A talk given on the Integers Conference (West Georgia Univ., Oct. 28, 2005).

SOME CONGRUENCES MOTIVATED BY ALGEBRAIC TOPOLOGY

Zhi-Wei Sun

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

Dedicated to Prof. R. L. Graham for his 70th birthday

Abstract. In July 2005, D. M. Davis posted several original number-theoretic conjectures arising from his investigation of homotopy exponents of the special unitary group $\mathrm{SU}(n)$. The recent study of these conjectures and their generalizations by the author and Davis led to a strong lower bound for the homotopy p-exponent of $\mathrm{SU}(n)$, as well as a number of new combinatorial congruences some of which extend vastly some classical congruences (such as Lucas' theorem) concerning binomial coefficients. We talk about these results and propose some further conjectures.

1. Davis' conjectures arising from algebraic topology

Let $\mathbb{N}=\{0,1,2,\ldots\}$. For a prime p and an integer m, we call

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

the *p-adic order* of m (or the order of m at prime p).

On July 8, 2005, Prof. Donald M. Davis (a topologist from Lehigh University) posted a message to `Number Theory Listserver and Archives` containing several conjectures arising from his study of algebraic topology. Here are three main conjectures of Davis:

Conjecture D1. *Let $m, n \in \mathbb{N}$ and $m \geqslant n$. If $L \in \mathbb{N}$ is sufficiently large (e.g. $L > 3n/2$), then*

$$\mathrm{ord}_2(m!S(2^L+n-1,m)) \geq n-1+\mathrm{ord}_2\left(\left\lfloor\frac{n}{2}\right\rfloor!\right),$$

where the Stirling number $S(k,m)$ of the second kind is defined as the number of partitions of a set of cardinality k into m nonempty subsets.

Conjecture D2. *If $n > l \geqslant 0$ are integers, then*

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

Conjecture D3. *For $l, n \in \mathbb{N}$ we have*

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

Davis noted that D3 $\Rightarrow$ D2 $\Rightarrow$ D1. After posting the message publicly, Davis wrote me the following:

"**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.**"

Then, in July and August I worked very hard on Davis' conjectures. Later Davis and I wrote two joint papers:

1. D. M. Davis and Z. W. Sun, *A number-theoretic approach to homotopy exponents of* SU(n), submitted, `arXiv:math.AT/0508083`.

2. Z. W. Sun and D. M. Davis, *Combinatorial congruences modulo prime powers*, submitted, `arXiv:math.NT/0508087`.

2. The mains results of Davis and Sun

Theorem 1 [Davis and Sun, `arXiv:math.AT/0508083`]. *Let p be a prime, $\alpha, n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then, for any polynomial $f(x) \in \mathbb{Z}[x]$, we have*

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

where $\{a\}_{p^\alpha}$ is the least nonnegative residue of a modulo p^α, and $\tau_p(a,b)=\operatorname{ord}_p\binom{a+b}{a}$ is the number of carries occurring in the addition of a and b in base p.

Theorem 1 in the case $p=2$, $\alpha=1$ and $r=0$ implies Conj. D2.

Theorem 1 in the case $r=0$ has the following consequence on p-adic orders of Stirling numbers of the second kind.

Corollary 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*

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

When $p=2$, Corollary 1 yields Conj. D1.

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 1 in algebraic topology.

Theorem 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 2 is very strong.

Theorem 3 [Sun and Davis, `arXiv:math.NT/0508087`]. *Let p be a prime, and let $\alpha,n\in\mathbb{N}$ and $r\in\mathbb{Z}$. Then, for any polynomial $f(x)\in\mathbb{Z}[x]$, we have*

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

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

Clearly Theorem 3 in the case $p=\alpha=r=2$ and $f(x)=l!\binom{x}{l}$ implies Conj. D3.

The following lemma (obtained by means of roots of unity) plays an important role in our proofs of Theorems 1 and 3.

Lemma 1 [Sun and Davis, `arXiv:math.NT/0508087`]. *Let $d,m\in\mathbb{Z}^+=\{1,2,\ldots\}$, $n\in\mathbb{N}$ and $r\in\mathbb{Z}$, and let $f(x)$ be a function from $\mathbb{Z}$ to the complex field. Then we have*

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

where

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

A famous theorem of E. Lucas states that if p is a prime, and $n, r, s, t \in \mathbb{N}$ and $s, t < p$ then

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

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

Theorem 4 [Sun and Davis, `arXiv:math.NT/0508087`]**.** *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*

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

When $\alpha > \log_p(\max\{n, p\})$ and $l = 0$, Theorem 4 yields the classical congruence of Lucas.

Conjecture 1 [Sun and Davis, `arXiv:math.NT/0508087`]**.** *Theorem 4 also holds with $\alpha = 1$. When $s = t = 0$, the congruence in Theorem 4 even holds modulo p^3 with $p > 3$, and modulo p^2 with $p = 3$.*

3. Some related results of another type

Theorem 5. *Let p be a prime, and let $\alpha, n \in \mathbb{N}$ and $r \in \mathbb{Z}$.*

(i) (A. Fleck, 1913) *We have*

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

(ii) (C. S. Weisman, 1977; motivated by p-adic continuation) *Let φ be the Euler totient function. Then*

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

(iii) (D. Wan, May 2005; motivated by Fontaine's rings) *For $l\in\mathbb{N}$ we have*

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

(iv) (Z. W. Sun, June-July 2005, `arXiv:math.NT/0507008`; combinatorial arguments) *For $l\in\mathbb{N}$ we have*

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

If $\alpha>1$, then

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

(v) (D. Wan, August 2005, `arXiv:math.NT/0508159`; motivated by Iwasawa theory) *For $l\in\mathbb{N}$ we have*

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