A talk given at the 19th Annual International Conference
on Formal Power Series and Algebraic Combin. (Tianjin, July 4, 2007)

AN ADDITIVE THEOREM RELATED TO LATIN TRANSVERSALS

Zhi-Wei Sun

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

1. Hall's Theorem and Snevily's Conjecture

Let $n \in \mathbb{Z}^+ = \{1, 2, 3, \dots\}$. Any cyclic group of order n is isomorphic to the additive group $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ of residue classes modulo n. If n is odd, then

$$1+1,\ 2+2,\ \dots,\ n+n$$

are pairwise incongruent modulo n and hence they form a complete system of residues modulo n.

Let $a_1, \dots, a_n \in \mathbb{Z}$. If $a_1 + 1, \dots, a_n + n$ form a complete system of residues modulo n, then

$$\sum_{i=1}^{n}(a_i + i) \equiv 1 + \cdots + n \pmod{n}$$

and hence $\sum_{i=1}^{n} a_i \equiv 0 \pmod{n}$.

Cramer's Conjecture. *Let $a_1, \dots, a_n$ be integers with*

$$a_1 + \cdots + a_n \equiv 0 \pmod{n}.$$

Then there is a permutation $\sigma \in S_n$ such that $a_{\sigma(1)} + 1, \dots, a_{\sigma(n)} + n$ form a complete system of residues modulo n.

In 1952 M. Hall [Proc. Amer. Math. Soc.] obtained an extension of Cramer's conjecture.

M. Hall's theorem. *Let $G = \{b_1, \dots, b_n\}$ be an additive abelian group, and let $a_1, \dots, a_n$ be elements of G with $a_1 + \cdots + a_n = 0$. Then there exists a permutation $\sigma \in S_n$ such that $\{a_{\sigma(1)} + b_1, \dots, a_{\sigma(n)} + b_n\} = G$.*

Observation. If $a_1, \dots, a_n \in \mathbb{Z}$ are incongruent modulo n with $a_1 + \cdots + a_n \equiv 0 \pmod{n}$, then n divides $0 + 1 + \cdots + (n-1) = n(n-1)/2$ and hence n is *odd*.

Motivated by M. Hall's theorem and the above observation, in 1999 H. Snevily [Amer. Math. Monthly] raised the following nice conjecture.

Snevily's Conjecture. *Let G be an additive abelian group with $|G|$ odd. Let A and B be subsets of G with cardinality $n \in \mathbb{Z}^+$. 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 the sums $a_1 + b_1, \dots, a_n + b_n$ are distinct.*

Note that an abelian group of even order has an element g of order 2 and hence we don't have the described result for $A = B = \{0, g\}$.

In our opinion, Snevily's conjecture belongs to the central part of combinatorial number theory due to its **simplicity and beauty**.

After your serious attempt to prove Snevily's conjecture, you will realize that the conjecture is very sophisticated and challenging.

Let M be an $n \times n$ matrix. A *line* of M is a row or a column of M. M is called a *Latin square* over a set S of cardinality n if all its entries come from the set S and no line of which contains an element more than once. A *transversal* of the matrix M is a collection of n cells no two of which lie in the same line. A *Latin transversal* of M is a transversal whose cells contain no repeated element.

If $G = \{a_1, \ldots, a_n\}$ is an additive group, then the matrix $M = (a_i + a_j)_{1 \leqslant i,j \leqslant n}$ formed by the Cayley addition table is a Latin square over G.

Another Form of Snevily's Conjecture. *Let $G = \{a_1, \ldots, a_N\}$ be an additive abelian group with $|G| = N$ odd, and let M be the Latin square $(a_i + a_j)_{1 \leqslant i,j \leqslant N}$ formed by the Cayley addition table. Then any $n \times n$ submatrix of M contains a Latin transversal.*

In 1967 H. J. Ryser conjectured that every Latin square of *odd* order has a Latin transversal. Another conjecture of Brualdi states that every Latin square of order n has a partial Latin transversal of size $n-1$. These conjectures remain open.

2. Snevily's Conjecture for $\mathbb{Z}_p$

In 2000 N. Alon [Israel J. Math.] was able to prove Snevily's conjecture for $\mathbb{Z}_p$ with p an odd prime, via the following powerful tool.

