# Some Sophisticated Applications of the Combinatorial Nullstellensatz

Zhi-Wei Sun

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

Feb. 6, 2010

# Part I.

# The Strong Form of the Combinatorial Nullstellensatz and its Proof

# Usual form of Alon's Combinatorial Nullstellensatz

**Usual Form of the Combinatorial Nullstellensatz (CN)** [Combin. Probab. Comput. 8(1999)]. Let $A_1, \ldots, A_n$ be finite nonempty subsets of a field $F$ and let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$. Suppose that $0 \leqslant k_i < |A_i|$ for $i = 1, \ldots, n$, $k_1 + \cdots + k_n = \deg f$ and

$$[x_1^{k_1} \cdots x_n^{k_n}] f(x_1, \ldots, x_n) \text{ (the coefficient of } x_1^{k_1} \cdots x_n^{k_n} \text{ in } f)$$

does not vanish. Then there are $a_1 \in A_1, \ldots, a_n \in A_n$ such that $f(a_1, \ldots, a_n) \neq 0$.

**Advantage**: This advanced algebraic tool enables us to establish existence via computation. It has many applications.

# Strong form of the Combinatorial Nullstellensatz

**Strong Form of the Combinatorial Nullstellensatz** [Alon, Combin. Probab. Comput. 8(1999)]. Let $A_1, \ldots, A_n$ be finite nonempty subsets of a field $F$ and let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$. Set $g_i(x) = \prod_{a \in A_i}(x - a)$ for $i = 1, \ldots, n$. Then

$$f(a_1, \ldots, a_n) = 0 \ \text{ for all } a_1 \in A_1, \ldots, a_n \in A_n$$

if and only if there are

$$h_1(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$$

with $\deg h_i \leqslant \deg f - \deg g_i$ for $i = 1, \ldots, n$, such that

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} g_i(x_i) h_i(x_1, \ldots, x_n).$$

**Remark**: Let $I$ be the ideal of $F[x_1, \ldots, x_n]$ generated by $g_1(x_1), \ldots, g_n(x_n)$. Then the strong form of CN tells us that $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ vanishes on $Z(I) = A_1 \times \cdots \times A_n$ if and only if $f \in I$, where

$$Z(I) = \{(x_1, \ldots, x_n) \in F^n : \ P(x_1, \ldots, x_n) = 0 \text{ for all } P \in I\}.$$

# Strong Form implies the Usual Form

Suppose that $f$ vanishes on $A_1 \times \cdots \times A_n$. Then, by the Strong Form, we can write

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} g_i(x_i) h_i(x_1, \ldots, x_n)$$

with $h_i(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ and $\deg h_i \leqslant \deg f - \deg g_i$. Since $k_1 + \cdots + k_n = \deg f$ and $k_i < |A_i|$ for $i = 1, \ldots, n$, we have

$$[x_1^{k_1} \cdots x_n^{k_n}] f(x_1, \ldots, x_n) = \sum_{i=1}^{n} [x_1^{k_1} \cdots x_n^{k_n}] x_i^{|A_i|} h_i(x_1, \ldots, x_n) = 0,$$

which contradicts the condition that the coefficient is nonzero.

# A Lemma

**Lemma** [Alon, Nathanson and Ruzsa, Amer. Math. Monthly 1995; J. Number Theory 1996] Let $F$ be a field and $A_1, \ldots, A_n$ its subsets which are finite and nonempty. Let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ have degree less than $k_i = |A_i|$ in $x_i$ for each $i = 1, \ldots, n$. If $f(a_1, \ldots, a_n) = 0$ for all $a_1 \in A_1, \ldots, a_n \in A_n$, then $f(x_1, \ldots, x_n)$ is identically zero.

This lemma can be proved by using induction on $n$ and noting that a nonzero polynomial $P(x) \in F[x]$ of degree less than a positive integer $k$ can't have $k$ distinct zeroes in $F$.

# Proof of the Strong Form

If there are $h_1(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ such that

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} g_i(x_i) h_i(x_1, \ldots, x_n),$$

then for any $a_1 \in A_1, \ldots, a_n \in A_n$ we have

$$f(a_1, \ldots, a_n) = \sum_{i=1}^{n} g_i(a_i) h_i(a_1, \ldots, a_n) = 0.$$

Now we consider the converse. Write

$$f(x_1, \ldots, x_n) = \sum_{j_1, \ldots, j_n \geqslant 0} f_{j_1, \ldots, j_n} x_1^{j_1} \ldots x_n^{j_n}$$

and

$$x^j = g_i(x) q_{ij}(x) + r_i^{(j)}(x),$$

where $q_{ij}(x), r_i^{(j)}(x) \in F[x]$ and $\deg r_i^{(j)}(x) < \deg g_i(x) = |A_i|$. Note that both $r_i^{(j)}(x)$ and $g_i(x) q_{ij}(x) = x^j - r_i^{(j)}(x)$ have degree not exceeding $j$.

