arXiv:math.GR/0411289 v1 12 Nov 2004

A talk given at the Institute of Math. Science, Nanjing Univ. on Oct. 8, 2004.

GROUPS AND COMBINATORIAL NUMBER THEORY

Zhi-Wei Sun

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

Abstract. In this talk we introduce several topics in combinatorial number theory which are related to groups; the topics include combinatorial aspects of covers of groups by cosets, and also restricted sumsets and zero-sum problems on abelian groups. A survey of known results and open problems on the topics is given in a popular way.

1. Nontrivial problems and results on cyclic groups

Any infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ of all integers. Subgroups of $\mathbb{Z}$ different from $\{0\}$ are those $n\mathbb{Z} = \{nq : q \in \mathbb{Z}\}$ with $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$. Any cyclic group of order n is isomorphic to the additive group $\mathbb{Z}/n\mathbb{Z}$ of residue classes modulo n. A coset of the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ has the form

$$a + n\mathbb{Z} = \{a + nq : q \in \mathbb{Z}\} = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$$

2000 *Mathematics Subject Classifications*: Primary 20D60; Secondary 05A05, 11B25, 11B75, 11P70.

All papers of the author mentioned in this survey are available from his homepage http://pweb.nju.edu.cn/zwsun.

which is called a *residue class* with *modulus* n or an arithmetic sequence with common difference n. For convenience we also write $a(n)$ or $a(\mathrm{mod}\ n)$ for $a+n\mathbb{Z}$, thus $0(1)=\mathbb{Z}$ and $1(2)$ is the set of odd integers.

We can decompose the group $\mathbb{Z}$ into n cosets of $n\mathbb{Z}$, namely

$$\{r(n)\}_{r=0}^{n-1}=\{0(n),\ 1(n),\ \ldots,\ n-1(n)\}$$

is a partition of $\mathbb{Z}$ (i.e., a disjoint cover of $\mathbb{Z}$). For the index of the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$, we clearly have $[\mathbb{Z}:n\mathbb{Z}]=|\mathbb{Z}/n\mathbb{Z}|=n$.

Since $0(2^n)$ is a disjoint union of the residue classes $2^n(2^{n+1})$ and $0(2^{n+1})$, the systems

$$A_1=\{1(2),0(2)\},\ A_2=\{1(2),2(4),0(4)\},\ A_3=\{1(2),2(4),4(8),0(8)\},$$
$$\cdots\cdots,\ A_k=\{1(2),2(2^2),\ldots,2^{k-1}(2^k),0(2^k)\},\ \cdots\cdots$$

are disjoint covers of $\mathbb{Z}$.

The concept of cover of $\mathbb{Z}$ was first introduced by P. Erdős in the early 1930s. He noted that $\{0(2),\ 0(3),\ 1(4),\ 5(6),\ 7(12)\}$ is a cover of $\mathbb{Z}$ with the moduli $2,3,4,6,12$ distinct.

Soon after his invention of the concept of cover of $\mathbb{Z}$, Erdős made the following conjecture: *If $A=\{a_s(n_s)\}_{s=1}^k$ $(k>1)$ is a system of residue classes with the moduli $n_1,\ldots,n_k$ distinct, then it cannot be a disjoint cover of $\mathbb{Z}$.*

Theorem 1.1. *Let $A=\{a_s(n_s)\}_{s=1}^k$.*

(i) (H. Davenport, L. Mirsky, D. Newman and R. Radó) *If A is a disjoint cover of $\mathbb{Z}$ with $1<n_1\leqslant n_2\leqslant\cdots\leqslant n_{k-1}\leqslant n_k$, then we must have $n_{k-1}=n_k$.*

(ii) [Z. W. Sun, Chinese Quart. J. Math. 1991] *Let* n_0 *be a positive period of the function* $w_A(x) = |\{1 \leqslant s \leqslant k : x \in a_s(n_s)\}|$. *For any positive integer* d *with* $d \nmid n_0$ *and* $I(d) = \{1 \leqslant s \leqslant k : d \mid n_s\} \neq \emptyset$, *we have*

$$|I(d)| \geqslant |\{a_s \bmod d : s \in I(d)\}| \geqslant \min_{\substack{0 \leqslant s \leqslant k \\ d \nmid n_s}} \frac{d}{\gcd(d, n_s)} \geqslant p(d),$$

where $p(d)$ *is the least prime divisor of* d.

Proof of part (*i*). Without loss of generality we let $0 \leqslant a_s < n_s$ $(1 \leqslant s \leqslant k)$. For $|z| < 1$ we have

$$\sum_{s=1}^{k} \frac{z^{a_s}}{1 - z^{n_s}} = \sum_{s=1}^{k} \sum_{q=0}^{\infty} z^{a_s + q n_s} = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}.$$

If $n_{k-1} < n_k$ then

$$\infty = \lim_{\substack{z \to e^{2\pi i/n_k} \\ |z|<1}} \frac{z^{a_k}}{1 - z^{n_k}} = \lim_{\substack{z \to e^{2\pi i/n_k} \\ |z|<1}} \left(\frac{1}{1-z} - \sum_{s=1}^{k-1} \frac{z^{a_s}}{1 - z^{n_s}} \right) < \infty,$$

a contradiction! $\square$

Part (ii) in the case $n_0 = 1$ and $d = n_k$ yields the Davenport-Mirsky-Newman-Radó result, a further extension of part (ii) was given by Z. W. Sun [Math. Res. Lett. 11(2004)] and [J. Number Theory, to appear].