Combinatorial Nullstellensatz (Alon, 1999). *Let $A_1, \ldots, A_n$ be finite subsets of a field F with $|A_i| > k_i \geqslant 0$ for $i = 1, \ldots, n$. If the total degree of $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ is $k_1 + \cdots + k_n$ and the coefficient of the monomial $x_1^{k_1} \cdots x_n^{k_n}$ in $f(x_1, \ldots, x_n)$ is nonzero, then $f(a_1, \ldots, a_n) \neq 0$ for some $a_1 \in A_1, \ldots, a_n \in A_n$.*

Alon made use of the fact that $\mathbb{Z}_p$ **is a field when** p **is an odd prime.**

Theorem 1 (N. Alon, 2000). *Let p be an odd prime and let $b_1, \ldots, b_n \in \mathbb{Z}_p$ with $n < p$. If $a_1, \ldots, a_n \in \mathbb{Z}_p$ are distinct, then there is $\sigma \in S_n$ such that $a_{\sigma(1)} + b_1, \ldots, a_{\sigma(n)} + b_n$ are distinct.*

Proof. Let $A_1, \ldots, A_n$ be the set $A = \{a_1, \ldots, a_n\}$ of cardinality n. We want to find distinct $x_1 \in A_1, \ldots, x_n \in A_n$ such that $x_1 + b_1, \ldots, x_n + b_n$ are distinct. In view of the Combinatorial Nullstellensatz, it suffices to note that

$$\begin{aligned}
&[x_1^{n-1}\cdots x_n^{n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(x_j+b_j-x_i-b_i)\\
=&[x_1^{n-1}\cdots x_n^{n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^2\\
=&[x_1^{n-1}\cdots x_n^{n-1}](-1)^{\binom{n}{2}}|x_i^{n-j}|_{1\leqslant i,j\leqslant n}|x_i^{j-1}|_{1\leqslant i,j\leqslant n}\\
=&[x_1^{n-1}\cdots x_n^{n-1}](-1)^{\binom{n}{2}}\sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{i=1}^{n}x_i^{n-\sigma(i)}\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{i=1}^{n}x_i^{\tau(i)-1}\\
=&(-1)^{\binom{n}{2}}\sum_{\sigma\in S_n}\varepsilon(\sigma)^2e=(-1)^{\binom{n}{2}}n!e\neq 0\ \ (\text{since } n<p),
\end{aligned}$$

where $\varepsilon(\sigma)$ denotes the sign of $\sigma\in S_n$ which is 1 or -1 according as σ is even or odd, and e stands for the multiplicative identity of the field $F=\mathbb{Z}_p$.

Remark 1. (a) For an odd composite number $n>0$, we cannot use Alon's idea to prove Snevily's conjecture for the additive cyclic group $\mathbb{Z}_n$ since $\mathbb{Z}_n$ is not a field. (b) In Alon's proof of Theorem 1, it does not matter whether $b_1,\dots,b_n$ are distinct or not.

3. Snevily's Conjecture for $\mathbb{Z}_n$ with n odd

In 2001 Dasgupta, Károlyi, Serra and Szegedy [Israel J. Math.] succeeded in proving Snevily's conjecture for cyclic groups of odd order. Their first important observation is that **a cyclic group of odd order n can be viewed as a subgroup of the multiplicative group of a field of characteristic 2**.

Theorem 2 (Dasgupta, Károlyi, Serra and Szegedy, 2001)**.** *Let G be a cyclic group of odd order m. If $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$ are two subsets of G with cardinality n. Then, for some $\sigma \in S_n$, the sums $a_{\sigma(1)} + b_1, \ldots, a_{\sigma(n)} + b_n$ are distinct.*

Proof. As $2^{\varphi(m)} \equiv 1 \pmod{m}$, the multiplicative group of the finite field F with order $2^{\varphi(m)}$ has a cyclic subgroup of order m which is isomorphic to G. Thus, we may simply view G as a subgroup of the multiplicative group $F^* = F \setminus \{0\}$.

In light of the Combinatorial Nullstellensatz, it suffices to show that

$$c := [x_1^{n-1} \cdots x_n^{n-1}] \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)(b_j x_j - b_i x_i) \neq 0.$$

c depends on $b_1, \ldots, b_n$ so that the condition $\prod_{1 \leqslant i < j \leqslant n}(b_j - b_i) \neq 0$ might be helpful.

