A talk given at University of Wisconsin at Madison (April 6, 2006).

RECENT PROGRESS ON CONGRUENCES INVOLVING BINOMIAL COEFFICIENTS

Zhi-Wei Sun

Department of Mathematics
Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://pweb.nju.edu.cn/zwsun

Abstract. In 1913 A. Fleck proved that if p is a prime, and $n > 0$ and r are integers then

$$\sum_{k\equiv r\ (\mathrm{mod}\ p)} \binom{n}{k}(-1)^k \equiv 0\ \left(\mathrm{mod}\ p^{\lfloor (n-1)/(p-1)\rfloor}\right).$$

Only recently the significance of Fleck's congruence was realized. It plays a fundamental role in Colmez' and Wan's investigation of the ψ-operator related to Fontaine's theory and p-adic Langlands correspondence. In this talk we give a survey of the recent developments of Fleck's congruence and its various extensions, as well as some important applications to Stirling numbers of the second kind and homotopy exponents of special unitary groups given by Davis and the speaker. Both number-theoretic and combinatorial approaches will be introduced.

1. Lucas' and Wolstenholeme's congruences

Let $(x)_0 = 1$ and $(x)_k = x(x-1)\cdots(x-k+1)$ for $k \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.

For $k \in \mathbb{N} = \{0, 1, 2, \ldots\}$, define the binomial coefficient

$$\binom{x}{k} = \frac{(x)_k}{k!}$$

which is an integer if $x\in\mathbb{Z}$. It is easy to see that

$$\binom{-x}{k}=(-1)^k\binom{x+k-1}{k}.$$

A fundamental congruence involving binomial coefficients was given by E. Lucas in 1878.

Theorem 1.1 (Lucas' Theorem)**.** *Let p be a prime, and let $n,r\in\mathbb{N}$ and $s,t\in\{0,\ldots,p-1\}$. Then*

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

In the case $s=t=0$, the Lucas congruence can be further improved.

Theorem 1.2. *Let $p\geqslant 5$ be a prime.*

(i) (Wolstenholeme, 1862) *We have*

$$\binom{2p-1}{p-1}=\frac{1}{2}\binom{2p}{p}\equiv 1\pmod{p^3}.$$

(ii) (Ljunggren, 1952) *For $n,r\in\mathbb{N}$ we have*

$$\binom{pn}{pr}\equiv\binom{n}{r}\pmod{p^3}.$$

(iii) (Jacobsthal, 1952) *If $n\geqslant r\geqslant 0$ then*

$$\binom{np}{rp}\Big/\binom{n}{r}\in 1+p^3nr(n-r)\mathbb{Z}_p,$$

where $\mathbb{Z}_p$ is the ring of p-adic integers in the p-adic field $\mathbb{Q}_p$.

For $n\in\mathbb{N}$ define the q-integer $[n]_q$ by

$$[n]_q=\frac{1-q^n}{1-q}=\sum_{0\leqslant r<n}q^r.$$

For $n, r \in \mathbb{N}$ the Gauss q-binomial coefficient

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \begin{cases} \frac{[n]_q[n-1]_q\cdots[n-r+1]_q}{[r]_q[r-1]_q\cdots[1]_q} & \text{if } n \geqslant r, \\ 0 & \text{otherwise.} \end{cases}$$

is a natural q-analogue of the usual binomial coefficient $\binom{n}{r}$. Note that

$$\lim_{q\to 1} \begin{bmatrix} n \\ r \end{bmatrix}_q = \binom{n}{r}.$$

Both Lucas' theorem and Wolstenholme's congruence have their q-analogues.

2. Fleck's and Weisman's congruences

For $m \in \mathbb{Z}^+$, $n \in \mathbb{N}$ and $r \in \mathbb{Z}$, we set

$$C_m(n, r) = \sum_{k\equiv r \pmod{m}} \binom{n}{k}(-1)^k.$$

For a prime p and a p-adic number α, we let $\mathrm{ord}_p(\alpha)$ denote the *p-adic order* of α.

In 1913 A. Fleck published the following result; we don't know his motivation.

