Plenary talk on the Combin. Satellite Confer. of ICM 2002 (Shijiazhuang, 2002-08-19)

PROBLEMS AND RESULTS IN COMBINATORIAL NUMBER THEORY

Zhi-Wei Sun

Department of Mathematics
Nanjing University
Nanjing 210093
The People's Republic of China
E-mail: zwsun@nju.edu.cn
Homepage: http://pweb.nju.edu.cn/zwsun

Abstract. In this talk we give a survey of some problems and results in combinatorial number theory (i.e. combinatorics of numbers). The selected topics include harmonic sequences, covers of the integers and groups, the combinatorial sum $\sum_{k\equiv r \pmod m}\binom{n}{k}$ and values of Bernoulli polynomials at rationals.

1. On Harmonic Sequences

For integers a and $n>0$, we call

$$a(n)=a+n\mathbb{Z}=\{x\in\mathbb{Z}\colon x\equiv a \pmod n\}$$

a residue class with modulus n. A finite sequence $\{n_s\}_{s=1}^k$ of positive integers is said to be *harmonic* if there exist integers $a_1,\ldots,a_k$ such that the residue classes $a_1(n_1),\ldots,a_k(n_k)$ are pairwise disjoint. Note that $a_i(n_i)\cap a_j(n_j)\neq\emptyset$ if and only if $(n_i,n_j)\mid a_i-a_j$. So, whether $\{n_s\}_{s=1}^k$ $(k>1)$ is harmonic or not, just depends on those greatest common divisors $d_{ij}=(n_i,n_j)$ $(1\leqslant i<j\leqslant k)$. A necessary condition for $\{n_s\}_{s=1}^k$ to be harmonic, is that $d_{ij}>1$ for all $1\leqslant i<j\leqslant k$.

In 1982 A. P. Huhn and L. Megyesi [Discrete Math. 41(1982)] used a graph-theoretic argument to obtain the following result: *If all those $d_{ij}=(n_i,n_j)$ $(i<j)$ are distinct and greater than one, then $\{n_s\}_{s=1}^k$ is harmonic.*

In 1992 Z. W. Sun developed a new method to study harmonic sequences, and used it to deduce the following extension of the Huhn–Megyesi result.

Theorem 1 [Sun, Discrete Math. 104(1992)]. *Let $n_1,\ldots,n_k$ be positive integers. Then $\{n_s\}_{s=1}^k$ is harmonic if*

$$\#d=|\{\{i,j\}:\ 1\leqslant i<j\leqslant k\ \&\ (n_i,n_j)=d\}|<\sqrt{\frac{d+7}{8}}$$

for those $d=1,2,\ldots,2^{k-2}$ or those $d=\prod_{i=1}^r p_i^{\alpha_i}$ ($p_1,\ldots,p_r$ are distinct primes) with $\sum_{i=1}^r\alpha_i(p_i-1)\leqslant k-2$.

Sun's Conjecture [Discrete Math., 104(1992)] The above $\sqrt{(d+7)/8}$ can be replaced by $2d-1$.

Though the conjecture is still open, following Sun's approach Y. G. Chen [Discrete Math. 162(1996)] proved the following result: *If $\#1=0,\ \#2\leqslant 1,\ \#3\leqslant 1$ and $\#d\leqslant d/4$ for all $d=4,5,\ldots,2k-2$, then $\{n_s\}_{s=1}^k$ is harmonic.*

In their 1982 paper, Huhn and Megyesi also posed two open problems on harmonic sequences. Both were solved by Sun [Chinese Ann. Math., 13A(1992)] negatively. Inspired by the second problem, we have the following

Conjecture. *Let $\{n_s\}_{s=1}^k$ be a harmonic sequence. Then $(n_i,n_j)\geqslant k$ for some $1\leqslant i<j\leqslant k$.*

This conjecture is quite striking and far from transparent. Maybe it is extremely difficult. It is known that the conjecture holds for $k\leqslant 12$.