Observe that

$$\prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)(b_j x_j - b_i x_i) = (-1)^{\binom{n}{2}} |x_i^{n-j}|_{1 \leqslant i,j \leqslant n} |b_i^{j-1} x_i^{j-1}|_{1 \leqslant i,j \leqslant n}$$

$$= (-1)^{\binom{n}{2}} \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_i^{n-\sigma(i)} \sum_{\tau \in S_n} \varepsilon(\tau) \prod_{i=1}^{n} b_i^{\tau(i)-1} x_i^{\tau(i)-1}.$$

Therefore

$$\begin{aligned}(-1)^{\binom{n}{2}}c =& \sum_{\sigma\in S_n} \varepsilon(\sigma)^2 \prod_{i=1}^{n} b_i^{\sigma(i)-1} = \operatorname{per}((b_i^{j-1})_{1\leqslant i,j\leqslant n}) \\ =& \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} b_i^{\sigma(i)-1} \quad (\text{because } \operatorname{ch}(F)=2) \\ =& |b_j^{i-1}|_{1\leqslant i,j\leqslant n} = \prod_{1\leqslant i<j\leqslant n} (b_j - b_i) \neq 0 \text{ (Vandermonde)}.\end{aligned}$$

In 2003 Sun [J. Combin. Theory Ser. A] obtained some further extensions of the Dasgupta-Károlyi-Serra-Szegedy result via restricted sums in a field. Here are two basic observations of Sun:

(1) Any finitely generated abelian group with the torsion subgroup

$$\operatorname{Tor}(G) = \{g \in G : \ g \text{ has a finite order}\}$$

cyclic is isomorphic to a subgroup of the multiplicative group of nonzero complex numbers.

(2) In Theorem 2, instead of the condition that $|G|$ is odd, we may just require that all elements of B have odd order.

In 2004 W. D. Gao and D. J. Wang [Israel J. Math.] studied Snevily's conjecture for abelian p-groups by using the DKSS method and group rings.

Snevily's conjecture for elementarily abelian groups $\mathbb{Z}_p^k$ remains open.

4. The speaker's New Discovery

Let $b_1,\ldots,b_n$ be elements of a field F. In Section 3, we noted that

$$[x_1^{n-1}\cdots x_n^{n-1}]|(b_ix_i)^{j-1}|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)$$
$$=(-1)^{\binom n2}\mathrm{per}((b_i^{j-1})_{1\leqslant i,j\leqslant n}).$$

Similarly,

$$[x_1^{n-1}\cdots x_n^{n-1}]\mathrm{per}((b_ix_i)^{j-1})_{1\leqslant i,j\leqslant n})\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)$$
$$=(-1)^{\binom n2}\det((b_i^{j-1})_{1\leqslant i,j\leqslant n})=(-1)^{\binom n2}\prod_{1\leqslant i<j\leqslant n}(b_j-b_i).$$

Theorem 3 (Sun, 2006)**.** *Let A, B and $C=\{c_1,\ldots,c_n\}$ be three subsets of a field F with cardinality n. 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 $a_1b_1c_1,\ldots,a_nb_nc_n$ are distinct.*

Proof. Since

$$[x_1^{n-1}\cdots x_n^{n-1}]\mathrm{per}((c_ix_i)^{j-1})_{1\leqslant i,j\leqslant n})\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)$$
$$=(-1)^{\binom n2}\prod_{1\leqslant i<j\leqslant n}(c_j-c_i)\neq 0,$$

by the Combinatorial Nullstellensatz there are distinct $b_1,\ldots,b_n\in B$ such that $\mathrm{per}(((b_ic_i)^{j-1})_{1\leqslant i,j\leqslant n})\neq 0$. As

$$[x_1^{n-1}\cdots x_n^{n-1}]|(b_ic_ix_i)^{j-1}|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)$$
$$=(-1)^{\binom n2}\mathrm{per}(((b_ic_i)^{j-1})_{1\leqslant i,j\leqslant n})\neq 0,$$

by the Combinatorial Nullstellensatz there are distinct $a_1, \ldots, a_n \in A$ such that

$$|(a_i b_i c_i)^{j-1}|_{1\leqslant i,j\leqslant n} = \prod_{1\leqslant i<j\leqslant n} (a_j b_j c_j - a_i b_i c_i) \neq 0.$$

We can restate Theorem 3 in the following form.

