&\equiv\sum_{\substack{0\le i\le m\\ p\nmid i}}\binom{m}{i}(-1)^{m-i}\sum_{k=1}^{p}((ai)^{p-1})^{kp^{\alpha-1}}C_{p^\alpha(p-1),r-kp^{\alpha-1}(p-1)}(n,1,ai)\\
&\equiv\sum_{\substack{0\le i\le m\\ p\nmid i}}\binom{m}{i}(-1)^{m-i}\sum_{k=1}^{p}C_{p^\alpha(p-1),r-kp^{\alpha-1}(p-1)}(n,1,ai)\pmod{p^{\lfloor\frac{n-p^\alpha}{p^\alpha(p-1)}\rfloor+1}}.
\end{aligned}
$$

Now

$$
\begin{aligned}
\sum_{k=1}^{p}C_{p^\alpha(p-1),r-kp^{\alpha-1}(p-1)}(n,1,ai)&=\sum_{k=1}^{p}\sum_{\substack{l\equiv r-kp^{\alpha-1}(p-1)\\ (\mathrm{mod}\,p^\alpha(p-1))}}s(n,l)(ai)^l\\
&=\sum_{l\equiv r\,(\mathrm{mod}\,p^{\alpha-1}(p-1))}s(n,l)(ai)^l=C_{p^{\alpha-1}(p-1),r}(n,1,ai).
\end{aligned}
$$

Thus it suffices to show that

$$\mathrm{ord}_p(C_{p^{\alpha-1}(p-1),r}(n,1,ai)) \geq \left\lfloor \frac{n-p^\alpha}{p^\alpha(p-1)} \right\rfloor + 1.$$

Note that $n \geq p^\alpha$ now. If $\alpha = 1$, then by (1.10),

$$\mathrm{ord}_p(C_{p-1,r}(n,1,ai)) \geq \mathrm{ord}_p(n!) \geq \left\lfloor \frac{n}{p} \right\rfloor \geq \left\lfloor \frac{n+p(p-2)}{p(p-1)} \right\rfloor = \left\lfloor \frac{n-p}{p(p-1)} \right\rfloor + 1.$$

Also if $\alpha \geq 2$, by the induction hypothesis, we have

$$\mathrm{ord}_p(C_{p^{\alpha-1}(p-1),r}(n,1,ai)) \geq \left\lfloor \frac{n-p^{\alpha-1}}{p^{\alpha-1}(p-1)} \right\rfloor \geq \left\lfloor \frac{n-p^\alpha}{p^\alpha(p-1)} \right\rfloor + 1. \quad \blacksquare$$

Acknowledgements. We thank our advisor, Professor Zhi-Wei Sun, for his helpful suggestions on this paper.

References

[1] L. Comtet, *Advanced Combinatorics*, Reidel, Dordrecht, 1974.

[2] 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.

[3] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York, 1966.

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

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

[6] J. Sándor and B. Crstici, *Handbook of Number Theory II*, Kluwer, Dordrecht, 2004.

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

[8] —, *Combinatorial congruences and Stirling numbers*, ibid. 126 (2007), 387–398.

[9] —, *Fleck quotients and Bernoulli numbers*, preprint, arXiv:math.NT/0608328.

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

[11] Z. W. Sun and D. Wan, *Lucas type congruences for cyclotomic ψ-coefficients*, Int. J. Number Theory 4 (2008), 155–170.

[12] —, —, *On Fleck quotients*, Acta Arith. 127 (2007), 337–363.

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

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

Hui-Qin Cao
Department of Applied Mathematics
Nanjing Audit University
Nanjing 210029
People's Republic of China
E-mail: caohq@nau.edu.cn

Hao Pan
Department of Mathematics
Nanjing University
Nanjing 210093
People's Republic of China
E-mail: haopan79@yahoo.com.cn

Received on 2.4.2007 (5422)