Recall that

$$A_k = \{1(2), 2(2^2), \ldots, 2^{k-1}(2^k), 0(2^k)\}$$

is a disjoint cover of $\mathbb{Z}$. Thus the system $\{1(2), 2(2^2), \ldots, 2^{k-1}(2^k)\}$ covers $1, \ldots, 2^k - 1$ but does not cover any multiple of 2^k. In 1965 P. Erdős made the following conjecture.

Erdős' Conjecture. *$A = \{a_s(n_s)\}_{s=1}^k$ forms a cover of $\mathbb{Z}$ if it covers those integers from 1 to 2^k.*

In 1969–1970 R. B. Crittenden and C. L. Vanden Eynden [Bull. Amer. Math. Soc. 1969; Proc. Amer. Math. Soc. 1970] supplied a long and awkward proof of the Erdős conjecture for $k \geqslant 20$, which involves some deep results concerning the distribution of primes.

The following result is stronger than Erdős' conjecture.

Theorem 1.2 [Z. W. Sun, Acta Arith. 72(1995), Trans. Amer. Math. Soc. 348(1996)]**.** *Let $A = \{a_s(n_s)\}_{s=1}^k$ be a finite system of residue classes, and let $m_1, \ldots, m_k$ be integers relatively prime to $n_1, \ldots, n_k$ respectively. Then system A forms an m-cover of $\mathbb{Z}$ (i.e., A covers every integer at least m times) if it covers $|S|$ consecutive integers at least m times, where*

$$S = \left\{ \left\{ \sum_{s \in I} \frac{m_s}{n_s} \right\} : \, I \subseteq \{1, \ldots, k\} \right\}.$$

(As usual the fractional part of a real number x is denoted by $\{x\}$.)

`Proof of Theorem 1.2 in the case` $m = 1$. For any integer x, clearly

$$\begin{aligned}
& x \text{ is covered by } A \\
\iff & e^{2\pi i (a_s - x) m_s / n_s} = 1 \text{ for some } s = 1, \ldots, k \\
\iff & \prod_{s=1}^{k} \left(1 - e^{2\pi i (a_s - x) m_s / n_s} \right) = 0 \\
\iff & \sum_{I \subseteq \{1, \ldots, k\}} (-1)^{|I|} e^{2\pi i \sum_{s \in I} a_s m_s / n_s} \cdot e^{-2\pi i x \sum_{s \in I} m_s / n_s} = 0 \\
\iff & \sum_{\theta \in S} e^{-2\pi i x \theta} z_\theta = 0,
\end{aligned}$$

where

$$z_\theta = \sum_{\substack{I\subseteq\{1,\ldots,k\}\\ \{\sum_{s\in I} m_s/n_s\}=\theta}} (-1)^{|I|} e^{2\pi i \sum_{s\in I} a_s m_s/n_s}.$$

Suppose that A covers $|S|$ consecutive integers $a, a+1, \ldots, a+|S|-1$ where $a \in \mathbb{Z}$. By the above,

$$\sum_{\theta\in S} (e^{-2\pi i\theta})^r (e^{-2\pi i a\theta} z_\theta) = 0$$

for $r = 0, 1, \ldots, |S|-1$. As the determinant $\|(e^{-2\pi i\theta})^r\|_{0\leqslant r<|S|,\,\theta\in S}$ is of Vandermonde's type and hence nonzero, by Cramer's rule we have $z_\theta = 0$ for all $\theta \in S$. Therefore $\sum_{\theta\in S} e^{-2\pi i x\theta} z_\theta = 0$ for all $x \in \mathbb{Z}$, i.e., any $x \in \mathbb{Z}$ is covered by A. This proves the theorem in the case $m = 1$. $\square$

The following theorem shows that disjoint covers of $\mathbb{Z}$ are related to unit fractions, actually further results were obtained by Z. W. Sun.

Theorem 1.3 (Z. W. Sun [Acta Arith. 1995; Trans. Amer. Math. Soc. 1996])**.** *Let $A = \{a_s(n_s)\}_{s=1}^k$ be a disjoint cover of $\mathbb{Z}$.*

(i) *If $\emptyset \neq J \subset \{1, \ldots, k\}$, then there exists an $I \subseteq \{1, \ldots, k\}$ with $I \neq J$ such that $\sum_{s\in I} 1/n_s = \sum_{s\in J} 1/n_s$.*

(ii) *For any $1 \leqslant t \leqslant k$ and $r \in \{0, 1, \ldots, n_t - 1\}$, there is an $I \subseteq \{1, \ldots, k\} \setminus \{t\}$ such that $\sum_{s\in I} 1/n_s = r/n_t$.*

Proof. Let $N = [n_1, \ldots, n_k]$ be the least common multiple of $n_1, \ldots, n_k$. Then

$$\prod_{s=1}^{k} \left(1 - z^{N/n_s} e^{2\pi i a_s/n_s}\right) = 1 - z^N$$

because each Nth root of unity is a single zero of the left hand side. Thus

$$\sum_{I\subseteq\{1,\ldots,k\}}(-1)^{|I|}z^{\sum_{s\in I}N/n_s}e^{2\pi i\sum_{s\in I}a_s/n_s}=1-z^N.$$

Comparing the degrees of both sides we obtain the well-known equality $\sum_{s=1}^k 1/n_s=1$. As $\emptyset\neq J\subset\{1,\ldots,k\}$, $0<\sum_{s\in J}N/n_s<N$ and hence

$$\sum_{\substack{I\subseteq\{1,\ldots,k\}\\ \sum_{s\in I}1/n_s=\sum_{s\in J}1/n_s}}(-1)^{|I|}e^{2\pi i\sum_{s\in I}a_s/n_s}=0$$

which implies that $\sum_{s\in I}1/n_s=\sum_{s\in J}1/n_s$ for some $I\subseteq\{1,\ldots,k\}$ with $I\neq J$.