Theorem 2.1 (Fleck, 1913)**.** *Let p be any prime, and let $n \in \mathbb{Z}^+$ and $r \in \mathbb{Z}$. Then*

$$C_p(n, r) \equiv 0 \pmod{p^{\lfloor (n-1)/(p-1)\rfloor}};$$

in other words,

$$\mathrm{ord}_p(C_p(n, r)) \geqslant \left\lfloor \frac{n-1}{p-1} \right\rfloor.$$

Proof. (A. Granville) Let ζ_p be a primitive p-th root of unity. Then

$$\begin{aligned} pC_p(n,r) &= \sum_{k=0}^{n}\binom{n}{k}(-1)^k\sum_{j=0}^{p-1}\zeta_p^{j(k-r)} \\ &= \sum_{j=0}^{p-1}\zeta_p^{-jr}\sum_{k=0}^{n}\binom{n}{k}(-\zeta_p^j)^k = \sum_{j=1}^{p-1}\zeta_p^{-jr}(1-\zeta_p^j)^n \end{aligned}$$

as is well-known. Clearly

$$\prod_{j=1}^{p-1}(1-\zeta_p^j) = \lim_{x\to 1}\frac{x^p-1}{x-1} = p,$$

and each $(1-\zeta_p^j)/(1-\zeta_p)$ with $1\leqslant j\leqslant p-1$ is a unit in the ring $\mathbb{Z}[\zeta_p]$. So $\mathrm{ord}_p(1-\zeta_p^j)=1/(p-1)$ for all $j=1,\ldots,p-1$. Therefore

$$\mathrm{ord}_p(C_p(n,r)) \geqslant \frac{n}{p-1}-1 > \frac{n-1}{p-1}-1$$

and hence $\mathrm{ord}_p(C_p(n,r))\geqslant \lfloor (n-1)/(p-1)\rfloor$. $\square$

For a p-adically continuous function $f(x)$ from $\mathbb{Z}_p$ to the p-adic completion of $\mathbb{Q}_p$, there are two popular ways to expand $f(x)$: One is Mahler's interpolation series $f(x)=\sum_{n=0}^{\infty}a_n\binom{x}{n}$, another is van der Put's expansion $f(x)=\sum_{n=0}^{\infty}b_n\chi_n(x)$ where $\chi_n(x)=[\![\mathrm{ord}_p(x-n)>\log_p\max\{n,1\}]\!]$. (For a proposition P we let $[\![P]\!]$ take 1 or 0 according as P holds or not.) If $0\leqslant n<p^\alpha$ then we have the relation

$$a_n = C_p(n,0)b_0+\sum_{0<\beta\leqslant\alpha}\sum_{p^{\beta-1}\leqslant r<p^\beta}C_{p^\beta}(n,r)b_r.$$

Motivated by this and unaware of Fleck's earlier result, C. S. Weisman [Michigan Math. J. 24(1977)] obtained the following result.

Theorem 2.2 (Weisman, 1977). *Let p be any prime, and let $a \in \mathbb{Z}^+$, $n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then*

$$\mathrm{ord}_p(C_{p^a}(n,r)) \geqslant \left\lfloor \frac{n-p^{a-1}}{\varphi(p^a)} \right\rfloor.$$

If $n - p^{a-1} = m\varphi(p^a) - 1$ for some $m \in \mathbb{Z}^+$, then

$$C_{p^a}(n,r) \equiv (-p)^{m-1} \pmod{p^m}.$$

The first part of Theorem 2.2 is a generalization of Fleck's result; Weisman's proof is very complicated. Quite recently Z.W. Sun and D. Wan were able to give a proof via roots of unity on the basis of the identity

$$C_{p^a}(n,r) = \frac{1}{p}\sum_{k=0}^{n}\binom{n}{k} C_{p^{a-1}}(k,r)\sum_{j=0}^{p-1}\zeta_{p^a}^{j(k-r)}(1-\zeta_{p^a}^{j})^{n-k},$$

where ζ_{p^a} is a primitive p^a-th root of unity in the complex field $\mathbb{C}$.

