A talk given at the 6th Int. Confer. of Combin. (Shanghai, May 28, 2008)

RECENT PROBLEMS AND RESULTS INVOLVING BINOMIAL COEFFICIENTS

Zhi-Wei Sun

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

Abstract. In this talk we will introduce some recent problems and results on representations or congruences involving binomial coefficients. In particular, the talk includes some conjectures and results on representations of integers involving triangular numbers $T_x=\binom{x+1}{2}$, some deep congruences for sums of Catalan numbers, and various lower bounds for p-adic orders of certain sums involving binomial coefficients. A useful lemma of R. M. Wilson and its extension will be also introduced.

1. Representations of integers involving triangular numbers

As $1+2+\cdots+n=n(n+1)/2$, those

$$T_x=\binom{x+1}{2}=\frac{x(x+1)}{2}\quad (x\in\mathbb{Z})$$

are called *triangular numbers*. Clearly

$$T_{-x}=T_{x-1}\quad\text{and}\quad 8T_x+1=(2x+1)^2.$$

Let $n\in\mathbb{N}=\{0,1,2,\ldots\}$. Then

(i) (Lagrange's theorem) $n=w^2+x^2+y^2+z^2$ for some $w,x,y,z\in\mathbb{Z}$.

(ii) (Gauss-Legendre Theorem) $n=x^2+y^2+z^2$ for some $x,y,z\in\mathbb{Z}$ if and only if n is not of the form $4^k(8l+7)$ with $k,l\in\mathbb{N}$.

(iii) (Fermat) $n=T_x+T_y+T_z$ for some $x,y,z\in\mathbb{Z}$, equivalently $8n+3$ is a sum of three squares of (odd) integers.

(iv) (Euler) $n=x^2+y^2+T_z$ for some $x,y,z\in\mathbb{Z}$. In fact, $8n+1=(2x)^2+(2y)^2+(2z+1)^2$ for some $x,y,z\in\mathbb{Z}$ with $x\equiv y\pmod 2$; this yields the representation

$$n=\frac{x^2+y^2}{2}+t_z=\left(\frac{x+y}{2}\right)^2+\left(\frac{x-y}{2}\right)^2+T_z$$

(v) (E. Lionnet, V. A. Lebesgue and M. S. Réalis, 1872) $n=x^2+T_y+T_z$ for some $x,y,z\in\mathbb{Z}$.

(vi) (B. W. Jones and G. Pall [Acta Math., 1939]) We can write $8n+1$ in the form $8x^2+32y^2+z^2$ with $x,y,z\in\mathbb{Z}$, i.e., n is a sum of a square, an *even* square and a triangular number.

(vii) (Z. W. Sun [Acta Arith., 2007]) n is a sum of an *even* square and two triangular numbers. If $n\neq 2T_m$ for any $m\in\mathbb{N}$, then n is also a sum of an odd square and two triangular numbers.

(viii) (Z. W. Sun [Acta Arith., 2007]) If n is not a triangular number, then it is a sum of an *odd* square, an *even* square and a triangular number

(ix) (B.-K. Oh and Z. W. Sun, `arxiv:0804.3750`) Suppose $n\in\mathbb{Z}^+=\{1,2,3,\ldots\}$. Then n is a sum of a square, an *odd* square and a triangular number. n cannot be written as a sum of an odd square and two triangular numbers if and only if it is of the form $2T_m$ ($m\in\mathbb{Z}^+$) with $2m+1$ having no prime divisor congruent to 3 mod 4.

(x) (B.-K. Oh and Z. W. Sun, `arxiv:0804.3750`) $p=2n+1$ is a prime congruent to 3 modulo 4 if and only if T_n cannot be expressed as a sum of two odd squares and a triangular number, i.e., $p^2=x^2+8(y^2+z^2)$ for no odd integers x,y,z.