Now fix $1\leqslant t\leqslant k$. Observe that

$$\prod_{\substack{s=1\\ s\neq t}}^k\left(1-z^{N/n_s}e^{2\pi ia_s/n_s}\right)=\frac{1-z^N}{1-z^{N/n_t}e^{2\pi ia_t/n_t}}=\sum_{r=0}^{n_t-1}z^{Nr/n_t}e^{2\pi ia_tr/n_t}.$$

Thus, for any $r=0,1,\ldots,n_t-1$ we have

$$\sum_{\substack{I\subseteq\{1,\ldots,k\}\setminus\{t\}\\ \sum_{s\in I}1/n_s=r/n_t}}(-1)^{|I|}e^{2\pi i\sum_{s\in I}a_s/n_s}=e^{2\pi ia_tr/n_t}\neq 0$$

and hence $\sum_{s\in I}1/n_s=r/n_t$ for some $I\subseteq\{1,\ldots,k\}\setminus\{t\}$. $\square$

We mention that covers of $\mathbb{Z}$ by residue classes have many surprising applications. For example, on the basis of Cohen and Selfridge's work, Z. W. Sun [Proc. Amer. Math. Soc. 2000] showed that *if*

$$x\equiv 47867742232066880047611079 \pmod M$$

then x is not of the form $\pm p^a \pm q^b$, where p, q are primes and a, b are nonnegative integers, and M is a 29-digit number given by

$$\prod_{p \leqslant 19} p \times 31 \times 37 \times 41 \times 61 \times 73 \times 97 \times 109 \times 151 \times 241 \times 257 \times 331$$
$$= 66483084961588510124010691590.$$

If $A = \{a_1 < \cdots < a_k\}$ and $B = \{b_1 < \cdots < b_l\}$ are finite subsets of $\mathbb{Z}$, then clearly the sumset $A + B = \{a + b : a \in A \ \&\ b \in B\}$ contains at least the following $k + l - 1$ elements:

$$a_1 + b_1 < a_2 + b_1 < \cdots < a_k + b_1 < a_k + b_2 < \cdots < a_k + b_l.$$

However, the following result for cyclic groups of prime orders is nontrivial and very useful.

Theorem 1.4 (Cauchy-Davenport Theorem)**.** *Let A and B be nonempty subsets of $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ where p is a prime. Then we have*

$$|A + B| \geqslant \min\{p, |A| + |B| - 1\}.$$

In 1964 P. Erdős and Heilbronn posed the following conjecture for cyclic groups of prime orders.

Erdős-Heilbronn Conjecture. *Let A be a nonempty subset of $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ where p is a prime. Then we have*

$$|2^\wedge A| \geqslant \min\{p, 2|A| - 3\}$$

where $2^\wedge A=\{a+b:\ a,b\in A\ \&\ a\neq b\}$.

This conjecture remained open until it was confirmed by Dias da Silva and Y. Hamidoune [Bull. London. Math. Soc. 1994] thirty years later, with the help of the representation theory of groups.

Theorem 1.5 (The da Silva–Hamidoune Theorem). *Let p be a prime and $\emptyset\neq A\subseteq\mathbb{Z}_p$. Then we have*

$$|n^\wedge A|\geq\min\{p,\ n|A|-n^2+1\},$$

where $n^\wedge A$ denotes the set of all sums of n distinct elements of A.

If p is a prime, $A\subseteq\mathbb{Z}_p$ and $|A|>\sqrt{4p-7}$, then by the da Silva–Hamidoune theorem, any element of $\mathbb{Z}_p$ can be written as a sum of $\lfloor|A|/2\rfloor$ distinct elements of A.

In 1995–1996 Alon, Nathanson and Ruzsa [Amer. Math. Monthly 1995, J. Number Theory 1996] developed a polynomial method rooted in [Alon and Tarsi, Combinatorica 1989] to prove the Erdős-Heilbronn conjecture and some similar results. The method turns out to be very powerful and has many applications in number theory and combinatorics.

An extension of Theorem 1.5 appeared in Q. H. Hou and Z. W. Sun [Acta Arith. 2002]. H. Pan and Z. W. Sun [J. Combin. Theory Ser. A 2002] obtained a general result on sumsets with polynomial restrictions which includes the Cauchy-Davenport theorem as a special case.

Suppose that

$$\{a_1,\cdots,a_n\},\ \{b_1,\cdots,b_n\}\text{ and }\{a_1+b_1,\cdots,a_n+b_n\}$$

are complete systems of residues modulo n. Let

$$\sigma = 0 + 1 + \cdots + (n-1) = \frac{n(n-1)}{2}.$$

As

$$\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i,$$

we have $\sigma \equiv \sigma + \sigma \pmod{n}$ and hence $2 \nmid n$.