3. On Fleck quotients and generalized Fleck quotients

Let p be a prime, and let $n \in \mathbb{N}$ and $r \in \mathbb{Z}$. We define the *Fleck quotient*

$$F_p(n,r) := (-p)^{-\lfloor (n-1)/(p-1)\rfloor} C_p(n,r) + [\![n=0]\!].$$

If $a \in \mathbb{Z}^+$ then we define the *generalized Fleck quotient* (or Weisman quotient)

$$F_{p^a}(n,r) = (-p)^{-\lfloor (n-p^{a-1})/\varphi(p^a)\rfloor} C_{p^a}(n,r) + [\![n < p^{a-1}]\!].$$

For $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$ we let $\{a\}_m$ be the least nonnegative residue of a mod m. (Thus $\{a\}_m/m$ is the fractional part $\{a/m\}$ of a/m.)

Theorem 3.1 (Z. W. Sun and D. Wan, 2006, `arxiv:math.NT/0603462`). *Let p be a prime, and let $a\in\mathbb{Z}^+$ and $n\in\mathbb{N}$.*

(i) *$F_{p^a}(n,r)\not\equiv 0\pmod p$ for some $r\in\mathbb{Z}$.*

(ii) *For all $r\in\mathbb{Z}$, we have*

$$F_p(n+p^a(p-1),r)\equiv F_p(n,r)\pmod{p^a},$$

and

$$F_{p^a}(n+p^a(p-1),r)\equiv F_{p^a}(n,r)\pmod p$$

if $n\geqslant 2p^{a-1}$.

(iii) *For any $r\in\mathbb{Z}$ we have*

$$F_{p^a}(n,r)\equiv\sum_{k=0}^{d}\binom{r+k-1}{k}F_{p^a}(n+k,0)\pmod p,$$

where $d=\{p^{a-1}-1-n\}_{\varphi(p^a)}$ is the least nonnegative integer with $n+d\equiv p^{a-1}-1\pmod{\varphi(p^a)}$.

In view of the Kummer-type congruences in Theorem 3.1(ii), the following conjecture looks reasonable.

Conjecture 3.1 (Z. W. Sun and D. Wan, 2006). *Let p be a prime, and let $a,b,n\in\mathbb{Z}^+$ and $r\in\mathbb{Z}$. If $n\geqslant 2p^{a+b-2}$, then*

$$F_{p^a}\left(n+\varphi(p^{a+b}),r\right)\equiv F_{p^a}(n,r)\pmod{p^b}.$$

For a prime p and an integer a, we define $q_p(a)=(a^{p-1}-1)/p$ which is called a *Fermat quotient* when $a\not\equiv 0\pmod p$.

By a number-theoretic method involving roots of unity, Gauss sums and the Stickelberger congruence, Z. W. Sun and D. Wan recently determined $F_p(n,r)$ modulo p explicitly.

Theorem 3.2 (Z. W. Sun and D. Wan, `arXiv:math.NT/0603462`)**.** *Let p be a prime, and let $n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Set $n_0 = \{n\}_p$ and $n_1 = \{n_0 - n\}_{p-1} = \{-\lfloor n/p \rfloor\}_{p-1}$. If $n_0 \leqslant n_1$, then*

$$F_p(n,r) \equiv \frac{(-1)^{n_1}}{n_1!}\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{n_1} \pmod p.$$

If $n_0 > n_1 = 0$, then

$$F_p(n,r) \equiv (-1)^{\{r\}_p}\binom{n_0}{\{r\}_p} \pmod p.$$

If $n_0 > n_1 > 0$, then

$$F_p(n,r) \equiv \frac{(-1)^{n_1-1}}{(n_1-1)!}\sum_{k=0}^{n_0}\binom{n_0}{k}(-1)^k(k-r)^{n_1}q_p(k-r) \pmod p.$$

Let p be an odd prime. For each $a \in \mathbb{Z}$ let $\bar{a} = a + p\mathbb{Z} \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let ω be the Teichmüller character of the multiplicative group $F_p^* = F_p \setminus \{\bar{0}\}$. For $a \in \mathbb{F}_p^*$, $\omega(\bar{a})$ is just the $(p-1)$-th root of unity in the unique unramified extension of the p-adic field $\mathbb{Q}_p$ such that $\omega(\bar{a}) \equiv a \pmod p$. If ζ_p is a primitive p-th root of unity in the algebraic closure of $\mathbb{Q}_p$, then for $n \in \mathbb{N}$ and $\pi = 1 - \zeta_p$ we have

$$\sum_{a=1}^{p-1} a^n\zeta_p^a \equiv \sum_{a=1}^{p-1}\omega^n(\bar{a})\zeta_p^a \equiv -\frac{(-\pi)^{n^*}}{n^*!} \pmod{\pi^{n^*+1}}$$

by Stickelberger's congruence for Gauss' sums, where $n^* = \{-n\}_{p-1}$. Moreover, we have the following lemma which plays a key role in the proof of Theorem 3.2.

