A talk given at the Institute of Mathematics, Academia Sinica (Taiwan) (Taipei; July 6, 2011)

On Arithmetic Properties of Bell Numbers, Delannoy Numbers and Schröder Numbers

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/~zwsun

July 6, 2011
Abstract

Bell numbers, Delannoy numbers and Schröder numbers are important quantities arising from enumerative combinatorics. Surprisingly they also have nice number-theoretic properties. We will talk about congruences related to Bell numbers, Delannoy numbers and Schroder numbers.
Let $p$ be a prime. A rational number is called a $p$-integer (or a rational $p$-adic integer) if it can be written in the form $a/b$ with $a, b \in \mathbb{Z}$ and $(b, p) = 1$. All $p$-integers form a ring $R_p$ which is a subring of the ring $\mathbb{Z}_p$ of all $p$-adic integers. For a $p$-integer $a/b$, an integer $c$ and a nonnegative integer $n$ if $a/b = c + p^n q$ for some $q \in R_p$ (equivalently, $a \equiv bc \pmod{p^n}$), then we write

$$\frac{a}{b} \equiv c \pmod{p^n}.$$ 

An Example for Congruences involving $p$-Integers:

$$1 + \frac{1}{2} \equiv 1 - 4 = -3 \pmod{3^2}.$$
Classical congruences for central binomial coefficients

A central binomial coefficient has the form
\[
\binom{2k}{k} (k = 0, 1, 2, \ldots).
\]

**Wolstenholme’s Congruence.** For any prime \( p > 3 \) we have
\[
H_{p-1} = \sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \pmod{p^2}
\]
and
\[
\binom{2p-1}{p-1} = \frac{1}{2} \binom{2p}{p} \equiv 1 \pmod{p^3}.
\]

**Remark.** In 1900 Glaiser proved that for any prime \( p > 3 \) we have
\[
\binom{2p-1}{p-1} \equiv 1 - \frac{2}{3} p^3 B_{p-3} \pmod{p^4},
\]
where \( B_n \) denotes the \( n \)th Bernoulli number.
Classical congruences for central binomial coefficients

Morley’s Congruence. For any prime \( p > 3 \) we have

\[
\binom{p - 1}{(p - 1)/2} \equiv \left( \frac{-1}{p} \right) 4^{p-1} \pmod{p^3}.
\]

Gauss’ Congruence. Let \( p \equiv 1 \pmod{4} \) be a prime and write \( p = x^2 + y^2 \) with \( x \equiv 1 \pmod{4} \) and \( y \equiv 0 \pmod{2} \). Then

\[
\binom{(p - 1)/2}{(p - 1)/4} \equiv 2x \pmod{p}.
\]

Further Refinement of Gauss’ Result (Chowla, Dwork and Evans, 1986):

\[
\binom{(p - 1)/2}{(p - 1)/4} \equiv \frac{2^{p-1} + 1}{2} \left( 2x - \frac{p}{2x} \right) \pmod{p^2}.
\]

It follows that

\[
\binom{(p - 1)/2}{(p - 1)/4}^2 \equiv 2^{p-1}(4x^2 - 2p) \pmod{p^2}.
\]
Catalan numbers

For \( n \in \mathbb{N} = \{0, 1, 2, \ldots\} \), the \( n \)th Catalan number is given by

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

Recursion.

\[
C_0 = 1 \quad \text{and} \quad C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k} \quad (n = 0, 1, 2, \ldots).
\]

Generating Function.

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

Combinatorial Interpretations. The Catalan numbers arise in many enumeration problems. For example, \( C_n \) is the number of binary parenthesizations of a string of \( n + 1 \) letters, and it is also the number of ways to triangulate a convex \((n + 2)\)-gon into \( n \) triangles by \( n - 1 \) diagonals that do not intersect in their interiors.
Recent results on $\sum_{k=0}^{p-1} \binom{2k}{k}$ and $\sum_{k=0}^{p-1} C_k \mod p^2$

Let $p$ be a prime and let $a \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.


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

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


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

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

$$\sum_{k=1}^{p-1} \frac{(2k)}{k} \equiv \frac{8}{9} p^2 B_{p-3} \pmod{p^3} \quad \text{for } p > 3.$$
Determination of $\sum_{k=0}^{p-1} \frac{(2k)}{m^k} \mod p^2$

Let $p$ be an odd prime. If $p/2 < k < p$ then

$$\binom{2k}{k} = \frac{(2k)!}{(k!)^2} \equiv 0 \pmod p.$$ 

Thus

$$\sum_{k=0}^{(p-1)/2} \frac{(2k)}{m^k} \equiv \sum_{k=0}^{p-1} \frac{(2k)}{m^k} \pmod p,$$

where $m$ is an integer with $p \nmid m$.