# Continue the Proof

Clearly

$$f(x_1,\ldots,x_n) = \sum_{\substack{j_1,\ldots,j_n \geqslant 0 \\ j_1+\cdots+j_n \leqslant \deg f}} f_{j_1,\ldots,j_n} \prod_{i=1}^{n} \Big( g_i(x_i) q_{ij_i}(x_i) + r_i^{(j_i)}(x_i) \Big)$$

$$= \bar{f}(x_1,\ldots,x_n) + \sum_{i=1}^{n} g_i(x_i) h_i(x_1,\ldots,x_n),$$

where

$$\bar{f}(x_1,\ldots,x_n) = \sum_{j_1,\ldots,j_n \geqslant 0} f_{j_1,\ldots,j_n} \prod_{i=1}^{n} r_i^{(j_i)}(x_i)$$

and each $h_i(x_1,\ldots,x_n)$ is a suitable polynomial over $F$ with $\deg g_i + \deg h_i \leqslant \deg f$. If $a_1 \in A_1, \ldots, a_n \in A_n$, then

$$\bar{f}(a_1,\ldots,a_n) = \sum_{j_1,\ldots,j_n \geqslant 0} f_{j_1,\ldots,j_n} \prod_{i=1}^{n} a_i^{j_i} = f(a_1,\ldots,a_n) = 0.$$

As the degree of $\bar{f}(x_1,\ldots,x_n)$ with respect to $x_i$ is smaller than $|A_i|$, by the Lemma the polynomial $\bar{f}(x_1,\ldots,x_n)$ is identically zero.

# Part II.
# Applications to Lev's Conjecture

# Lev's Conjecture

Let $A$ and $B$ be finite nonempty subsets of an additive abelian group $G$. In contrast with the Cauchy-Davenport theorem, J.H.B. Kemperman (1960) and P. Scherk (1955) proved that

$$|A+B| \geqslant |A| + |B| - \min_{c \in A+B} \nu_{A,B}(c),$$

where

$$\nu_{A,B}(c) = |\{(a,b) \in A \times B\colon a+b=c\}|;$$

in particular, we have $|A+B| \geqslant |A|+|B|-1$ if some $c \in A+B$ can be uniquely written as $a+b$ with $a \in A$ and $b \in B$.

Motivated by the Kemperman-Scherk theorem and the Erdős-Heilbronn conjecture, V. F. Lev (2005) proposed the following interesting conjecture.

**Lev's Conjecture**. Let $A$ and $B$ be finite nonempty subsets of an abelian group $G$. Set $A \dotplus B = \{a+b:\ a \in A,\ b \in B,\ a \neq b\}$. Then

$$|A \dotplus B| \geqslant |A| + |B| - 2 - \min_{c \in A+B} \nu_{A,B}(c).$$

# Progress due to H. Pan and Z. W. Sun

**Theorem 1** [H. Pan and Z. W. Sun, Israel J. Math. 2006]. Let $A$ and $B$ be finite nonempty subsets of a field $F$. Let $P(x, y) \in F[x, y]$ and

$$C = \{a + b \colon a \in A,\ b \in B,\ \text{and } P(a, b) \neq 0\}.$$

If $C$ is nonempty, then

$$|C| \geqslant |A| + |B| - \deg P - \min_{c \in C} \nu_{A,B}(c).$$

**Theorem 2** [H. Pan and Z. W. Sun, Israel J. Math. 2006. Let $A$ and $B$ be finite nonempty subsets of an abelian group $G$ with cyclic torsion subgroup. For $i = 1, \ldots, l$ let $m_i$ and $n_i$ be nonnegative integers and let $d_i \in G$. Suppose that

$$C = \{a + b \colon a \in A,\ b \in B,\ \text{and } m_i a - n_i b \neq d_i \text{ for all } i = 1, \ldots, l\}$$

is nonempty. Then

$$|C| \geqslant |A| + |B| - \sum_{i=1}^{l} (m_i + n_i) - \min_{c \in C} \nu_{A,B}(c).$$

# Progress due to H. Pan and Z. W. Sun

The following result on difference-restricted sumsets follows from the above two theorems.