Lemma 3.1. *Let p be a prime, and let $n\in\mathbb{N}$ and $n^*=\{-n\}_{p-1}$. Define $G(n)=\sum_{a=1}^{p-1}a^n\zeta_p^a$ and $\pi=1-\zeta_p$, where ζ_p is a primitive p-th root of unity in the complex field $\mathbb{C}$. Then*

$$G(n)\equiv(-1)^{n^*-1}\sum_{m=n^*}^{p-2}s(m,n^*)\frac{\pi^m}{m!}\pmod p,$$

where $s(m,0),\ldots,s(m,m)$ are Stirling numbers of the first kind defined by $(x)_m=\sum_{k=0}^m(-1)^{m-k}s(m,k)x^k$.

Here is a consequence of Theorem 3.2.

Corollary 3.1. *Let p be a prime and let $n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Then*

$$F_p(pn,r)\equiv\frac{r^{n^*}}{n^*!}\pmod p$$

where $n^*=\{-n\}_{p-1}$. Consequently,

$$F_p\left(p\frac{p-1}{2},r\right)\equiv\begin{cases}(-1)^{(h(-p)+1)/2}(\frac{r}{p})\pmod p & \text{if } p\neq 3\ \&\ 4\mid p+1,\\ (-1)^{(h(p)-1)/2}(\frac{r}{p})\frac{v}{2}\pmod p & \text{if } 4\mid p-1,\end{cases}$$

where $(\frac{\cdot}{p})$ is the Legendre symbol, and $h(-p)$ and $h(p)$ are the class numbers of the quadratic fields $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Q}(\sqrt{p})$ respectively, and for $p\equiv 1\pmod 4$ we write the fundamental unit of $\mathbb{Q}(\sqrt{p})$ in the form $(v+u\sqrt{p})/2$ with $u,v\in\mathbb{Z}$ and $u\equiv v\pmod 2$.

Let n be a positive integer and $p>2n+1$ be a prime. By the first part of Corollary 3.1 in the case $r=0$, we have

$$\binom{2pn-1}{pn-1}=\frac{1}{2}\binom{2pn}{pn}\equiv\sum_{k=0}^{n-1}(-1)^{n-1-k}\binom{2pn}{pk}\pmod{p^{2n+1}}.$$

This is a new extension of Wolstenholme's congruence; in the case $n = 2$ it gives

$$\binom{4p-1}{2p-1} \equiv \binom{4p}{p} - 1 \pmod{p^5}.$$

Z. W. Sun and D. Wan also presented a combinatorial approach to Fleck quotients. The following lemma provides a basis for induction arguments.

Lemma 3.2. *Let p be a prime, and let $n \in \mathbb{N}$ with $n \geqslant p$. Then*

$$F_p(n,r) \equiv -\sum_{j=1}^{p-1} \frac{1}{j} \sum_{i=0}^{j-1} F_p(n-p+1, r-i) \pmod{p}.$$

For $n \in \mathbb{N}$ the Stirling numbers $S(n,k)$ $(k \in \mathbb{N})$ of the second kind are given by

$$x^n = \sum_{k \in \mathbb{N}} S(n,k)(x)_k.$$

It is well known that

$$\sum_{n=k}^{\infty} S(n,k) \frac{x^n}{n!} = \frac{(e^x-1)^k}{k!};$$

in other words,

$$(e^x-1)^k = \sum_{n=k}^{\infty} \bar{S}(n,k) x^n \quad \text{where } \bar{S}(n,k) = \frac{k!}{n!} S(n,k).$$

For $m = 1, 2, \ldots$, the m-th order Bernoulli polynomials $B_n^{(m)}(t)$ $(n \in \mathbb{N})$ are defined by

$$\frac{x^m e^{tx}}{(e^x-1)^m} = \sum_{n=0}^{\infty} B_n^{(m)}(t) \frac{x^n}{n!},$$

and those $B_n^{(m)} = B_n^{(m)}(0)$ are called higher-order Bernoulli numbers. The usual Bernoulli polynomials and numbers are $B_n(t) = B_n^{(1)}(t)$ and $B_n = B_n(0) = B_n^{(1)}$ respectively.