In 2001, Dasgupta, Károlyi, Serra and Szegedy [Israel J. Math. 2001] confirmed a conjecture of H. S. Snevily for cyclic groups.

Theorem 1.6 (Dasgupta-Károlyi-Serra-Szegedy Theorem). *Let G be an additive cyclic group with $|G|$ odd. Let A and B be subsets of G with cardinality $n > 0$. Then there is a numbering $\{a_i\}_{i=1}^n$ of the elements of A and a numbering $\{b_i\}_{i=1}^n$ of the elements of B such that $a_1+b_1, \cdots, a_n+b_n$ are pairwise distinct.*

Proof. As $2^{\varphi(|G|)} \equiv 1 \pmod{|G|}$ (where φ is Euler's totient function), the **multiplicative** group of the finite field F with order $2^{\varphi(|G|)}$ has a cyclic subgroup isomorphic to G. Thus we can view G as a subgroup of the multiplicative group $F^* = F \setminus \{0\}$.

Write $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$. We want to show that there is a $\sigma \in S_n$ such that $a_{\sigma(i)}b_i \neq a_{\sigma(j)}b_j$ whenever $1 \leqslant i < j \leqslant n$. In other words,

$$c = \sum_{\sigma \in S_n} \prod_{1 \leqslant i < j \leqslant n} \left(a_{\sigma(j)}b_j - a_{\sigma(i)}b_i\right) \neq 0.$$

In fact,

$$
\begin{aligned}
c=&\sum_{\sigma\in S_n}\|a_{\sigma(j)}^{i-1}b_j^{i-1}\|_{1\leqslant i,j\leqslant n}\quad\text{(Vandermonde)}\\
=&\sum_{\sigma\in S_n}\sum_{\tau\in S_n}\mathrm{sign}(\tau)\prod_{j=1}^n a_{\sigma(j)}^{\tau(j)-1}b_j^{\tau(j)-1}\\
=&\sum_{\tau\in S_n}\mathrm{sign}(\tau)\prod_{j=1}^n b_j^{\tau(j)-1}\sum_{\sigma\in S_n}\prod_{j=1}^n a_{\sigma(j)}^{\tau(j)-1}\\
=&\sum_{\tau\in S_n}\mathrm{sign}(\tau)\prod_{j=1}^n b_j^{\tau(j)-1}\sum_{\sigma\in S_n}\mathrm{sign}(\sigma\tau^{-1})\prod_{i=1}^n a_{\sigma\tau^{-1}(i)}^{i-1}\ (\text{as }-1=1\text{ in }F)\\
=&\|b_j^{i-1}\|_{1\leqslant i,j\leqslant n}\times\|a_j^{i-1}\|_{1\leqslant i,j\leqslant n}=\prod_{1\leqslant i<j\leqslant n}(a_j-a_i)(b_j-b_i)\neq 0.
\end{aligned}
$$

This concludes the proof. □

The following conjecture remains unsolved.

Snevily's Conjecture. *Let $a_1,\ldots,a_k\in\mathbb{Z}$, and let n be a positive integer greater than k. Then there is a permutation $\sigma\in S_k$ such that all the $i+a_{\sigma(i)}$ $(i=1,\ldots,k)$ modulo n are distinct.*

2. Nontrivial Problems and Results on Abelian Groups

Let G be an additive abelian group of order n, and let $b_1,\cdots,b_n\in G$. If both $\{a_i\}_{i=1}^n$ and $\{a_i+b_i\}_{i=1}^n$ are numberings of the elements of G, then $\sum_{i=1}^n(a_i+b_i)=\sum_{i=1}^n a_i$ and hence $b_1+\cdots+b_n=0$. In 1952 M. Hall [Proc. Amer. Math. Soc.] obtained the converse.

Theorem 2.1 (Hall's Theorem). *Let $G=\{a_1,\cdots,a_n\}$ be an additive abelian group, and let $b_1,\cdots,b_n$ be any elements of G with $b_1+\cdots+b_n=0$.*

Then there exists a permutation $\sigma \in S_n$ *such that* $a_{\sigma(1)} + b_1, \cdots, a_{\sigma(n)} + b_n$ *are distinct.*

Hall's proof is highly technical.

In 1999 H. S. Snevily made the following general conjecture:

Let G *be any additive abelian group with* $|G|$ *odd. Let* A *and* B *be subsets of* G *with cardinality* $n > 0$*. Then there is a numbering* $\{a_i\}_{i=1}^n$ *of the elements of* A *and a numbering* $\{b_i\}_{i=1}^n$ *of the elements of* B *such that* $a_1 + b_1, \cdots, a_n + b_n$ *are pairwise distinct.*

The proof of the following result in this direction involves linear algebra, field theory and Dirichlet's unit theorem in algebraic number theory

Theorem 2.2 (Z. W. Sun [J. Combin. Theory Ser. A, 2003])**.** *Let* G *be an additive abelian group whose finite subgroups are all cyclic. Let* $A_1, \cdots, A_n$ *be finite subsets of* G *with cardinality* $k > m(n-1)$ *(where* m *is a positive integer), and let* $b_1, \cdots, b_n$ *be elements of* G*.*

(i) *If* $b_1, \cdots, b_n$ *are distinct, then there are at least* $(k-1)n - m\binom{n}{2} + 1$ *multi-sets* $\{a_1, \cdots, a_n\}$ *such that* $a_i \in A_i$ *for* $i = 1, \cdots, n$ *and all the* $ma_i + b_i$ *are distinct.*