**Theorem 3** [H. Pan and Z. W. Sun, Israel J. Math. 2006]. Let $G$ be an abelian group, and let $A, B, S$ be finite nonempty subsets of $G$ with

$$C = \{a + b\colon a \in A,\ b \in B,\ \text{and } a - b \notin S\} \neq \emptyset.$$

(i) If $G$ is torsion-free or elementary abelian, then

$$|C| \geqslant |A| + |B| - |S| - \min_{c \in C} \nu_{A,B}(c).$$

(ii) If $\mathrm{Tor}(G)$ (the torsion subgroup of $G$) is cyclic, then

$$|C| \geqslant |A| + |B| - 2|S| - \min_{c \in C} \nu_{A,B}(c).$$

**Remark**. Clearly $\min_{c\in C} \nu_{A,B}(c) \geqslant \min_{c\in A+B} \nu_{A,B}(c)$ since $C \subseteq A + B$. So, when $\mathrm{Tor}(G)$ is cyclic and $S = \{0\}$, Theorem 3(ii) gives a result slightly weaker than Lev's conjecture.

# Deduce Theorem 3 from Theorems 1 and 2

Pan and Sun used **the strong form** of the Combinatorial Nullstellensatz to obtain Theorems 1 and 2. Now we deduce Theorem 3 from Theorems 1 and 2.

Without loss of generality we can assume that $G$ is generated by the finite set $A \cup B$.

If $G \cong \mathbb{Z}^n$, then we can simply view $G$ as the ring of algebraic integers in an algebraic number field $K$ with $[K : \mathbb{Q}] = n$.

If $G \cong (\mathbb{Z}/p\mathbb{Z})^n$ where $p$ is a prime, then $G$ is isomorphic to the additive group of the finite field with $p^n$ elements.

Thus part (i) follows from Theorem 1 in the case $P(x, y) = \prod_{s \in S}(x - y - s)$.

Let $d_1, \ldots, d_l$ be all the distinct elements of $S$. Applying Theorem 2 with $m_i = n_i = 1$ for all $i = 1, \ldots, l$, we immediately get the second part.

# A Key Lemma

The following lemma plays a key role in the proof of Th. 1-2.

**Lemma** [H. Pan and Z. W. Sun, Israel J. Math. 2006]. Let $A$ and $B$ be finite nonempty subsets of a field $F$, and write

$$\nu_i = |\{(a,b) \in A \times B \colon a + \lambda_i b = \mu_i\}|$$

for $i = 1, \ldots, k$ where $\lambda_i \in F \setminus \{0\}$ and $\mu_i \in F$. Let $P(x,y) \in F[x,y]$. Suppose that for any $i = 1, \ldots, k$ there are $a \in A$ and $b \in B$ with $P(a,b) \neq 0$ and $a + \lambda_i b = \mu_i$, and that for each $(a,b) \in A \times B$ with $P(a,b) \neq 0$ there is a unique $i \in \{1, \ldots, k\}$ with $a + \lambda_i b = \mu_i$. Then we have

$$k + \min\{\nu_1, \ldots, \nu_k\} \geqslant |A| + |B| - \deg P.$$

The proofs starts from the observation that

$$f(x,y) := P(x,y) \prod_{j=1}^{k} (x + \lambda_j y - \mu_j)$$

vanishes over $A \times B$. Then we apply the strong from of CN.

# Part III.
# A Polynomial Formula and its Applications

# A Polynomial Formula

**Lemma** [Z. W. Sun, Electron. Res. Announc. Amer. Math. Soc., 2003]. Let $R$ be a ring with identity, and let $f(x_1, \ldots, x_n)$ be a polynomial over $R$. If $J \subseteq [1, n] = \{1, \ldots, n\}$ and $|J| \geqslant \deg f$, then we have the identity

$$\sum_{I \subseteq J} (-1)^{|J|-|I|} f([\![1 \in I]\!], \ldots, [\![n \in I]\!]) = \Big[\prod_{j \in J} x_j\Big] f(x_1, \ldots, x_n),$$

where $[\![s \in I]\!]$ takes 1 or 0 according as $s \in I$ or not.

*Remark*. The polynomial formula is powerful, it implies the key lemma in Rónyai's study of the Kemnitz conjecture, as well as the Combinatorial Nullstellenstaz in the case $k_1, \ldots, k_n \in \{0, 1\}$.

# A Useful Technique

Let $m$ be an integer and let $p$ be a prime. Fermat's little theorem tells that we can characterize whether $p$ divides $m$ as follows:

$$[\![p \mid m]\!] \equiv 1 - m^{p-1} \pmod{p}.$$

To handle general abelian $p$-groups in a similar way, we need to characterize whether a given power of $p$ divides $a$. Thus, the following lemma is of technical importance. It first appeared in Sun's preprint `arXiv:math/NT/0305369` dated May 24, 2003.