**Sun [Sci. China Math. 2010]:** Let $p$ be an odd prime and let $a, m \in \mathbb{Z}$ with $a > 0$ and $p \nmid m$. Then

$$\sum_{k=0}^{p^a-1} \frac{(2k)}{m^k} \equiv \left( \frac{m^2 - 4m}{p^a} \right) + \left( \frac{m^2 - 4m}{p^{a-1}} \right) u_{p^{-\left(\frac{m^2-4m}{p}\right)}} \pmod{p^2},$$

where $(-)$ is the Jacobi symbol and $\{u_n\}_{n\geq0}$ is the Lucas sequence given by

$$u_0 = 0, \ u_1 = 1, \ \text{and} \ u_{n+1} = (m - 2)u_n - u_{n-1} \ (n = 1, 2, 3, \ldots).$$
Euler numbers and some congruences mod $p^3$

Recall that Euler numbers $E_0, E_1, \ldots$ are given by

$$E_0 = 1, \quad \sum_{2 \mid k} \binom{n}{k} E_{n-k} = 0 \ (n = 1, 2, 3, \ldots).$$

It is known that $E_1 = E_3 = E_5 = \cdots = 0$ and

$$\sec x = \sum_{n=0}^{\infty} (-1)^n E_{2n} \frac{x^{2n}}{(2n)!} \quad (|x| < \frac{\pi}{2}).$$


$$\sum_{k=0}^{p-1} \frac{(2k)}{k} \frac{2^k}{2^k} \equiv (-1)^{(p-1)/2} - p^2 E_{p-3} \pmod{p^3},$$

$$\sum_{k=0}^{(p-1)/2} \frac{(2k)}{8^k} \equiv \left( \frac{2}{p} \right) + \left( \frac{-2}{p} \right) \frac{p^2}{4} E_{p-3} \pmod{p^3}. $$
Bell numbers

For \( n = 1, 2, 3, \ldots \), the \( n \)th Bell number \( B_n \) denotes the number of partitions of a set of cardinality \( n \). In addition, \( B_0 := 1 \). Here are values of \( B_1, \ldots, B_{10} \):

\[
1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975.
\]

Recursion:

\[
B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k \quad (n = 0, 1, 2, \ldots).
\]

Exponential Generating Function:

\[
\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = e^{e^x - 1}.
\]

Touchard’s Congruence: For any prime \( p \) and \( m, n = 0, 1, 2, \ldots \) we have

\[
B_{p^m+n} \equiv mB_n + B_{n+1} \pmod{p}.
\]
A conjecture on Bell numbers

**Conjecture** (Sun, July 17, 2010). For any positive integer $n$ there is a unique integer $a(n)$ such that

$$\sum_{k=0}^{p-1} \frac{B_k}{(-n)_k} \equiv a(n) \pmod{p} \text{ for any prime } p \mid n.$$ 

In particular,

$$a(2) = 1, \ a(3) = 2, \ a(4) = -1, \ a(5) = 10, \ a(6) = -43, \ a(7) = 266, \ a(8) = -1853, \ a(9) = 14834, \ a(10) = -133495.$$ 

**Remark.** It is easy to see that $a(1) = 2$. In fact, if $p$ is a prime then

$$\sum_{k=0}^{p-1} (-1)^k B_k \equiv \sum_{k=0}^{p-1} \binom{p-1}{k} B_k = B_p$$

$$\equiv B_0 + B_1 = 2 \pmod{p} \text{ (by Touchard’s congruence).}$$
Sun and Zagier’s results on Bell numbers

For $n = 1, 2, 3, \ldots$ the $n$th derangement number $D_n$ is the number of permutations $\sigma$ of $\{1, \ldots, n\}$ with $\sigma(i) \neq i$ for all $i = 1, \ldots, n$; in addition, $D_0 := 1$. It is well known that

$$
\frac{D_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!} \quad \text{for all } n \in \mathbb{N}.
$$

**Theorem** (Sun and D. Zagier, Bull. Austral. Math. Soc., 84(2011)) (i) For every positive integer $n$ we have

$$
\sum_{k=1}^{p-1} \frac{B_k}{(-n)^k} \equiv (-1)^{n-1}D_{n-1} \pmod{p}
$$

for any prime $p$ not dividing $n$.