2. On Covers of the Integers and Groups

For a finite system $A=\{a_s(n_s)\}_{s=1}^k$, its *covering function* $w_A:\mathbb{Z}\to\mathbb{N}=\{0,1,2,\ldots\}$ is given by

$$w_A(x)=|\{1\leqslant s\leqslant k\colon x\in a_s(n_s)\}|.$$

Clearly $w_A(x)$ is periodic modulo the least common multiple $N = [n_1, \dots, n_k]$ of the moduli $n_1, \dots, n_k$. Observe that

$$\frac{1}{N}\sum_{x=0}^{N-1} w_A(x) = \sum_{s=1}^{k} \frac{|\{0 \leqslant x < N\colon x \in a_s(n_s)\}|}{N} = \sum_{s=1}^{k} \frac{1}{n_s}.$$

If $w_A(x) = m$ for all $x \in \mathbb{Z}$, then we call A an *exact m-cover* of $\mathbb{Z}$, and in this case $\sum_{s=1}^{k} 1/n_s = m$.

Š. Porubský once asked whether each exact m-cover is a formal union of m disjoint covers. In 1976 Choi constructed an exact 2-cover which is not a union of two disjoint covers. Later M. Z. Zhang [J. Sichuan Univ. (Nat. sci. Ed.), 28(1991)] used a graph-theoretic approach to show that for each $m = 2, 3, \dots$ there exists an exact m-cover no subcover of which is an exact n-cover with $0 < n < m$.

Despite the negative answer to Porubský's question, in 1992 Z. W. Sun obtained a result which has a positive aspect in some sense.

Theorem 2. *Let $A = \{a_s(n_s)\}_{s=1}^{k}$ be an exact m-cover of $\mathbb{Z}$.*

(i) [Sun, Israel J. Math. 77(1992)] *For each $n = 1, \dots, m$ there are at least $\binom{m}{n}$ subsets I of $\{1, \dots, k\}$ such that $\sum_{i \in I} 1/n_i = n$. (The lower bound $\binom{m}{n}$ is best possible.) In particular, there exist m subsets I of $\{1, \dots, k\}$ with the property $\sum_{i \in I} 1/n_i = 1$.*

(ii) [Sun, Acta Arith. 81(1997)] *For any $t = 1, \dots, k$ and $a = 0, 1, 2, \dots$ we have*

$$\left|\left\{I \subseteq \{1, \dots, k\}\colon t \notin I \ \&\ \sum_{i \in I}\frac{1}{n_i} = \frac{a}{n_t}\right\}\right| \geqslant \binom{m-1}{\lfloor a/n_t \rfloor}$$

where $\lfloor x \rfloor$ refers to the greatest integer not exceeding x, and the lower bound is best possible.

Note that $\mathbb{Z}$ is an additive cyclic group and the residue class $a(n) = a + n\mathbb{Z}$ is just a coset of the subgroup $n\mathbb{Z}$ with index n.

Let G be a group and $G_1,\ldots,G_k$ be subgroups of G. Let $a_1,\ldots,a_k\in G$. If the system $\mathcal{A}=\{a_iG_i\}_{i=1}^k$ of left cosets covers all the elements of G at least m times but none of its proper subsystems does, then all the indices $[G:G_i]$ are known to be finite and furthermore $[G:\bigcap_{i=1}^k G_i]\leqslant k!$. (See [Sun, Fund. Math. 124(1990), European J. Combin. 22(2001)].)

The Herzog-Schönheim Conjecture. *Let $\mathcal{A}=\{a_iG_i\}_{i=1}^k$ $(k>1)$ be a partition (i.e. disjoint cover) of a group G into left cosets of subgroups $G_1,\ldots,G_k$. Then the indices $n_1=[G:G_1],\ldots,n_k=[G:G_k]$ cannot be pairwise distinct.*

In this direction we made the following progress.

Theorem 3 [Sun, J. Algebra 273(2004)]. *Let G be a group, and $\mathcal{A}=\{a_iG_i\}_{i=1}^k$ $(k>1)$ be a system of left cosets of subnormal subgroups. Suppose that $\mathcal{A}$ covers each $x\in G$ the same times, and*

$$n_1=[G:G_1]\leqslant\ldots\leqslant n_k=[G:G_k].$$

Then the indices $n_1,\ldots,n_k$ cannot be distinct. Moreover, if each index occurs in $n_1,\ldots,n_k$ at most M times, then

$$\log n_1\leqslant\frac{e^\gamma}{\log 2}M\log^2 M+O(M\log M\log\log M)$$

where $\gamma=0.577\ldots$ is the Euler constant and the O-constant is absolute.

We mention that the above theorem also answers a question analogous to a famous problem of Erdős negatively.