A Conjecture of Z. W. Sun [Acta Arith. 2007]**.** *Every $n\in\mathbb{N}$ can be written in the form $x^2+2y^2+3T_z$ (with $x,y,z\in\mathbb{Z}$) except $n=23$, in the form $x^2+5y^2+2T_z$ (or the equivalent form $5x^2+T_y+T_z$) except $n=19$, in the form $x^2+6y^2+T_z$ except $n=47$, and in the form $2x^2+4y^2+T_z$ except $n=20$.*

The speaker has verified the conjecture for $n\leqslant 10,000$.

A Result of B. Kane (2008)**.** *The above conjecture holds under the generalized Riemann hypothesis. Without GRH, sufficiently large integers can be written in any of the forms $x^2+2y^2+3T_z$, $x^2+5y^2+2T_z$, $5x^2+T_y+T_z$, $x^2+6y^2+T_z$, $2x^2+4y^2+T_z$.*

Kane's proof involves many deep tools such as modular forms, class numbers and L-functions.

In a forthcoming joint paper, B. Kane and Z. W. Sun essentially determine those positive integers m such that the form $mT_x+T_y+T_z$ (resp., $x^2+my^2+T_z$, $x^2+mT_y+T_z$, $mx^2+2T_y+T_z$, $mT_x+2T_y+T_z$, $mx^2+2y^2+2T_z$, $mT_x+2T_y+2T_z$) with $x,y,z\in\mathbb{Z}$ represents sufficiently large integers. For

example,

$$\begin{aligned} &x^2+my^2+T_z \text{ represents sufficiently large integers}\\ \iff &mx^2+2T_y+T_z \text{ represents sufficiently large integers}\\ \iff &\text{all odd prime divisors of } m \text{ are congruent to 1 or 3 mod 8}\end{aligned}$$

and

$$\begin{aligned} &mT_x+2T_y+2T_z \text{ represents sufficiently large integers}\\ \iff &mT_x+2y^2+4T_z \text{ represents sufficiently large integers}\\ \iff &\text{all prime divisors of } m \text{ are congruent to 1 mod 4.}\end{aligned}$$

Prime numbers play a key role in number theory. By the prime number theorem, for $x \geqslant 2$ the number $\pi(x)$ of primes not exceeding x is approximately $x/\log x$ (in fact, $\lim_{x\to\infty}\pi(x)/(x/\log x)=1$).

Vinogradov's Theorem. *Every sufficiently large odd integer can be written as a sum of three primes.*

The following result of Linnik (1960) is also remarkable: Any sufficiently large integer can be written as a sum of a prime and two squares of integers.

Goldbach's Conjecture. *Any even number greater than 2 can be expressed as a sum of two primes.*

Now we are in the 21st century, *not* the time of Fermat or Goldbach. It seems quite difficult to formulate a new and simple conjecture concerning representations involving primes. Nevertheless, recently I got some new observations in this field.

Conjecture 1.1 (Z. W. Sun, March 2008)**.**

(i) **Each natural number** $n \neq 216$ **can be written in the form** $p + T_x$**, where** p **is zero or a prime.**

(ii) *In general, for any* $a, b \in \mathbb{N}$ *and odd integer* r*, all sufficiently large integers can be written in the form* $2^a p + T_x$ *with* $x \in \mathbb{Z}$*, where* p *is either zero or a prime congruent to* r *mod* 2^b*.*

Concerning the particular case $a = 0$ and $b = 2$ of Conjecture 1.1(ii), we have a more concrete conjecture: *For* $r = 1, 3$*, any natural number* $n > 10^5$ *can be written in the form* $p + T_x$ *with* $x \in \mathbb{Z}$*, where* p *is either zero or a prime congruent to* r *mod* 4*.*

In March 2008, I verified Conjecture 1.1 for $n \leqslant 17,000,000$ and then T. Noe continued the verification for $n \leqslant 2 \times 10^9$. It is interesting to compare Conjecture 1.1 with the Goldbach conjecture. Note that

$$|\{p \leqslant x : \ p \text{ is a prime}\}| \sim \frac{x}{\log x} \ \text{ and } \ |\{T_n \leqslant x : \ n \in \mathbb{N}\}| \sim \sqrt{2x}.$$

A well-known assertion of Fermat (proved by Euler) states that each prime $p \equiv 1 \pmod 4$ can be written in the form $x^2 + y^2$ with x even and y odd. Thus Conjecture 1.1 implies that for any $a = 0, 1, 2, \ldots$ all sufficiently large integers have the form $2^a(x^2 + y^2) + T_z$ with $x, y, z \in \mathbb{Z}$. If $p = x^2 + y^2$ with x even and y odd, then $2p = (x + y)^2 + (x - y)^2$ with $x \pm y$ odd. Thus our following conjecture is reasonable in view of Conjecture 1.1.