(ii) Let $p$ be any prime. Then for all $n = 1, \ldots, p - 1$ we have

$$
B_n \equiv \sum_{k=1}^{p-1} (-1)^k D_{k-1}(-k)^n \pmod{p}.
$$
Part (i) implies part (ii)

**Part (i) implies part (ii).** For \( k, n \in \{1, \ldots, p - 1\} \) with \( k \neq n \), as \( p - 1 \nmid n - k \) we have

\[
\sum_{m=1}^{p-1} (-m)^{n-k} \equiv 0 \pmod{p}.
\]

Thus, with the help of part (i), if \( n \in \{1, \ldots, p - 1\} \) then

\[
-B_n \equiv \sum_{k=1}^{p-1} B_k \sum_{m=1}^{p-1} (-m)^{n-k} = \sum_{m=1}^{p-1} (-m)^n \sum_{k=1}^{p-1} \frac{B_k}{(-m)^k}
\]

\[
\equiv \sum_{m=1}^{p-1} (-m)^n(-1)^{m-1}D_{m-1} \pmod{p}.
\]
A direct proof of $B_p \equiv 2 \pmod{p}$

Note that

$$B_n = \sum_{k=0}^{n} S(n, k),$$

where $S(n, k)$ (a Stirling number of the second kind) is the number of ways to partition $\{1, \ldots, n\}$ into $k$ nonempty sets. It is well known that

$$S(n, k) = \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n \quad \text{for all } n \in \mathbb{Z}^+ \text{ and } k \in \mathbb{N}.$$

Clearly, $S(n, 0) = 0$ and $S(n, 1) = S(n, n) = 1$ for any $n \in \mathbb{Z}^+$.

Let $p$ be a prime. With the help of Fermat’s little theorem, if $1 < k < p$ then $S(p, k) \equiv S(1, k) = 0 \pmod{p}$. Therefore

$$B_p \equiv S(p, 1) + S(p, p) = 2 \pmod{p}.$$
Prove part (i) by induction

For any prime $p$,

$$\sum_{k=1}^{p-1} (-1)^k B_k \equiv \sum_{k=1}^{p-1} \left( \begin{array}{c} p - 1 \\ k \end{array} \right) B_k = B_p - B_0 \equiv 1 \pmod{p}.$$ 

So the desired result holds when $n = 1$.

Now fix $n \in \mathbb{Z}^+$ and suppose that

$$\sum_{k=1}^{p-1} \frac{B_k}{(-n)^k} \equiv (-1)^{n-1} D_{n-1} \pmod{p}$$

for every prime $p \nmid n$.

Let $p$ be any prime not dividing $n + 1$. Recall the easy identity

$$D_n = nD_{n-1} + (-1)^n.$$

If $p \mid n$, then $D_n \equiv (-1)^n \pmod{p}$ and hence

$$\sum_{k=1}^{p-1} \frac{B_k}{(-n - 1)^k} \equiv \sum_{k=1}^{p-1} \frac{B_k}{(-1)^k} \equiv 1 \equiv (-1)^n D_n \pmod{p}.$$
Prove part (i) by induction

Now suppose that \( p \nmid n \). Observe that

\[
\begin{align*}
\sum_{k=1}^{p-1} \frac{B_k}{(-n)^k} & = \sum_{k=1}^{p-1} \frac{\sum_{l=0}^{k-1} \binom{k-1}{l} B_l}{(-n)^k} = \sum_{l=0}^{p-2} \frac{B_l}{(-n)^l} \sum_{k=l+1}^{p-1} \frac{\binom{k-1}{l}}{(-n)^{k-l}} \\
& = \sum_{l=0}^{p-2} \frac{B_l}{(-n)^{l+1}} \sum_{r=1}^{p-1-l} \frac{\binom{l+r-1}{r-1}}{(-n)^{r-1}} \\
& = \sum_{l=0}^{p-2} \frac{B_l}{(-n)^{l+1}} \sum_{r=1}^{p-1-l} \frac{(-1)^{l-1}}{(r-1) n^{r-1}} \\
& \equiv \sum_{l=0}^{p-2} \frac{B_l}{(-n)^{l+1}} \sum_{r=1}^{p-1-l} \binom{p-1-l}{r-1} n^{-(r-1)} \\
& \equiv \sum_{l=0}^{p-1} \frac{B_l}{(-n)^{l+1}} \left( \left(1 + \frac{1}{n}\right)^{p-1-l} - \frac{1}{n^{p-1-l}} \right) \pmod{p}.
\end{align*}
\]
Prove part (i) by induction

Thus, applying Fermat’s little theorem we get

\[-n \sum_{k=1}^{p-1} \frac{B_k}{(-n)^k} \equiv \sum_{l=1}^{p-1} \frac{B_l}{(-n-1)^l} - \sum_{l=1}^{p-1} \frac{B_l}{(-1)^l} \pmod{p}.