(ii) *The sets*

$$\{\{a_1, \cdots, a_n\} \colon a_i \in A_i,\ a_i \neq a_j \text{ and } ma_i + b_i \neq ma_j + b_j \text{ if } i \neq j\}$$

and

$$\{\{a_1, \cdots, a_n\} \colon a_i \in A_i,\ ma_i \neq ma_j \text{ and } a_i + b_i \neq a_j + b_j \text{ if } i \neq j\}$$

have more than $(k-1)n-(m+1)\binom{n}{2} \geqslant (m-1)\binom{n}{2}$ *elements, provided that* $b_1, \cdots, b_n$ *are distinct and of odd order, or they have finite order and* $n!$ *cannot be written in the form* $\sum_{p\in P} px_p$ *where all the* x_p *are nonnegative integers and* P *is the set of primes dividing one of the orders of* $b_1, \cdots, b_n$*.*

In the 1960's M. Knerser obtained the following remarkable theorem on abelian groups.

Theorem 2.3 (Kneser's Theorem)**.** *Let* G *be an additive abelian group. Let* A *and* B *be finite nonempty subsets of* G*, and let* $H = H(A+B)$ *be the stablizer* $\{g \in G:\ g+A+B = A+B\}$*. If* $|A+B| \leqslant |A|+|B|-1$*, then*

$$|A+B| = |A+H| + |B+H| - |H|.$$

The following consequence is an extension of the Cauchy-Davenport theorem.

Corollary 2.1. *Let* G *be an additive abelian group. Let* $p(G)$ *be the least order of a nonzero element of* G*, or* $p(G) = +\infty$ *if* G *is torsion-free. Then, for any finite nonempty subsets* A *and* B *of* G*, we have*

$$|A+B| \geqslant \min\{p(G), |A|+|B|-1\}.$$

Proof. Suppose that $|A+B| < |A|+|B|-1$. Then $H = H(A+B) \neq \{0\}$ by Kneser's theorem. Therefore $|H| \geqslant p(G)$ and hence

$$|A+B| = |A+H| + |B+H| - |H| \geqslant |A+H| \geqslant |H| \geqslant p(G).$$

We are done. $\square$

Quite recently G. Károlyi was able to extend the Erdős-Heilbronn conjecture to any abelian groups.

Theorem 2.4 (G. Károlyi [Israel J. Math. 2004]). *Let G be an additive abelian group. Then, for any finite nonempty subset A of G, we have*

$$|2^\wedge A| \geqslant \min\{p(G), 2|A| - 3\}.$$

The characteristic function of a residue class is a periodic arithmatical map. Dirichlet characters are also periodic functions. If an element a in an additive abelian group G has order n, then the map $\psi : \mathbb{Z} \to G$ given by $\psi(x) = xa$ is periodic mod n.

Theorem 2.5 (Z. W. Sun, 2004). *Let G be any additive abelian group, and let $\psi_1, \ldots, \psi_k$ be maps from $\mathbb{Z}$ to G with periods $n_1, \ldots, n_k \in \mathbb{Z}^+$ respectively. Then the function $\psi = \psi_1 + \cdots + \psi_k$ is constant if $\psi(x)$ equals a constant for $|T| \leqslant n_1 + \cdots + n_k - k + 1$ consecutive integers x, where*

$$T = \bigcup_{s=1}^{k} \left\{ \frac{r}{n_s} : r = 0, 1, \ldots, n_s - 1 \right\}.$$

The proof of Theorem 2.5 involves linear recurrences and algebraic integers.

Corollary 2.2 (Z. W. Sun [Math. Res. Lett. 11(2004)]). *The system $A = \{a_s (\bmod\ n_s)\}_{s=1}^{k}$ covers every integer exactly m times if it covers $|T|$ consecutive integers exactly m times, where T is as in Theorem 2.5.*

In 1966 J. Mycielski [Fund. Math.] posed an interesting conjecture on disjoint covers (i.e. partitions) of abelian groups. Before stating the conjecture we give a definition first.

Definition 2.1. The Mycielski function $f : \mathbb{Z}^+ = \{1, 2, \ldots\} \to \mathbb{N} = \{0, 1, 2, \ldots\}$ is given by

$$f(n) = \sum_{p \in P(n)} \mathrm{ord}_p(n)(p-1),$$

where $P(n)$ denotes the set of prime divisors of n and $\mathrm{ord}_p(n)$ represents largest integer α such that $p^\alpha \mid n$. In other words, $f(\prod_{t=1}^r p_t^{\alpha_t}) = \sum_{t=1}^r \alpha_t(p_t - 1)$ where $p_1, \ldots, p_r$ are distinct primes.

Mycielski's Conjecture. *Let G be an abelian group, and $\{a_s G_s\}_{s=1}^k$ be a disjoint cover of G by left cosets of subgroups. Then $k \geqslant 1 + f([G : G_t])$ for each $t = 1, \ldots, k$. (It is known that $[G : G_t] < \infty$ for all $t = 1, \ldots, k$.)*

Mycielski's conjecture was first confirmed by Š. Znám [Colloq. Math., 1966] in the case $G = \mathbb{Z}$.