Conjecture 1.2 (Z. W. Sun, April 2008)**.** (i) *A natural number can be written as a sum of two* **even** *squares and a triangular number unless it*

is among the following list of 19 *exceptions:*

$$2,\ 12,\ 13,\ 24,\ 27,\ 34,\ 54,\ 84,\ 112,\ 133,$$
$$162,\ 234,\ 237,\ 279,\ 342,\ 399,\ 652,\ 834,\ 864.$$

(ii) *Each natural number* $n \notin E$ *is either a triangular number, or a sum of a triangular number and two* **odd** *squares, where the exceptional set* E *consists of the following* 25 *numbers:*

$$4,\ 7,\ 9,\ 14,\ 22,\ 42,\ 43,\ 48,\ 52,\ 67,\ 69,\ 72,\ 87,\ 114,$$
$$144,\ 157,\ 159,\ 169,\ 357,\ 402,\ 489,\ 507,\ 939,\ 952,\ 1029.$$

We have verified Conjecture 1.2 for $n \leqslant 2\times 10^6$.

In contrast to the Goldbach conjecture for *even* numbers, here we have a new conjecture for *odd* numbers.

Conjecture 1.3 (Z. W. Sun, May 2008)**.** (i) **Any odd integer** $n > 1$ **can be written in the form** $p + x(x+1)$ **with** p **a prime and and** x **an integer.**

(ii) *In general, for any* $b \in \mathbb{N}$ *and* $r \in \{1, 3, 5, \ldots\}$ *all sufficiently large odd integers can be written in the form* $p + x(x+1)$ *with* $x \in \mathbb{Z}$*, where* p *is a prime congruent to* r *mod* 2^b*.*

Conjectures 1.1-1.3 has been made public via messages to the Number Theory Mailing List. Some related results and conjectures can be found in my preprint *"On sums of primes and triangular numbers"* (`arXiv:0803:3737`).

2. Some congruences for sums involving central binomial coefficients or Catalan numbers

For $n \in \mathbb{N} = \{0, 1, \dots\}$, the nth Catalan number is given by

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1}.$$

Here is an alternate definition:

$$C_0 = 1 \ \text{ and } \ C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k} \ \ (n = 0, 1, 2, \dots).$$

The Catalan numbers play important roles in combinatorics; they arise naturally in many enumeration problems. For example, C_n is the number of binary parenthesizations of a string of $n+1$ letters; it is also the number of triangulations of a convex $(n+2)$-gon into n triangles by $n-1$ diagonals that do not intersect in their interiors. The generating function of the sequence $\{C_n\}_{n\geqslant 0}$ is

$$\sum_{n=0}^{\infty} C_n x^n = \frac{1-\sqrt{1-4x}}{2x}.$$

In 2006 H. Pan and Z.W. Sun [Discrete Math. 306(2006)] deduced the following combinatorial identity (for $l, m, n \in \mathbb{N}$)

$$\sum_{k=0}^{l}(-1)^{m-k}\binom{l}{k}\binom{m-k}{n}\binom{2k}{k-2l+m} = \sum_{k=0}^{l}\binom{l}{k}\binom{2k}{n}\binom{n-l}{m+n-3k-l},$$

and applied it to obtain the following result.