Theorem 4. *Let G be any additive abelian group with cyclic torsion subgroup, and let $A_1, \ldots, A_m$ be arbitrary subsets of G with cardinality $n \in \mathbb{Z}^+$, where m is odd. Then the elements of A_i $(1 \leqslant i \leqslant m)$ can be listed in a suitable order $a_{i1}, \ldots, a_{in}$, so that all the sums $\sum_{i=1}^{m} a_{ij}$ $(1 \leqslant j \leqslant n)$ are distinct. In other words, for a certain subset A_{m+1} of G with $|A_{m+1}| = n$, there is a matrix $(a_{ij})_{1\leqslant i\leqslant m+1,\, 1\leqslant j\leqslant n}$ such that $\{a_{i1}, \ldots, a_{in}\} = A_i$ for all $i = 1, \ldots, m+1$ and the column sum $\sum_{i=1}^{m+1} a_{ij}$ vanishes for every $j = 1, \ldots, n$.*

Remark 2. (1) In Theorem 4 we don't assume that $|G|$ is odd.

(2) Theorem 4 in the case $m = 3$ is essential; the result for $m = 5, 7, \ldots$ can be obtained by repeated use of the case $m = 3$.

Example 1. *The group G in Theorem 4 cannot be replaced by an arbitrary abelian group.* To illustrate this, we look at the Klein quaternion group

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$$

and its subsets

$$A_1 = \{(0,0), (0,1)\},\ A_2 = \{(0,0), (1,0)\},\ A_3 = \cdots = A_m = \{(0,0), (1,1)\},$$

where $m \geqslant 3$ is odd. For $i = 1, \ldots, m$ let a_i, a_i' be a list of the two elements of A_i, then

$$\sum_{i=1}^{m}(a_i + a_i') = (0,1) + (1,0) + (m-2)(1,1) = (0,0)$$

and hence $\sum_{i=1}^m a_i = -\sum_{i=1}^m a_i' = \sum_{i=1}^m a_i'$.

Recall that a line of an $n \times n$ matrix is a row or column of the matrix. We define a line of an $n \times n \times n$ cube in a similar way. A *Latin cube* over a set S of cardinality n is an $n \times n \times n$ cube whose entries come from the set S and no line of which contains a repeated element. A *transversal* of an $n \times n \times n$ cube is a collection of n cells no two of which lie in the same line. A *Latin transversal* of a cube is a transversal whose cells contain no repeated element.

Corollary 1. *Let N be any positive integer. For the $N \times N \times N$ Latin cube over $\mathbb{Z}/N\mathbb{Z}$ formed by the Cayley addition table, each $n \times n \times n$ subcube with $n \leqslant N$ contains a Latin transversal.*

Conjecture 1 (Sun, 2006)**.** *Every $n \times n \times n$ Latin cube contains a Latin transversal.*

Note that Conjecture 1 does not imply Theorem 3 since an $n \times n \times n$ subcube of a Latin cube might have more than n distinct entries.

In Theorem 4 the condition $2 \nmid m$ is indispensable. Let G be an additive cyclic group of even order n. Then G has a unique element g of order 2 and hence $a \neq -a$ for all $a \in G \setminus \{0, g\}$. Thus $\sum_{a \in G} a = 0 + g = g$. For each $i = 1, \dots, m$ let $a_{i1}, \dots, a_{in}$ be a list of the n elements of G. If those $\sum_{i=1}^m a_{ij}$ with $1 \leqslant j \leqslant n$ are distinct, then

$$\sum_{a\in G} a = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij} = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} = m\sum_{a\in G} a,$$

hence $(m-1)g = (m-1)\sum_{a\in G} a = 0$ and therefore m is odd.

Combining Theorem 4 with [Su03, Theorem 1.1(ii)], we obtain the following consequence.

Corollary 2. *Let G be any additive abelian group with cyclic torsion subgroup, and let $A_1, \dots, A_m$ be subsets of G with cardinality $n \in \mathbb{Z}^+$, where m is even. Suppose that all the elements of A_m have odd order. Then the elements of A_i $(1 \leqslant i \leqslant m)$ can be listed in a suitable order $a_{i1}, \dots, a_{in}$, so that all the sums $\sum_{i=1}^m a_{ij}$ $(1 \leqslant j \leqslant n)$ are distinct.*

As an essential result, Theorem 3 or 4 might have various potential applications in additive number theory and combinatorial designs.