By Lemma 3.2, Sun and Wan showed that if p is a prime, $n\in\mathbb{N}$, $r\in\mathbb{Z}$ and $m\equiv n\pmod p$ then

$$(-1)^nF_p(n,r)\equiv[x^{n^*}]\left(\frac{e^x-1}{x}\right)^m e^{-rx}\pmod p,$$

where $n^*=\{-n\}_{p-1}$ and $[x^{n^*}]f(x)$ denotes the coefficient of x^{n^*} in the power series expansion of $f(x)$. This yields the following result.

Theorem 3.3 (Z. W. Sun and D. Wan, `arXiv:math.NT/0603462`)**.** *Let p be a prime, and let $n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Set $n^*=\{-n\}_{p-1}$. For any integer $m\equiv n\pmod p$, if $m\geqslant 0$ then $(-1)^nF_p(n,r)$ is congruent to*

$$\begin{aligned}\sum_{k=0}^{n^*}\bar{S}(n^*-k+m,m)\frac{(-r)^k}{k!}&=\sum_{k=0}^{n^*}\bar{S}(m+n^*,m+k)\binom{-r}{k}\\&=\sum_{k=0}^{m}\binom{m}{k}(-1)^{m-k}\frac{(k-r)^{m+n^*}}{(m+n^*)!}\end{aligned}$$

modulo p; if $m<0$ then we have

$$F_p(n,r)\equiv\frac{(-1)^{n^*}}{n^*!}B_{n^*}^{(-m)}(-r)\equiv-(p-1-n^*)!B_{n^*}^{(-m)}(-r)\pmod p.$$

Let p be an odd prime, and let h_p and h_p^+ denote the class numbers of the cyclotomic field $\mathbb{Q}(\zeta_p)$ and its maximal real subfields $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ respectively, where ζ_p is a primitive p-th root of unity in the complex field $\mathbb{C}$. It is well known that $h_p^-=h_p/h_p^+$ is an integer. If p divides none of the numerators of the Bernoulli numbers $B_0,B_2,\ldots,B_{p-3}\in\mathbb{Z}_p$, then p is said to be a *regular* prime. In 1850 E. Kummer proved that

$$\begin{aligned}p\nmid h_p&\iff p\nmid h_p^-\iff p\text{ is regular}\\&\Longrightarrow x^p+y^p=z^p\text{ has no integral solution with }xyz\neq 0.\end{aligned}$$

Theorem 3.3 has the following interesting consequence.

Corollary 3.2 (Z. W. Sun and D. Wan, `arXiv:math.NT/0603462`). *Let p be a prime.*

(i) *For every $n = 2, \ldots, p$ we have*

$$\sum_{k=1}^{n}(-1)^{pk-1}\binom{pn-1}{pk-1} \equiv (n-1)!B_{p-n}p^n \pmod{p^{n+1}}.$$

(ii) *If $3 \leqslant n \leqslant p$ and $r \in \mathbb{Z}$ then*

$$F_p(pn-2, r) \equiv -n!\left(\frac{B_{p-n+1}(-r)}{n-1} + (r+1)\frac{B_{p-n}(-r)}{n}\right) \pmod{p}.$$

Note that Corollary 3.2(i) in the case $n = 2$ gives the Wolstenholme congruence.