Therefore

\[
\sum_{l=1}^{p-1} \frac{B_l}{(-n-1)^l} \equiv -n \sum_{k=1}^{p-1} \frac{B_k}{(-n)^k} + \sum_{l=1}^{p-1} \frac{B_l}{(-1)^l} \equiv -n(-1)^{n-1}D_{n-1} + 1 = (-1)^nD_n \pmod{p}.
\]

This concludes the induction step.
A further extension

The Touchard polynomial $T_n(x)$ of degree $n$ is given by

$$T_n(x) = \sum_{k=0}^{n} S(n, k)x^k.$$

Note that $T_n(1) = B_n$. Similar to the recursion for Bell numbers, we have the recursion

$$T_{n+1}(x) = x \sum_{k=0}^{n} \binom{n}{k} T_k(x).$$

**Theorem** (Sun & Zagier, Bull. Austral. Math. Soc., 84(2011)). For every positive integer $m$, we have

$$(-x)^m \sum_{0 < n < p} \frac{T_n(x)}{(-m)^n} \equiv -x^p \sum_{k=0}^{m-1} \frac{(m-1)!}{k!} (-x)^k \pmod{p}$$

for any prime $p$ not dividing $m$. 
Consequences

Let $p$ be a prime. The theorem implies the congruence

$$
\sum_{0<n<p} \frac{T_n(x)}{(-m)^n} \equiv \frac{1}{(-x)^{m-1}} \sum_{l=0}^{m-1} \frac{(m-1)!}{l!} (-x)^l \pmod{p}
$$

for any $p$-adic integer $x$ not divisible by $p$, special cases being

$$
\sum_{0<n<p} \frac{T_n(x)}{(-2)^n} \equiv \frac{x-1}{x} \pmod{p} \quad \text{for } p \neq 2,
$$

$$
\sum_{0<n<p} \frac{T_n(x)}{(-3)^n} \equiv \frac{x^2 - 2x + 2}{x^2} \pmod{p} \quad \text{for } p \neq 3,
$$

$$
\sum_{0<n<p} \frac{T_n(x)}{(-4)^n} \equiv \frac{x^3 - 3x^2 + 6x - 6}{x^3} \pmod{p} \quad \text{for } p \neq 2.
$$
On central Delannoy numbers

\[ D_n := \sum_{k=0}^{n} \binom{n}{k} \binom{n+k}{k} = \sum_{k=0}^{n} \binom{n+k}{2k} \binom{2k}{k}. \]

In combinatorics, \( D_n \) is the number of lattice paths from \((0, 0)\) to \((n, n)\) with steps \((1, 0), (0, 1)\) and \((1, 1)\).

**Theorem** (Sun, 2010-2011). Let \( p > 3 \) be a prime. Then

\[ \sum_{k=0}^{p-1} D_k \equiv \left( \frac{-1}{p} \right) - p^2 E_{p-3} \pmod{p^3}, \] \[ \sum_{k=0}^{p-1} D_k^2 \equiv \left( \frac{2}{p} \right) \pmod{p}, \]

\[ \sum_{k=1}^{p-1} \frac{D_k}{k} \equiv - q_p(2) \pmod{p}, \] \[ \sum_{k=1}^{p-1} \frac{D_k}{k^2} \equiv 2 \left( \frac{-1}{p} \right) E_{p-3} \pmod{p}, \]

\[ \sum_{k=1}^{p-1} \frac{D_k^2}{k^2} \equiv - 2q_p(2)^2 \pmod{p}, \]

where \( q_p(2) \) denotes the Fermat quotient \((2^{p-1} - 1)/p\).
An auxiliary identity

In the proof of the theorem, the following new identity plays an important role.

**New Identity** (Sun). For \( s = 1, 2 \) we have

\[
\sum_{k=-n}^{n} \frac{(-1)^k}{(2k + 1)^s} \binom{2n}{n+k} = \frac{16^n}{(2n + 1)^s \binom{2n}{n}}.
\]

Via Zeilberger’s algorithm we find that both sides satisfy the same recurrence relation.
On central Delannoy numbers

**Theorem** (Sun, 2010). Let $p > 3$ be a prime. Then

$$
\sum_{k=0}^{p-1} (2k + 1)(-1)^k D_k \equiv p - \frac{7}{12} p^4 B_{p-3} \pmod{p^5},
$$

$$
\sum_{k=0}^{p-1} (2k + 1) D_k \equiv p + 2 p^2 q_p(2) - p^3 q_p(2)^2 \pmod{p^4},
$$

where $B_0, B_1, B_2 \ldots$ are Bernoulli numbers.