A direct proof of Theorem 4 involves the following lemma.

Lemma 1. *Let R be a commutative ring with identity, and let $a_{ij} \in R$ for $i = 1, \dots, m$ and $j = 1, \dots, n$, where $m \in \{3, 5, \dots\}$. The we have the identity*

$$\sum_{\sigma_1,\dots,\sigma_{m-1}\in S_n} \varepsilon(\sigma_1\cdots\sigma_{m-1}) \prod_{1\leqslant i<j\leqslant n}\left(a_{mj}\prod_{s=1}^{m-1} a_{s\sigma_s(j)} - a_{mi}\prod_{s=1}^{m-1} a_{s\sigma_s(i)}\right)$$
$$= \prod_{1\leqslant i<j\leqslant n}(a_{1j}-a_{1i})\cdots(a_{mj}-a_{mi}).$$

We can extend Theorem 4 via restricted sumsets in a field. The additive order of the multiplicative identity of a field F is either infinite or a prime;

we call it the *characteristic* of F and denote it by $\mathrm{ch}(F)$. There are various results on restricted sumsets of the type

$$\{a_1+\cdots+a_n:\ a_1\in A_1,\ldots,a_n\in A_n \text{ and } P(a_1,\ldots,a_n)\neq 0\},$$

where $A_1,\ldots,A_n\subseteq F$ and $P(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n]$. See, e.g., Alon-Nathanson-Ruzsa [J. Number Theory, 1996], Qing-Hu Hou and Z. W. Sun [Acta Arith. 2002], Z. W. Sun [J. Combin. Theory, 2003], H. Pan and Z.W. Sun [Israel J. Math. 2006].

Theorem 5. *Let k,m,n be positive integers with $k-1\geqslant m(n-1)$, and let F be a field with $\mathrm{ch}(F)>\max\{mn,(k-1-m(n-1))n\}$. Assume that $c_1,\ldots,c_n\in F$ are distinct, and $A_1,\ldots,A_n,B_1,\ldots,B_n$ are subsets of F with $|A_1|=\cdots=|A_n|=k$ and $|B_1|=\cdots=|B_n|=n$. Let $S_{ij}\subseteq F$ with $|S_{ij}|<2m$ for all $1\leqslant i<j\leqslant n$. Then there are distinct $b_1\in B_1,\ldots,b_n\in B_n$ such that the restricted sumset*

$$S=\{a_1+\cdots+a_n:\ a_i\in A_i,\ a_i-a_j\notin S_{ij} \text{ and } a_ib_ic_i\neq a_jb_jc_j \text{ if } i<j\}$$

has at least $(k-1-m(n-1))n+1$ elements.

When $k=n$, $m=1$ and $S_{ij}=\{0\}$, Theorem 5 yields Theorem 3 or 4.

Now we state another extension of Theorem 4.

Theorem 6. *Let G be an additive abelian group with cyclic torsion subgroup. Let h, k, l, m, n be positive integers with $k-1 \geqslant m(n-1)$ and $l-1 \geqslant h(n-1)$. Assume that $c_1, \ldots, c_n \in G$ are distinct, and $A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ are subsets of G with $|A_1| = \cdots = |A_n| = k$ and $|B_1| = \cdots = |B_n| = l$. Then, for any sets S and T with $|S| \leqslant (k-1)n-(m+1)\binom{n}{2}$ and $|T| \leqslant (l-1)n-(h+1)\binom{n}{2}$, there are $a_1 \in A_1, \ldots, a_n \in A_n, b_1 \in B_1, \ldots, b_n \in B_n$ such that $\{a_1, \ldots, a_n\} \notin S$, $\{b_1, \ldots, b_n\} \notin T$, and also*

$$a_i + b_i + c_i \neq a_j + b_j + c_j,\ ma_i \neq ma_j,\ hb_i \neq hb_j \quad \textit{if } 1 \leqslant i < j \leqslant n.$$

Theorem 3 follows from Theorem 6 in the case $k = l = n$, $h = m = 1$ and $S = T = \emptyset$.

The speaker's results in this talk are contained in a paper available from `http://arxiv.org/abs/math.CO/0610981` or the speaker's homepage `http://math.nju.edu.cn/~zwsun`.

The topic here involves combinatorics as well as number theory and algebra. I do like such problems which are not of pure combinatorial interest.