3. On the Sum $\sum_{k\equiv r \pmod m}\binom{n}{k}$ and Bernoulli Polynomials

For integers $m>0$, $n\geqslant 0$ and r we define

$$\begin{bmatrix}n\\ r\end{bmatrix}_m=\sum_{\substack{0\leqslant k\leqslant n\\ k\equiv r \pmod m}}\binom{n}{k}.$$

How to evaluate this sum? Z. H. Sun and Z. W. Sun investigated this systematically in the summer of 1988.

Using

$$\binom{n}{k} = \binom{n}{n-k} \quad \text{and} \quad \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1},$$

one can easily prove that

$$\begin{bmatrix} n \\ r \end{bmatrix}_m = \begin{bmatrix} n \\ n-r \end{bmatrix}_m \quad \text{and} \quad \begin{bmatrix} n+1 \\ r \end{bmatrix}_m = \begin{bmatrix} n \\ r \end{bmatrix}_m + \begin{bmatrix} n \\ r-1 \end{bmatrix}_m .$$

So it suffices to consider $\left[\begin{smallmatrix} n \\ r \end{smallmatrix}\right]_m$ with n odd and r even.

The Pell sequence $\{P_n\}_{n\in\mathbb{N}}$ and its companion $\{Q_n\}_{n\in\mathbb{N}}$ are defined as follows:

$$P_0 = 0,\ P_1 = 1,\ \text{and } P_{n+1} = 2P_n + P_{n-1} \text{ for } n = 1, 2, \dots ;$$

$$Q_0 = 2,\ Q_1 = 2,\ \text{and } Q_{n+1} = 2Q_n + Q_{n-1} \text{ for } n = 1, 2, \dots .$$

By induction,

$$P_n = \frac{1}{2\sqrt{2}}\left((1+\sqrt{2})^n - (1-\sqrt{2})^n\right) \text{ and } Q_n = (1+\sqrt{2})^n + (1-\sqrt{2})^n.$$

Theorem 4 [Z. H. Sun, Nanjing Univ. J. Math. Biquarterly, 1993]**.** *Let $n > 0$ be odd. We have*

(i) *if $n \equiv 1 \pmod 8$, then*

$$\begin{bmatrix} n \\ 2r \end{bmatrix}_8 = 2^{n-3} + (-1)^r 2^{(n-5)/2} + (-1)^{[r/2]+(n-1)/8} 2^{(n-5)/4} P_{(n+(-1)^r)/2};$$

(ii) *if $n \equiv 3 \pmod 8$, then*

$$\begin{bmatrix} n \\ 2r \end{bmatrix}_8 = 2^{n-3} - (-1)^r 2^{(n-5)/2} + (-1)^{[r/2]+(n-3)/8} 2^{(n-11)/4} Q_{(n-(-1)^r)/2};$$

(iii) *if $n \equiv 5 \pmod 8$, then*

$$\begin{bmatrix} n \\ 2r \end{bmatrix}_8 = 2^{n-3} - (-1)^r 2^{(n-5)/2} + (-1)^{[(r+1)/2]+(n+3)/8} 2^{(n-5)/4} P_{(n-(-1)^r)/2};$$

(iv) *if $n \equiv 7 \pmod 8$, then*

$$\begin{bmatrix} n \\ 2r \end{bmatrix}_8 = 2^{n-3} + (-1)^r 2^{(n-5)/2} + (-1)^{[(r+1)/2]+(n+1)/8} 2^{(n-11)/4} Q_{(n+(-1)^r)/2}.$$

The Fibonacci sequence $\{F_n\}_{n\in\mathbb{N}}$ and its companion $\{L_n\}_{n\in\mathbb{N}}$ are defined as follows:

$$F_0 = 0,\ F_1 = 1,\ \text{and } F_{n+1} = F_n + F_{n-1} \text{ for } n = 1, 2, \dots ;$$

$$L_0 = 2,\ L_1 = 1,\ \text{and } L_{n+1} = L_n + L_{n-1} \text{ for } n = 1, 2, \dots .$$

By induction,

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \text{ and } L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Theorem 5 [Z. H. Sun & Z. W. Sun, Acta Arith. 60(1992)]**.** *Let $n > 0$ be odd.*