4. Polynomial extensions of Fleck's and Weisman's results

Let p be a prime, and let $A = \mathbb{Z}_p[\![T]\!]$ be the formal power series ring over $\mathbb{Z}_p$. The $\mathbb{Z}_p$-linear Frobenius map ϕ acts on the ring A by

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

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

$$\psi\left(\sum_{i=0}^{p-1}(1+T)^i\phi(x_i)\right) = x_0,$$

where $x_0, \ldots, x_{p-1} \in A$. The ψ-operator plays a basic role in L-functions of F-crystals, Fontaine's theory of (ϕ, Γ)-modules, Iwasawa theory, p-adic

L-functions and p-adic Langlands correspondence. Both P. Colmez and D. Wan noted that if $n\in\mathbb{N}$ and $r\in\mathbb{Z}$ then

$$\begin{aligned}\psi\left(\frac{T^n}{(1+T)^r}\right)=&\psi\bigg(\sum_{k=0}^n\binom{n}{k}(-1)^{n-k}(1+T)^{k-r})\bigg)\\=&\sum_{k=0}^n\binom{n}{k}(-1)^{n-k}\psi((1+T)^{k-r})\\=&\sum_{k\equiv r\ (\mathrm{mod}\ p)}\binom{n}{k}(-1)^{n-k}(1+T)^{(k-r)/p}\\=&\sum_{k\equiv r\ (\mathrm{mod}\ p)}\binom{n}{k}(-1)^k\sum_{l\in\mathbb{N}}\binom{(k-r)/p}{l}T^l=\sum_{l=0}^\infty T^lC_{l,p}(n,r),\end{aligned}$$

where we let

$$C_{l,m}(n,r)=\sum_{k\equiv r\ (\mathrm{mod}\ m)}\binom{n}{k}(-1)^k\binom{(k-r)/m}{l}.$$

This led Colmez (2004) and Wan (2005) to study the p-adic order of $C_{l,p}(n,r)$. Colmez did not know Fleck's congruence and just presented a weaker estimate $\mathrm{ord}_p(C_{l,p}(n,0))\geqslant\lfloor n/p\rfloor-l$. In May 2005, the speaker came to Univ. of California at Irvine and told Fleck's result to Wan who was studying the ψ-operator then, soon Wan got that if p is a prime, $l,n\in\mathbb{N}$ and $r\in\mathbb{Z}$ then

$$\mathrm{ord}_p(C_{l,p}(n,r))\geqslant\left\lfloor\frac{n-lp-1}{p-1}\right\rfloor,$$

Note that in the case $l=0$ this reduces to Fleck's result.

In June 2005, by a combinatorial argument the speaker was able to give a common generalization of Weisman's and Wan's extensions of Fleck's congruence.

Theorem 4.1 [Z. W. Sun, Acta Arith. 122(2006)]. *Let p be a prime, and let $l,\alpha,\beta\in\mathbb{N}$ and $\alpha\geqslant\beta$. Then we have*

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

for all integers $n\geqslant p^{\alpha-1}$ and r; moreover, we can substitute $[\![\beta=0]\!]$ for the first l in the exponent if α is greater than one.

In the case $\alpha=\beta=a>1$, Theorem 3.1 gives

$$\mathrm{ord}_p(C_{l,p^a}(n,r))\geqslant\left\lfloor\frac{n-p^{a-1}}{\varphi(p^a)}\right\rfloor-la,$$

which implies that

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

for any $m\equiv-1\pmod p$. This is also true for $a=1$ as pointed out by Fleck.

For a positive integer a, let ψ^a be the a-th iteration of ψ acting on the ring $A=\mathbb{Z}_p[\![T]\!]$. D. Wan noted that for any $n\in\mathbb{N}$ and $r\in\mathbb{Z}$ we have

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

To understand the ψ^a-action, it is thus essential to understand the p-adic property of the cyclotomic ψ-coefficients $C_{l,p^a}(n,r)$ $(l=0,1,\ldots)$.

Theorem 4.2 (D. Wan, Finite Fields Appl., in press). *Let p be a prime, and let $a,l,n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Then*

$$\mathrm{ord}_p(C_{l,p^a}(n,r))\geqslant\left\lfloor\frac{n-lp^a-p^{a-1}}{\varphi(p^a)}\right\rfloor.$$

To understand how sharp the congruence in Theorem 4.2 is, we define the *normalized cyclotomic ψ-coefficient*

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

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

In 2005 Sun and Wan proved the following new analogue of Lucas' theorem.

Theorem 4.3 (Sun and Wan, `arxiv:math.NT/0512012`)**.** *Let p be any prime, and let $r\in\mathbb{Z}$ and $a,l,n,s,t\in\mathbb{N}$ with $a\geqslant 2$ and $s,t<p$. Then we have the congruence*

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

in other words,

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

This theorem in the case $l=0$ was first obtained by Z. W. Sun and D. M. Davis [Trans. Amer. Math. Soc., `arXiv:math.NT/0508087`].