Theorem 2.1 (H. Pan and Z. W. Sun, 2006)**.** *Let p be a prime and $d \in \{0, \dots, p\}$. Then*

$$\sum_{k=0}^{p-1}\binom{2k}{k+d} \equiv \left(\frac{p-d}{3}\right) \pmod{p},$$

where the Legendre symbol $(\frac{a}{3})$ *is the unique integer in* $\{0,\pm1\}$ *satisfying* $a\equiv(\frac{a}{3})\pmod 3$. *If* $p>3$, *then*

$$\sum_{k=0}^{p-1}C_k\equiv\frac{3(\frac{p}{3})-1}{2}\pmod p\quad\text{and}\quad\sum_{k=0}^{p-1}kC_k\equiv\frac{1-(\frac{p}{3})}{2}\pmod p.$$

Here is a further extension of Theorem 2.1.

Theorem 2.2 (Z. W. Sun and R. Tauraso, 2007)**.** *Let* $p>3$ *be a prime, and let* a *be a positive integer. For* $d=0,1,\ldots,p$ *we have*

$$\sum_{k=0}^{p^a-1}\binom{2k}{k+d}\equiv\left(\frac{p^a-d}{3}\right)+2p^aS_d\pmod{p^2},$$

where

$$S_d=\sum_{0<k<d}\frac{(-1)^{k-1}}{k}\left(\frac{d-k}{3}\right)$$

and hence $S_0=S_1=0$, $S_2=1$ *and* $S_3=-3/2$. *If* $p>3$ *then*

$$\sum_{k=0}^{p^a-1}C_k\equiv1-3\left(\frac{p^a-1}{3}\right)\pmod{p^2}$$

and

$$\sum_{k=0}^{p^a-1}kC_k\equiv\left(\frac{p^a-1}{3}\right)\pmod{p^2}.$$

In the case $d=0$, the first congruence in Theorem 2.2 confirms a conjecture of A. Adamchuk and solves a problem of D. Callan.

The proof of Theorem 2.2 is very sophisticated. Here is one of the needed lemmas.

Lemma 2.1 (D. Finkel and E. Lehmer). *Let $n \in \mathbb{N}$ and $r \in \mathbb{Z}$. Then*

$$3\sum_{k\equiv r\ (\mathrm{mod}\ 3)}\binom{n}{k}=\begin{cases}2^n+2(-1)^n & \text{if } 3\mid n+r,\\ 2^n-(-1)^n & \text{if } 3\nmid n+r.\end{cases}$$

Problem 2.1 (Z. W. Sun and R. Tauraso, 2007). *Are there any composite numbers $n \not\equiv 0 \pmod 3$ such that*

$$\sum_{k=0}^{n-1}\binom{2k}{k}\equiv\left(\frac{n}{3}\right)\ (\mathrm{mod}\ n^2)\ ?$$

Are there any composite numbers $n \not\equiv 0 \pmod 3$ satisfying

$$\sum_{k=0}^{n-1}C_k\equiv 1-3\left(\frac{n-1}{3}\right)\ (\mathrm{mod}\ n^2)\ ?$$

It seems that the answers to Problem 2.1 are negative. We have confirmed this for $n \leqslant 5,000$ via Maple.

Here we state some typical results from a recent preprint of Z. W. Sun and R. Tauraso (`arXiv:0805.0563`).

Theorem 2.3 (Z. W. Sun and R. Tauraso, 2008). *Let p be a prime, and let $d \in \{0,\ldots,p^a\}$ with $a \in \mathbb{Z}^+$. If $p > 3$, then*

$$\left(\frac{p^a}{3}\right)\sum_{k=0}^{p^a-1}\binom{2k}{k}\equiv 1-\left(\frac{p}{3}\right)\frac{2}{9}p^2E_{p-3}\left(\frac{1}{3}\right)+\frac{26}{27}p^3B_{p-3}\ (\mathrm{mod}\ p^4)$$

and

$$\sum_{k=0}^{p^a-1}\binom{2k}{k+1}\equiv\left(\frac{p^a-1}{3}\right)+\frac{p^2}{9}\left(\frac{p^{a-1}}{3}\right)E_{p-3}\left(\frac{1}{3}\right)-\frac{18+13(\frac{p^a}{3})}{27}p^3B_{p-3}\ (\mathrm{mod}\ p^4),$$

where B_n is the nth Bernoulli number and $E_n(x)$ is the Euler polynomial of degree n; also

$$\sum_{k=1}^{p-1}\frac{\binom{2k}{k}}{k}\equiv\frac{8}{9}p^2B_{p-3}\pmod{p^3}$$

and

$$\sum_{k=1}^{p-1}\frac{C_k}{k}\equiv\frac{1-3(\frac{p}{3})}{2}+\frac{p^2}{9}\left(8B_{p-3}+3E_{p-3}\left(\frac{1}{3}\right)\right)\pmod{p^3}.$$