(a) *If $n \equiv 1 \pmod 4$, then*

$$10\begin{bmatrix} n \\ (n-1)/2 \end{bmatrix}_{10} = 2^n + L_{n+1} + 5^{(n+3)/4}F_{(n+1)/2},$$
$$10\begin{bmatrix} n \\ (n+3)/2 \end{bmatrix}_{10} = 2^n - L_{n-1} + 5^{(n+3)/4}F_{(n-1)/2},$$
$$10\begin{bmatrix} n \\ (n+7)/2 \end{bmatrix}_{10} = 2^n - L_{n-1} - 5^{(n+3)/4}F_{(n-1)/2},$$
$$10\begin{bmatrix} n \\ (n+11)/2 \end{bmatrix}_{10} = 2^n + L_{n+1} - 5^{(n+3)/4}F_{(n+1)/2}.$$

(b) *If $n \equiv 3 \pmod 4$, then*

$$10\begin{bmatrix} n \\ (n-1)/2 \end{bmatrix}_{10} = 2^n + L_{n+1} + 5^{(n+1)/4}L_{(n+1)/2},$$
$$10\begin{bmatrix} n \\ (n+3)/2 \end{bmatrix}_{10} = 2^n - L_{n-1} + 5^{(n+1)/4}L_{(n-1)/2},$$
$$10\begin{bmatrix} n \\ (n+7)/2 \end{bmatrix}_{10} = 2^n - L_{n-1} - 5^{(n+1)/4}L_{(n-1)/2},$$
$$10\begin{bmatrix} n \\ (n+11)/2 \end{bmatrix}_{10} = 2^n + L_{n+1} - 5^{(n+1)/4}L_{(n+1)/2}.$$

(c) *We have*

$$10\begin{bmatrix} n \\ (n-5)/2 \end{bmatrix}_{10} = 2^n - 2L_n.$$

Now we define a special Lucas sequence $\{S_n\}_{n\in\mathbb{N}}$ and its companion $\{T_n\}_{n\in\mathbb{N}}$ as follows:

$$S_0 = 0,\ S_1 = 1,\ \text{and } S_{n+1} = 4S_n - S_{n-1} \text{ for } n = 1, 2, \ldots ;$$

$$T_0 = 2,\ T_1 = 4,\ \text{and } T_{n+1} = 4T_n - T_{n-1} \text{ for } n = 1, 2, \ldots .$$

By induction,

$$S_n = \frac{1}{2\sqrt{3}}\left((2+\sqrt{3})^n - (2-\sqrt{3})^n\right) \text{ and } T_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n.$$

Theorem 6 [Z. W. Sun 1988; Israel J. Math. 128(2002)]**.** *Let $n > 0$ be odd and $r \in \mathbb{Z}$. Then*

$$12\begin{bmatrix} n \\ r \end{bmatrix}_{12} - 2^n - 1$$
$$=\begin{cases} 3^{\frac{n+1}{2}} + (-1)^{\frac{r(n-r)}{2}}(\frac{2}{n})(2^{\frac{n+1}{2}} + T_{\frac{n+1}{2}}) & \text{if } n - 2r \equiv \pm 1 \pmod{12}, \\ -3 + (-1)^{\frac{r(n-r)}{2}}(\frac{2}{n})(2^{\frac{n+1}{2}} - T_{\frac{n+1}{2}} + T_{\frac{n-1}{2}}) & \text{if } n - 2r \equiv \pm 3 \pmod{12}, \\ -3^{\frac{n+1}{2}} + (-1)^{\frac{r(n-r)}{2}}(\frac{2}{n})(2^{\frac{n+1}{2}} - T_{\frac{n-1}{2}}) & \text{if } n - 2r \equiv \pm 5 \pmod{12}, \end{cases}$$

where $(-)$ denotes the Jacobi symbol.

We mention that Theorems 4–6 have many interesting applications in number theory. For example, using Theorem 5 Z. H. Sun and Z. W. Sun proved in 1992 that if p is an odd prime with $p^2 \nmid F_{p-(\frac{5}{p})}$ (this is equivalent to an open conjecture of D. D. Wall), then there are no $x, y, z \in \mathbb{Z}$ such that $x^p + y^p = z^p$ and $p \nmid xyz$. For the general theory concerning the sum $\begin{bmatrix} n \\ r \end{bmatrix}_m$, the reader may consult Z. W. Sun [Israel J. Math. 128(2002)].