Note that $a\geqslant 2$ is assumed in Theorem 4.3. The case $a=1$ is more subtle.

Theorem 4.4 (Sun and Wan, `arxiv:math.NT/0512012`). *Let p be a prime, $l,n\in\mathbb{N}$, $r\in\mathbb{Z}$ and $s,t\in\{0,\ldots,p-1\}$. If $p\mid n$, or $p-1\nmid n-l-1$, or $s=2t$ and $p\neq 2$, then*

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

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

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

5. Further results related to Stirling numbers of the second kind and homotopy exponents of SU(n)

Let p be a prime. If $n\in\mathbb{Z}^+$ then

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

and hence $\mathrm{ord}_p(n!)\leqslant(n-1)/(p-1)$. Thus, when $a\in\mathbb{Z}^+$, $n\geqslant p^{a-1}$ and $r\in\mathbb{Z}$, by Weisman's result we have

$$\mathrm{ord}_p(C_{p^a}(n,r))\geqslant\left\lfloor\frac{n-p^{a-1}}{\varphi(p^a)}\right\rfloor=\left\lfloor\frac{\lfloor n/p^{a-1}\rfloor-1}{p-1}\right\rfloor\geqslant\mathrm{ord}_p\Big(\Big\lfloor\frac{n}{p^{a-1}}\Big\rfloor!\Big).$$

For a topological purpose, few years ago a topologist D. M. Davis conjectured that if $n>l\geqslant 0$ are integers then

$$\mathrm{ord}_2\left(\sum_{k\in\mathbb{N}}\binom{n}{2k}k^l\right)\geq\mathrm{ord}_2\left(\left\lfloor\frac{l+1}{2}\right\rfloor!\right).$$

This and his other related conjectures are indeed very sophisticated! In July 2005 he made his conjectures public and wrote to the speaker the following comments:

"**I have worked very hard off and on during the past two years trying to prove these conjectures. In the past, I have communicated them privately to others (at least 5 experts) without any significant progress.**"

Two weeks later the above conjecture was confirmed by the speaker, and the following general theorem was soon established.

Theorem 5.1 [Davis and Sun, `arXiv:math.AT/0508083`]. *Let p be a prime, $a,n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Then, for any polynomial $f(x)\in\mathbb{Z}[x]$, we have*

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

where $\tau_p(s,t)=\mathrm{ord}_p\binom{s+t}{s}$ is the number of carries occurring in the addition of s and t in base p.

For $k,n\in\mathbb{N}$ it is known that

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

Theorem 5.1 in the case $r=0$ has the following consequence on p-adic orders of Stirling numbers of the second kind.

Corollary 5.1 [Davis and Sun, `arXiv:math.AT/0508083`]. *Let p be any prime and n be a positive integer. If $L\geqslant n-1+\lfloor n/(p(p-1))\rfloor$, then for all $m\geqslant n$ we have*

$$\mathrm{ord}_p\left(m!S((p-1)p^L+n-1,m)\right)\geqslant n-1+\mathrm{ord}_p\bigg(\left\lfloor\frac{n}{p}\right\rfloor!\bigg).$$

The *special unitary group* $\mathrm{SU}(n)$ (of degree n) is the space of all $n\times n$ unitary matrices (the conjugate transpose of such a complex matrix equals its inverse) with determinant one. It plays important roles in many areas of mathematics and physics.

Here is an application of Corollary 5.1 in algebraic topology.

Theorem 5.2 [Davis and Sun, `arXiv:math.AT/0508083`]. *For any prime p and $n\geqslant 2$, some homotopy group $\pi_i(\mathrm{SU}(n))$ contains an element of order $p^{n-1+\mathrm{ord}_p(\lfloor n/p\rfloor!)}$.*

Numerical examples indicate that Theorem 5.2 is very strong.

The inequality in Theorem 5.1 can be improved when $\deg f<\lfloor n/p^a\rfloor$.

Theorem 5.3 [Sun and Davis, Trans. AMS, `arXiv:math.NT/0508087`]. *Let p be a prime, and let $a,n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Then, for any polynomial $f(x)\in\mathbb{Z}[x]$, we have*

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

where $\{x\}_{p^{a-1}}$ is regarded as 0 if $a=0$.