If $p\neq 2,5$ then

$$\sum_{k=1}^{p-1}(-1)^k\frac{\binom{2k}{k}}{k}\equiv-5\frac{F_{p-(\frac{p}{5})}}{p}\pmod{p},$$

where F_n denotes the nth Fibonacci number.

To prove Theorem 2.3 we need many auxiliary results. Here is a key lemma.

Lemma 2.2 (Z. W. Sun and R. Tauraso, 2008)**.** *For any $d,n\in\mathbb{N}$ we have the identity*

$$\sum_{0\leqslant k<n}\binom{2k}{k+d}+\left(\frac{d}{3}\right)=\sum_{0\leqslant k<n+d}\binom{2n}{k}\left(\frac{n+d-k}{3}\right).$$

We have also established the q-analogue of the identity in Lemma 2.2, which will appear in a forthcoming preprint.

3. p-adic orders of some sums involving binomial coefficients and an extension of Wilson's lemma

Let p be a prime, and let $n\in\mathbb{N}=\{0,1,2,\ldots\}$ and $r\in\mathbb{Z}$. In 1913 A. Fleck proved that

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

where $\lfloor\cdot\rfloor$ is the well-known floor function, and the p-adic order $\mathrm{ord}_p(\alpha)$ of a p-adic number α is given by $\sup\{a\in\mathbb{Z}:\ \alpha/p^a\in\mathbb{Z}_p\}$. (As usual $\mathbb{Z}_p$ denotes the ring of p-adic integers in the p-adic field $\mathbb{Q}_p$.)

Let $a\in\mathbb{Z}^+=\{1,2,3,\ldots\}$. In 1977, motivated by his study of p-adically continuous functions and **unaware of Fleck's earlier result**, C. S. Weisman [Michigan Math. J] extended Fleck's inequality as follows:

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

where φ is Euler's totient function.

Unaware of Fleck's and Weisman's earlier results, R. M. Wilson [Discrete Math. 2006] rediscovered Weisman's result in the case $n\equiv p^{a-1}\ (\mathrm{mod}\ \varphi(p^a))$, and used it to obtain the following lemma and give various applications on codewords in p-ary linear codes with weights.

Wilson's Lemma. *Let p be a prime, and let $a,b\in\mathbb{Z}^+$. Let f be an integer-valued function on the integers that is periodic modulo p^a. Then there exists a polynomial*

$$w(x)=c_0+c_1x+c_2\binom{x}{2}+\cdots+c_d\binom{x}{d}\quad(c_0,c_1,\ldots,c_d\in\mathbb{Z})$$

of degree smaller than $b\varphi(p^a)+p^{a-1}$ such that

$$\mathrm{ord}_p(c_n)\geqslant\left\lfloor\frac{n-p^{a-1}}{\varphi(p^a)}\right\rfloor\quad\textit{for all } n=0,\ldots,d,$$

and $w(x)\equiv f(x)\ (\mathrm{mod}\ p^b)$ for all $x\in\mathbb{Z}$.

This lemma is similar to a classical interpolation formula due to I. Newton and J. Gregory.

For a function f from the complex field $\mathbb{C}$ to $\mathbb{C}$, let $\Delta^0 f(x)=f(x)$, $\Delta f(x)=f(x+1)-f(x)$ and $\Delta^n f(x)=\Delta\Delta^{n-1}f(x)$ for $n=2,3,\ldots$.