**Conjecture** (Sun, 2010). For any prime $p > 3$ we have

$$
\sum_{k=1}^{p-1} \frac{D_k}{k} \equiv -q_p(2) + p q_p(2)^2 \pmod{p^2}.
$$

**Remark.** We can show the congruence modulo $p$. 
Congruences involving Schröder numbers

The $n$th Schröder number is given by

$$S_n = \sum_{k=0}^{n} \binom{n+k}{2k} C_k = \sum_{k=0}^{n} \frac{1}{k+1} \binom{n}{k} \binom{n+k}{k}$$

which is the number of lattice paths from $(0, 0)$ to $(n, n)$ with steps $(1, 0), (0, 1)$ and $(1, 1)$ that never rise above the line $y = x$.

**Theorem** (Sun, 2010). Let $p$ be an odd prime and let $m$ be an integer not divisible by $p$. Then

$$\sum_{k=1}^{p-1} \frac{S_k}{m^k} \equiv \frac{m^2 - 6m + 1}{2m} \left( 1 - \left( \frac{m^2 - 6m + 1}{p} \right) \right) \pmod{p}.$$ 

The theorem in the case $m = 6$ gives that

$$\sum_{k=1}^{p-1} \frac{S_k}{6^k} \equiv 0 \pmod{p} \quad \text{for any prime } p > 3.$$
An observation of van Hammer

Let \( p = 2n + 1 \) be a prime. As observed by van Hammer, for \( k = 0, \ldots, n \) we have

\[
\binom{n}{k} \binom{n+k}{k} (-1)^k = \binom{n}{k} \binom{-n-1}{k}
\]

\[
= \binom{(p-1)/2}{k} \binom{(-p-1)/2}{k}
\]

\[
= \prod_{j=0}^{k-1} \frac{p-1}{2} - j \left( \frac{-p-1}{2} - j \right)
\]

\[
= \prod_{j=0}^{k-1} \frac{(-1/2 - j)^2 - p^2/4}{(k!)^2}
\]

\[
\equiv \left( -1/2 \right)^2 \equiv \left( \frac{2k}{k} \right)^2 \equiv \frac{(2k)^2}{16^k} \pmod{p^2}
\]

Thus

\[
D_{(p-1)/2} \equiv \sum_{k=0}^{n} \frac{(2k)^2}{(-16)^k} \pmod{p^2}.
\]
On $D_{(p-1)/2}$ and $S_{(p-1)/2}$ mod $p^2$

**Theorem 1** (conjectured by Z. W. Sun in 2009 and proved by Z. H. Sun [Proc. AMS, 2011]) Let $p \equiv 1 \pmod{4}$ be a prime and write $p = x^2 + y^2$ with $x \equiv 1 \pmod{4}$ and $y \equiv 0 \pmod{2}$. Then

$$
\sum_{k=0}^{(p-1)/2} \frac{(2k)^2}{8^k} \equiv \sum_{k=0}^{(p-1)/2} \frac{(2k)^2}{(-16)^k} \equiv (-1)^{(p-1)/4} \left(2x - \frac{p}{2x}\right) \pmod{p^2}.
$$

**Theorem 2** (Z. W. Sun, 2011) Let $p \equiv 1 \pmod{4}$ be a prime and write $p = x^2 + y^2$ with $x \equiv 1 \pmod{4}$ and $y \equiv 0 \pmod{2}$. Then

$$
S_{(p-1)/2} \equiv \sum_{k=0}^{(p-1)/2} \frac{(2k)}{8^k} \frac{C_k}{(-16)^k} \equiv -8 \sum_{k=0}^{(p-1)/2} \frac{k(2k)^2}{(-16)^k} \equiv (-1)^{(p-1)/4} 2 \left(2x - \frac{p}{x}\right) \pmod{p^2}.
$$
**Conjecture** (Sun, 2010) Let \( p > 3 \) be a prime. Then

\[
\sum_{k=1}^{p-1} D_k S_k \equiv -2pH_{(p-1)/2} \pmod{p^3},
\]

and

\[
\sum_{k=1}^{(p-1)/2} D_k S_k \equiv \begin{cases} 
4x^2 \pmod{p} & \text{if } p \equiv 1 \pmod{4} \& p = x^2 + 4y^2, \\
0 \pmod{p} & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]
Thank you!