Theorem 2.6 (G. Lettl and Z. W. Sun, 2004)**.** *Let $\mathcal{A} = \{a_s G_s\}_{s=1}^k$ be a cover of an abelian group G by left cosets of subgroups. Suppose that $\mathcal{A}$ covers all the elements of G at least m times with the coset $a_t G_t$ irredundant. Then $[G : G_t] \leqslant 2^{k-m}$ and furthermore $k \geqslant m + f([G : G_t])$.*

In the case $m = 1$ and $G_t = \{e\}$, this confirms a conjecture of W. D. Gao and A. Geroldinger [European J. Combin. 2003]. The proof of Theorem 2.6 involves algebraic number theory and characters of abelian groups.

Conjecture (Z. W. Sun, 2004). *Let $\mathcal{A} = \{a_sG_s\}_{s=1}^k$ be a finite system of left cosets of subgroups of an abelian group G. Suppose that $\mathcal{A}$ covers all the elements of G at least m times but none of its proper subsystems does. Then we have $k \geqslant m + f(N)$ where N is the least common multiple of the indices $[G : G_1], \ldots, [G : G_k]$.*

In 1961 P. Erdős, A. Ginzburg and A. Ziv [Bull. Research Council. Israel] established the following celebrated theorem which initiated the study of zero-sums.

Theorem 2.7 (The EGZ Theorem). *Let G be any additive abelian group of order n. For any given $c_1, \cdots, c_{2n-1} \in G$, there is an $I \subseteq \{1, \ldots, 2n-1\}$ with $|I| = n$ such that $\sum_{s\in I} c_s = 0$.*

In 2003 Z. W. Sun connected the EGZ theorem with covers of $\mathbb{Z}$.

Theorem 2.8 (Z. W. Sun [Electron. Res. Announc. AMS, 2003]). *Let $A = \{a_s(\text{mod } n_s)\}_{s=1}^k$ and suppose that $|\{1 \leqslant s \leqslant k : x \equiv a_s \pmod{n_s}\}| \in \{2q-1, 2q\}$ for all $x \in \mathbb{Z}$, where q is a prime power. Let G be an additive abelian group of order q. Then, for any $c_1, \ldots, c_k \in G$, there exists an $I \subseteq \{1, \ldots, k\}$ such that $\sum_{s\in I} 1/n_s = q$ and $\sum_{s\in I} c_s = 0$.*

Definition 2.2. The Davenport constant $D(G)$ of a finite abelian group G (written additively) is defined as the smallest positive integer k such that any sequence $\{c_s\}_{s=1}^k$ (repetition allowed) of elements of G has a nonempty subsequence $c_{i_1}, \cdots, c_{i_l}$ $(i_1 < \cdots < i_l)$ with zero-sum (i.e. $c_{i_1} + \cdots + c_{i_l} = 0$).

For any abelian group G of order n we clearly have $D(G) \leqslant n$. In fact, if $c_1, \ldots, c_n \in G$, then the partial sums

$$s_0 = 0,\ s_1 = a_1,\ s_2 = a_1 + a_2,\ \ldots,\ s_n = a_1 + \cdots + a_n$$

cannot be distinct since $n + 1 > |G|$, so there are $0 \leqslant i < j \leqslant n$ such that $s_i = s_j$, i.e. $a_{i+1} + \cdots + a_j = 0$.

In 1966 Davenport showed that if K is an algebraic number field with ideal class group G, then $D(G)$ is the maximal number of prime ideals (counting multiplicity) in the decomposition of an irreducible integer in K.

In 1969 J. Olson [J. Number Theory] used the knowledge of group rings to show that the Davenport constant of an abelian p-group $G \cong \mathbb{Z}_{p^{h_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{h_l}}$ is $1 + \sum_{t=1}^{l}(p^{h_t} - 1)$.

In 1994 W. R. Alford, A. Granville and C. Pomerance [Ann. Math.] employed an upper bound for the Davenport constant of the unit group of the ring $\mathbb{Z}_n$ to prove that there are infinitely many Carmichael numbers which are those composites m such that $a^{m-1} \equiv 1 \pmod{m}$ for any $a \in \mathbb{Z}$ with $(a, m) = 1$.

The following well-known conjecture is still open, it is known to be true for $k = 1, 2$.

Olson's Conjecture. *Let k and n be positive integers. Then $D(\mathbb{Z}_n^k) = 1 + k(n-1)$ where $\mathbb{Z}_n^k$ is the direct sum of k copies of $\mathbb{Z}_n$.*

3. Nontrivial Problems and Results on General Groups

Let G be a group and $G_1, \cdots, G_k$ be subgroups of G. Let $a_1, \cdots, a_k \in$

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.

Theorem 3.1. *Let $\mathcal{A} = \{a_iG_i\}_{i=1}^k$ be a finite system of left cosets in a group G where $G_1, \ldots, G_k$ are subgroups of G. Suppose that $\mathcal{A}$ forms a minimal cover G (i.e. $\mathcal{A}$ covers all the elements of G but none of its proper systems does).*

(i) (B. H. Neumann [Publ. Math. Debrecen, 1954]) *There is a constant c_k depending only on k such that $[G : G_i] \leqslant c_k$ for all $i = 1, \ldots, k$.*

(ii) (M. J. Tomkinson [Comm. Algebra, 1987]) We have $[G : \bigcap_{i=1}^k G_i] \leqslant k!$ where the upper bound $k!$ is best possible.

Proof. We prove (ii) by induction. (Part (ii) is stronger than part (i).)