Newton-Gregory Interpolation Formula. *Given a function $f:\mathbb{C}\to\mathbb{C}$, for any $d\in\mathbb{N}$ we have*

$$f(x)=\sum_{n=0}^d c_n\binom{x}{n}+R_d(x),$$

where

$$c_n=\Delta^n f(0)=\sum_{k=0}^n\binom{n}{k}(-1)^{n-k}f(k)$$

and

$$R_d(x)=\begin{vmatrix}1&0&\cdots&0&f(0)\\1&1^1&\cdots&1^d&f(1)\\\cdots&\cdots&\cdots&\cdots&\cdots\\1&d^1&\cdots&d^d&f(d)\\1&x^1&\cdots&x^d&f(x)\end{vmatrix}\Bigg/\begin{vmatrix}1^1&1^2&\cdots&1^d\\2^1&2^2&\cdots&2^d\\\cdots&\cdots&\cdots&\cdots\\d^1&d^2&\cdots&d^d\end{vmatrix}.$$

(*Note that $R_d(x)=0$ if f is a polynomial with* $\deg f\leqslant d$).

Now I cite a report on Wilson's lemma available from the internat.

At a conference (held in Iran) Prof. Wilson was one of several **keynote** invited speakers, and his well received lectures were given on two days. The first was called *A Lemma on Polynomials Modulo p^m and Applications to Coding Theory.* It had a certain fascination for those who could understand, and the first question asked after the lecture was: **"How did you think of this lemma? Were you awake late one night with a glass of wine?"**

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

(i) (Daqing Wan [Finite Fields Appl. 2006]) *We have*

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

(ii) (D. M. Davis and Z. W. Sun [J. Pure Appl. Algebra 2007]) *For any polynomial* $f(x)\in\mathbb{Z}[x]$, *we have*

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

(iii) (Z. W. Sun and D. M. Davis [Trans. Amer. Math. Soc. 2007])

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

Unaware of Fleck's result, in May 2005 D. Wan realized part (i) in the case $a=1$ during his study of the ψ-operator. Then I told him Fleck's and Weisman's results and obtained a common generalization of Weisman's and Wans's results [Acta Arith. 2006] by combinatorial arguments. Later Wan published part (i) of Theorem 3.1.

Unaware of Fleck's result, in 2005 D. M. Davis conjectured a weaker form of part (ii) in the case $p^a=2$ and $r=0$, and part (iii) in the case $p^a=4$ and $r=2$. After I learned Davis' conjectures in June 2005, I worked hard to attack the problems, and this finally resulted in two papers with Davis.

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 Theorem 3.1(ii).

Theorem 3.2 (Davis and Sun [J. Pure Appl. Algebra 2007]). *Let p be any prime and n be a positive integer.*

(i) *If $L \geqslant n-1+\lfloor n/(p(p-1))\rfloor$, then for all $m \geqslant n$ we have the following result for Stirling numbers of the second kind:*

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

(ii) *Some homotopy group $\pi_i(\mathrm{SU}(n))$ of the Lie group $\mathrm{SU}(n)$ contains an element of order $p^{n-1+\mathrm{ord}_p(\lfloor n/p\rfloor!)}$.*

Numerical examples indicate that Theorem 3.2 is very sharp.

For a prime p, we let $\overline{\mathbb{Q}}_p$ be the algebraic closure of the field $\mathbb{Q}_p$ and let $\overline{\mathbb{Z}}_p$ be the ring of p-adic algebraic integers in $\overline{\mathbb{Q}}_p$. For $m,n\in\mathbb{N}$ we use $[m,n]$ to denote the set $\{x\in\mathbb{Z}: m\leqslant x\leqslant n\}$.

Here is our further extension of Wilson's lemma based on Theorem 3.1.