A particular case of this theorem is the following conjecture of Davis: For $l,n\in\mathbb{N}$ we have

$$\mathrm{ord}_2\bigg(\sum_{k\in\mathbb{N}}\binom{n}{4k+2}\binom{k}{l}\bigg)\geq\mathrm{ord}_2\left(\left\lfloor\frac{n}{2}\right\rfloor!\right)-l-\mathrm{ord}_2(l!).$$

The following result is a vast generalization of Lucas' theorem.

Theorem 5.4. *Let p be any prime. And and let $l,n\in\mathbb{N}$, $r,s,t\in\mathbb{Z}$ and $0\leqslant s,t<p$.*

(i) [Sun and Davis, Trans. AMS, `arXiv:math.NT/0508087`] *For every $a=2,3,\ldots$, we have*

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

(ii) [Sun and Wan, `arXiv:math.NT/0512012`] *The congruence in the first part also holds for $a=1$ as conjectured by Sun and Davis.*

When $a>\log_p(\max\{n,p\})$ and $l=0$, Theorem 5.4(i) yields the classical congruence of Lucas.

Theorem 5.5 (Z. W. Sun, `arXiv:math.NT/0512071`)**.** *Let p be any prime, and let $a\in\mathbb{Z}^+$, $l,n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Then*

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

where

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

Let p be a prime, $a,n\in\mathbb{N}$ and $r\in\mathbb{Z}$. When $p^a>n$ and $l=0\leqslant r\leqslant n$, the congruence in Theorem 5.5 reduces to Ljunggren's congruence $\binom{pn}{pr}\equiv$

$\binom{n}{r} \pmod{p^{\alpha_p}}$. Note also that the congruence holds for every $l \in \mathbb{N}$ if and only if we have

$$\binom{pn}{pr}_{f,\,p^{a+1}} \equiv \binom{n}{r}_{f,\,p^a} \pmod{p^{\alpha_p}}$$

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

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

The following theorem shows that the inequality in Theorem 5.1 is sharp for infinitely many values of l provided that $n \geqslant 2p^a - 1$.

Theorem 5.6 (Z. W. Sun, `arXiv:math.NT/0512071`). *Let p be a prime, and let $a, l, n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Set $r_* = \{r\}_{p^a}$, $n_* = r_* + \{n-r\}_{p^a}$ and*

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

Suppose that $l \geqslant m > 0$ and

$$l \equiv m \ \left(\mathrm{mod}\ (p-1)p^{\lfloor \log_p m\rfloor - [\![\lfloor r/p^\alpha\rfloor \in p\mathbb{Z}\ \&\ \log_p m\in\mathbb{Z}^+]\!]}\right).$$

Then we have

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

In particular,

$$\frac{1}{\lfloor n/p^a\rfloor!} \sum_{k\equiv 0\,(\mathrm{mod}\ p^a)} (-1)^k \binom{n}{k} \left(-\frac{k}{p^a}\right)^{\lfloor n/p^a\rfloor} \equiv 1 \pmod{p}.$$

The following result follows from Theorem 5.3.

Theorem 5.7 (Z. W. Sun, arXiv:math.NT/0512071). *Let p be any prime. Let $a\in\mathbb{Z}$, $l,l',m\in\mathbb{Z}^+$, $l'\geqslant l>m/p$ and*

$$l'\equiv l\ \left(\mathrm{mod}\ (p-1)p^{\lfloor\log_p m\rfloor-[\![p|a\ \&\ \log_p m\in\mathbb{Z}^+]\!]}\right).$$

Then we have

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

Corollary 5.2 (L. Carlitz, 1955). *Let p be any prime. Suppose that $a,m\in\mathbb{N}$, $m\geqslant p$ and $p^a<m\leqslant p^{a+1}$. Then $p^a(p-1)$ is a period of the sequence $\{S(l,m)\}_{l\geqslant m}$ modulo p.*

In 1899 J.W.L. Glaisher proved that

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

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

Corollary 5.3. *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

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

A different extension of the Glaisher congruence was given by the speaker and R. Tauraso [arXiv:math.NT/0502187] in Feb. 2005.