We want to show that

$$\Big[\bigcap_{i\in I} G_i : \bigcap_{i=1}^k G_i\Big] \leqslant (k - |I|)! \qquad (*_I)$$

for all $I \subseteq \{1, \ldots, k\}$, where $\bigcap_{i\in\emptyset} G_i$ is regarded as G.

Clearly $(*_I)$ holds for $I = \{1, \ldots, k\}$.

Now let $I \subset \{1, \ldots, k\}$ and assume $(*_J)$ for all $J \subseteq \{1, \ldots, k\}$ with $|J| > |I|$. Since $\{a_iG_i\}_{i\in I}$ is not a cover of G, there is an $a \in G$ not covered by $\{a_iG_i\}_{i\in I}$. Clearly $a(\bigcap_{i\in I} G_i)$ is disjoint from the union $\bigcup_{i\in I} a_iG_i$ and hence contained in $\bigcup_{j\notin I} a_jG_j$. Thus

$$a\Big(\bigcap_{i\in I} G_i\Big) = \bigcup_{\substack{j\notin I \\ a_jG_j\cap a(\bigcap_{i\in I} G_i)\neq\emptyset}} \Big(a_jG_j \cap a\Big(\bigcap_{i\in I} G_i\Big)\Big)$$

and hence

$$\left[\bigcap_{i\in I} G_i : H\right] \leqslant \sum_{j\notin I}\left[G_j \cap \bigcap_{i\in I} G_i : H\right] \leqslant \sum_{j\notin I}(k-(|I|+1))! = (k-|I|)!$$

where $H=\bigcap_{i=1}^k G_i$. This concludes the induction proof. $\square$

Definition 3.1. Let H be a subnormal subgroup of a group G with finite index, and

$$H_0 = H \subset H_1 \subset \cdots \subset H_n = G$$

be a composition series from H to G (i.e. H_i is maximal normal in H_{i+1} for each $0 \leqslant i < n$). If the length n is zero (i.e. $H=G$), then we set $d(G,H)=0$, otherwise we put

$$d(G,H)=\sum_{i=0}^{n-1}([H_{i+1}:H_i]-1).$$

Let H be a subnormal subgroup of a group G with $[G:H]<\infty$. By the Jordan–Hölder theorem, $d(G,H)$ does not depend on the choice of the composition series from H to G. Clearly $d(G,H)=0$ if and only if $H=G$. If K is a subnormal subgroup of H with $[H:K]<\infty$, then

$$d(G,H)+d(H,K)=d(G,K).$$

When H is normal in G, the 'distance' $d(G,H)$ was first introduced by I. Korec [Fund. Math. 1974]. The current general notion is due to Z. W. Sun [Fund. Math. 1990]. Z. W. Sun [Fund. Math. 1990] showed that

$$[G:H]-1 \geqslant d(G,H) \geqslant f([G:H]) \geqslant \log_2[G:H]$$

where f is the Mycielski function. Moreover, Sun [European J. Combin. 2001] noted that $d(G,H) = f([G:H])$ if and only if G/H_G is solvable where $H_G = \bigcap_{g\in G} gHg^{-1}$ is the largest normal subgroup of G contained in H.

In 1968 Š. Znam [Coll. Math. Soc. János Bolyai] made the following further conjecture: *If $A = \{a_s(n_s)\}_{s=1}^k$ is a disjoint cover of $\mathbb{Z}$ then*

$$k \geqslant 1 + f(N_A) \quad \textit{and hence } N_A \leqslant 2^{k-1},$$

where $N_A = [n_1, \ldots, n_k] = [\mathbb{Z} : \bigcap_{s=1}^k n_s\mathbb{Z}]$.

In 1974 I. Korec [Fund. Math.] confirmed Znaám's conjecture and Mycielski's conjecture by proving the following deep result: *Let $\{a_iG_i\}_{i=1}^k$ be a partition of a group into left cosets of normal subgroups. Then $k \geqslant 1 + f([G : \bigcap_{i=1}^k G_i])$.*

Here is a further extension of Korec's result.

Theorem 3.2 (Z. W. Sun [European J. Combin. 22(2001)]). *Let G be a group and $\{a_iG_i\}_{i=1}^k$ cover each elements of G exactly m times, where $G_1, \ldots, G_k$ are subnormal subgroups of G. Then*

$$k \geqslant m + d\Big(G, \bigcap_{i=1}^k G_i\Big),$$

where the lower bound can be attained. Moreover, for any subgroup K of G not contained in all the G_i we have

$$|\{1 \leqslant i \leqslant k : K \not\subseteq G_i\}| \geqslant 1 + d\Big(K, K \cap \bigcap_{i=1}^k G_i\Big).$$

Corollary 3.1 (Z. W. Sun [Fund. Math. 1990]). *Let H be a subnormal subgroup of a group G with $[G:H]<\infty$. Then*

$$[G:H]\geqslant 1+d(G,H_G)\geqslant 1+f([G:H_G]) \text{ and hence } [G:H_G]\leqslant 2^{[G:H]-1}.$$

Proof. Let $\{Ha_i\}_{i=1}^k$ be a right coset decomposition of G where $k=[G:H]$. Then $\{a_iG_i\}_{i=1}^k$ is a disjoint cover of G where all the $G_i=a_i^{-1}Ha_i$ are subnormal in G. Observe that

$$\bigcap_{i=1}^k G_i=\bigcap_{i=1}^k\bigcap_{h\in H}a_i^{-1}h^{-1}Hha_i=\bigcap_{g\in G}g^{-1}Hg=H_G.$$