Theorem 3.3 (Z. W. Sun, `arXiv:0608560`). *Let p be a prime, and let $a\in\mathbb{N}$ and $b\in\mathbb{Z}^+$. Let $f(x)\in\overline{\mathbb{Q}}_p[x]$ with $\deg f\leqslant l\in\mathbb{N}$ and $f(m)\in\overline{\mathbb{Z}}_p$ for all $m\in\mathbb{Z}$, and let g be a function from $[0,p^a-1]$ to $\overline{\mathbb{Z}}_p$. Let $d\in\mathbb{N}$ be the maximal integer with $M_d<b$, where M_d denotes*

$$\max\left\{\left\lfloor\frac{d-lp^a-p^{a-1}}{\varphi(p^a)}\right\rfloor,\mathrm{ord}_p\bigg(\left\lfloor\frac{d}{p^{a-1}}\right\rfloor!\bigg)-\mathrm{ord}_p(l!)-\min\left\{l,\left\lfloor\frac{d}{p^a}\right\rfloor\right\}\right\}.$$

Then there exists a polynomial

$$P(x)=\sum_{n=0}^{d}c_n\binom{x}{n}\quad(c_0,\ldots,c_d\in\overline{\mathbb{Z}}_p)$$

with $\mathrm{ord}_p(c_n)\geqslant M_n$ for all $n=0,\ldots,d$, such that

$$P(p^aq+r)\equiv f(q)g(r)\pmod{p^b}\ \text{ for all } q\in\mathbb{Z} \text{ and } r\in[0,p^a-1].$$

In the case $l = 0$, Theorem 3.3 reduces to the Wilson lemma.

The following celebrated theorem is well known and quite useful.

Chevalley-Warning Theorem. *Let $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$ be polynomials over a finite field F of characteristic p with $\deg f_1 + \cdots + \deg f_m < n$. Then the number of solutions to the system of equations*

$$f_1(x_1, \dots, x_n) = 0, \ \dots, \ f_m(x_1, \dots, x_n) = 0 \qquad (*)$$

over F^n is a multiple of p.

Here is a further refinement of the Chevalley-Warning theorem due to J. Ax [Amer. J. Math. 1964] in the case $m = 1$, and N. Katz [Amer. J. Math. 1971] in the general case.

Ax-Katz Theorem. *Let F_q be the finite field with $q = p^a$ elements where p is a prime and $a \in \mathbb{Z}^+$. Let $f_1(x, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$ be nonzero polynomials over F_q with degrees $d_1 \geqslant \cdots \geqslant d_m$ respectively. Then, for any positive integer b satisfying $n > (b-1)d_1 + (d_1 + \cdots + d_m)$, q^b divides the number of solutions to the system $(*)$ over F^n.*

D. Wan [Amer. J. Math., 1989; Proc. Amer. Math. Soc.] gave a new proof of the Ax-Katz theorem via the Stickelberger theorem. In 2005 X.-D. Hou [Finite Fields Appl.] reduced the Ax-Katz theorem to the Ax theorem on a single polynomial equation. In 2006 Wilson [Discrete Math.] reproved the Ax-Katz theorem for prime fields by using Wilson's Lemma.

With the help of Theorem 3.3, we establish the following extension of the Ax-Katz theorem for prime fields.

Theorem 3.4 (Z. W. Sun, 2006)**.** *Let $f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n)$ be nonzero polynomials with integer coefficients having degrees $d_1\geqslant\cdots\geqslant d_m$ respectively. If p is a prime, $a,b\in\mathbb{Z}^+$, $l_1,\ldots,l_m\in\mathbb{N}$ and*

$$n>(b-1)d_1p^{a-1}+\frac{p^a-1}{p-1}\sum_{k=1}^m d_k+\frac{p^a}{p-1}\sum_{k=1}^m l_kd_k,$$

then we have

$$\sum_{\substack{x_1,\ldots,x_n\in[0,p-1]\\ p^a\mid f_k(x_1,\ldots,x_n)\text{ for all }k\in[1,m]}}\prod_{k=1}^m\binom{f_k(x_1,\ldots,x_n)/p^a}{l_k}\equiv 0\ (\mathrm{mod}\ p^b).$$

In the case $a=1$ and $l_1=\cdots=l_m=0$ this reduces to the Ax-Katz theorem for the field $F_p=\mathbb{Z}/p\mathbb{Z}$.

THANK YOU VERY MUCH!