For $n = 0, 1, 2, \ldots$ the nth Bernoulli polynomial $B_n(x)$ is given by

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k},$$

where the Bernoulli numbers $B_0, B_1, B_2, \ldots$ is defined by the power series

$$\frac{z}{e^z - 1} = \sum_{k=0}^{\infty} B_k \frac{z^k}{k!} \quad (0 < |z| < 2\pi).$$

Let $n \in \mathbb{N}$. It is known that

$$B_n\left(\frac{1}{2}\right) = \left(2^{1-n} - 1\right) B_n.$$

Also, if $2 \mid n$ then

$$\begin{aligned} B_n\left(\frac{1}{3}\right) = B_n\left(\frac{2}{3}\right) =&(3^{1-n} - 1)\frac{B_n}{2}, \\ B_n\left(\frac{1}{4}\right) = B_n\left(\frac{3}{4}\right) =&2^{-n}(2^{1-n} - 1)B_n, \\ B_n\left(\frac{1}{6}\right) = B_n\left(\frac{5}{6}\right) =&(2^{1-n} - 1)(3^{1-n} - 1)\frac{B_n}{2}. \end{aligned}$$

Observe that $\varphi(1) = \varphi(2) = 1$ and $\varphi(3) = \varphi(4) = \varphi(6) = 2$.

Let p be an odd prime. For an integer a not divisible by p we use $q_p(a)$ to denote the Fermat quotient $(a^{p-1} - 1)/p$. Note that

$$B_{p-1}\left(\frac{1}{2}\right) - B_{p-1} = 2^{1-(p-1)}\left(1 - 2^{p-1}\right) B_{p-1} \equiv 2q_p(2) \pmod p$$

since $pB_{p-1} \equiv -1 \pmod p$.

In 1996 A. Granville and Z. W. Sun proved the following surprising result for Bernoulli polynomials.

Theorem 7 [Granville and Sun, Pacific J. Math. 172(1996)]**.** *Let p be an odd prime, and a and m be integers with $1 \leqslant a < m$ and $p \nmid m$. Then*

$$B_{p-1}\left(\frac{a}{m}\right) - B_{p-1} \equiv \frac{m}{2p}(U_p - 1) \pmod p,$$

where $\{U_n\}_{n=0}^{+\infty}$ is a certain linearly recurrent sequence of order $\lfloor m/2 \rfloor$ which depends only on a, m and p mod m, namely

$$U_n = \frac{1}{2m}\sum_{\substack{\gamma^m=1\\ \gamma\neq 1}} \frac{2 - \gamma^a - \gamma^{-a}}{2 - \gamma^p - \gamma^{-p}}(2 - \gamma - \gamma^{-1})^n \quad \textit{for } n = 0, 1, 2, \ldots .$$

Moreover we can express the sequence $\{U_n\}_{n=0}^{+\infty}$ *in terms of linear recurrences with orders in* $\{1\}\cup\{\varphi(d)/2\colon d\mid m\ \&\ d>2\}$*, namely*

$$mU_n=\sum_{\substack{d\mid m\\ d>2}}u_n(d;a,p)+\begin{cases}2^{2n-1} & \text{if } 2\nmid a\ \&\ 2\mid m,\\ 0 & \text{otherwise},\end{cases}$$

where

$$u_n(d;a,p)=\sum_{\substack{0<c<d/2\\ (c,d)=1}}\left(\frac{\sin(\pi ac/d)}{\sin(\pi pc/d)}\right)^2\left(4\sin^2\frac{\pi c}{d}\right)^n.$$

(*Note that* $u_n(m;a,p)=mU_n$ *if* m *is an odd prime.*)

Let p be an odd prime, and a,m be integers with $1\le a<m$ and $(a,m)=1$. Here is a celebrated result of Granville and Sun deduced from the above theorem:

$$B_{p-1}\left(\frac{a}{m}\right)-B_{p-1}\equiv\begin{cases}(\frac{ap}{5})\frac{5}{4p}F_{p-(\frac{5}{p})}+\frac{5}{4}q_p(5)\pmod p & \text{if } m=5,\\ (\frac{2}{ap})\frac{2}{p}P_{p-(\frac{2}{p})}+4q_p(2)\pmod p & \text{if } m=8,\\ (\frac{ap}{5})\frac{15}{4p}F_{p-(\frac{5}{p})}+\frac{5}{4}q_p(5)+2q_p(2)\pmod p & \text{if } m=10,\\ (\frac{3}{a})\frac{3}{p}S_{p-(\frac{3}{p})}+3q_p(2)+\frac{3}{2}q_p(3)\pmod p & \text{if } m=12.\end{cases}$$