So the desired result follows from Theorem 3.2. □

Theorem 3.3. (i) (Berger-Felzenbaum-Fraenkel, 1988, Coll. Math.) *If $\{a_iG_i\}_{i=1}^k$ is a disjoint cover of a finite solvable group G, then $k\geqslant 1+f([G:G_i])$ for $i=1,\cdots,k$.*

(ii) [Z. W. Sun, European J. Combin. 2001] *Let G be a group and $\{a_iG_i\}_{i=1}^k$ be a finite system of left cosets which covers each elements of G exactly m times. For any $i=1,\leqslant,k$, whenever $G/(G_i)_G$ is solvable we have $k\geqslant m+f([G:G_i])$ and hence $[G:G_i]\leqslant 2^{k-m}$.*

Z. W. Sun [European J. Combin. 2001] suggested the following further conjecture.

Conjecture 3.1 (Z. W. Sun, 2001). *Let $a_1G_1,\ldots,a_kG_k$ be left cosets of a group G such that $\{a_iG_i\}_{i=1}^k$ covers each elements of G exactly m times and that all the $G/(G_i)_G$ are solvable. Then $k\geqslant m+f(N)$ where N is the least common multiple of the indices $[G:G_1],\cdots,[G:G_k]$.*

If $\{x_1, \ldots, x_k\}$ is a maximal subset of a group G with $x_ix_j \neq x_jx_i$ for all $1 \leqslant i < j \leqslant k$, then $\{C_G(x_i)\}_{i=1}^k$ is a minimal cover of G with $\bigcap_{i=1}^k C_G(x_i) = Z(G)$ (Tomkinson, Comm. Algebra, 1987) and $|G/Z(G)| \leqslant c^k$ for some absolute constant (L. Pyber, J. London Math. Soc., 1987).

Conjecture 3.2 (Z. W. Sun, 1996). *Let $\{G_i\}_{i=1}^k$ be a minimal cover of a group G by subnormal subgroups. Write $[G : \bigcap_{i=1}^k G_i] = \prod_{t=1}^r p_t^{\alpha_t}$, where $p_1, \ldots, p_r$ are distinct primes and $\alpha_1, \ldots, \alpha_r$ are positive integers. Then we have*

$$k \geqslant 1 + \sum_{t=1}^{r} (\alpha_t - 1)p_t.$$

Up to now, no counterexample to this conjecture has been found.

The following conjecture extends a conjecture of P. Erdős.

The Herzog-Schönheim Conjecture ([Canad. Math. Bull. 1974]). *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 $G_1, \cdots, G_k$. Then the indices $n_1 = [G : G_1], \cdots, n_k = [G : G_k]$ cannot be pairwise distinct.*

M. A. Berger, A. Felzenbaum and A. S. Fraenkel [1986, Canad. Math. Bull.; 1987, Fund. Math.] showed the conjecture for finite nilpotent groups and supersolvable groups. A quite recent progress was made by the speaker.

Theorem 3.4 (Z. W. Sun [J. Algebra, 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 number of times, and

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

Then the indices $n_1, \cdots, n_k$ cannot be distinct. Moreover, if each index occurs in $n_1, \cdots, n_k$ 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 $\gamma = 0.577\cdots$ is the Euler constant and the O-constant is absolute.

The above theorem also answers a question analogous to a famous problem of Erdős negatively. Theorem 3.4 was established by a combined use of tools from group theory and number theory.

One of the key lemmas is the following one which is the main reason why covers involving subnormal subgroups are better behaved than general covers.

Lemma 3.1 (Z. W. Sun [European J. Combin. 2001])**.** *Let G be a group, and let $P(n)$ denote the set of prime divisors of a positive integer n.*

(i) *If $G_1, \ldots, G_k$ are subnormal subgroups of G with finite index, then $\left[G : \bigcap_{i=1}^{k} G_i\right] \mid \prod_{i=1}^{k} [G : G_i]$ and hence $P\left(\left[G : \bigcap_{i=1}^{k} G_i\right]\right) = \bigcup_{i=1}^{k} P([G : G_i])$.*

(ii) *Let H be a subnormal subgroup of G with finite index. Then*

$$P(|G/H_G|) = P([G : H]).$$

We mention that part (ii) is a consequence of the first part, and the word "*subnormal*" cannot be removed from part (i).

Here is another useful lemma.

Lemma 3.2 (Z. W. Sun [J. Algebra, 2004]). *Let G be a group and H its subgroup with finite index N. Let $a_1, \ldots, a_k \in G$, and let $G_1, \ldots, G_k$ be subnormal subgroups of G containing H. Then $\bigcup_{i=1}^k a_i G_i$ contains at least $|\bigcup_{i=1} 0(n_i) \cap \{0, 1, \ldots, N-1\}|$ left cosets of H, where $n_i = [G : G_i]$.*

Finally we pose an interesting unsolved conjecture.

Conjecture 3.3 (Z. W. Sun). *Let G be a group, and $a_1 G_1, \ldots, a_k G_k$ be pairwise disjoint left cosets of G with all the indices $[G : G_i]$ finite. Then, for some $1 \leqslant i < j \leqslant k$ we have $\gcd([G : G_i], [G : G_j]) \geqslant k$.*

This conjecture is open even in the special case $G = \mathbb{Z}$.