**Lemma 2** [Z. W. Sun, Israel J. Math., 2009] Let $p$ be a prime, and let $a \in \mathbb{N}$ and $m \in \mathbb{Z}$. Then we have the following congruence

$$\binom{m-1}{p^a - 1} \equiv [\![p^a \mid m]\!] \pmod{p}.$$

# Sun's Proof of the Olson Theorem without Group Rings

**Olson's Theorem** [J. Number Theory 1969]. Let $G$ be an abelian $p$-group isomorphic to $\mathbb{Z}_{p^{a_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{a_r}}$ where $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Given $c, c_1, \ldots, c_k \in G$ with $k \geqslant 1 + \sum_{t=1}^{r}(p^{a_t} - 1)$, we have

$$\sum_{\substack{I \subseteq [1,k] \\ \sum_{s \in I} c_s = c}} (-1)^{|I|} \equiv 0 \pmod{p}.$$

In particular, when $c = 0$ it follows that there is a nonempty $I \subseteq [1, k]$ with $\sum_{s \in I} c_s = 0$.

**Remark**. Olson's theorem determined the Davenport constant for any abelian $p$-group. Olson used the group ring method in his proof of this classical theorem.

Now we prove Olson's theorem without any use of the group ring method. Identify $c$ with a vector $\langle c^{(1)} \bmod p^{a_1}, \ldots, c^{(r)} \bmod p^{a_r} \rangle$, and write $c_s$ in the form $\langle c_s^{(1)} \bmod p^{a_1}, \ldots, c_s^{(r)} \bmod p^{a_r} \rangle$.

# Sun's Proof of the Olson Theorem without Group Rings

Define

$$f(x_1,\ldots,x_k)=\prod_{t=1}^{r}\binom{\sum_{s=1}^{k}c_s^{(t)}x_s-c^{(t)}-1}{p^{a_t}-1}.$$

Clearly $\deg f\leqslant\sum_{t=1}^{r}(p^{a_t}-1)<k=|[1,k]|$. Applying the polynomial formula with $J=[1,k]$ we get

$$\sum_{I\subseteq[1,k]}(-1)^{k-|I|}f([\![1\in I]\!],\ldots,[\![k\in I]\!])=[x_1\cdots x_k]f(x_1,\ldots,x_k)=0,$$

i.e.,

$$\sum_{I\subseteq[1,k]}(-1)^{k-|I|}\prod_{t=1}^{r}\binom{\sum_{s\in I}c_s^{(t)}-c^{(t)}-1}{p^{a_t}-1}=0.$$

Thus, with the help of the second lemma,

$$\sum_{\substack{I\subseteq[1,k]\\ p^{a_t}\mid\sum_{s\in I}c_s^{(t)}-c^{(t)}}}(-1)^{|I|}\equiv 0\pmod p,\ \text{i.e.,}\ \sum_{\substack{I\subseteq[1,k]\\ \sum_{s\in I}c_s=c}}(-1)^{|I|}\equiv 0\pmod p.$$

We are done!

# Kemnitz's Conjecture

What is the smallest integer $l = s(\mathbb{Z}_n^2)$ such that every sequence of $l$ elements in $\mathbb{Z}_n^2 = \mathbb{Z}_n \oplus \mathbb{Z}_n$ contains a zero-sum subsequence of length $n$?

In 1983 Kemnitz [Ars Combin.] conjectured that $s(\mathbb{Z}_n^2) = 4n - 3$, and the conjecture can be reduced to the case with $n$ a prime.

In 1993 Alon and Dubiner showed that $s(\mathbb{Z}_n^2) \leqslant 6n - 5$. In 2000 Rónyai [Combinatorica] was able to prove that $s(\mathbb{Z}_p^2) \leqslant 4p - 2$ for every prime $p$; in 2001 W. D. Gao [J. Combin. Theory Ser. A] used Olson's group ring approach to deduce that $s(\mathbb{Z}_q^2) \leqslant 4q - 2$ for any prime power $q$.

These results were obtained by various algebraic methods.

The following lemma plays an indispensable role in the study of the Kemnitz conjecture.
**Alon-Dubiner Lemma** Let $q$ be a prime power, and let $c_1, \ldots, c_{3q}$ be elements of $\mathbb{Z}_q^2$ with $c_1 + \ldots + c_{3q} = 0$. Then there is an $I \subseteq [1, 3q]$ with $|I| = q$ such that $\sum_{i \in I} c_i = 0$.

# A Consequence of the Polynomial Formula

In March 2003 Sun deduced the following result from his polynomial formula.

**Theorem 1** [Z. W. Sun, Electron. Res. Announc. Amer. Math. Soc. 9(2003)]. Let $p$ be a prime and let $h>0$ be an integer. Let $a_i,b_i\in\mathbb{Z}$ for $i=1,\ldots,4p^h-2$.

(i) Set $\mathcal{I}=\{I\subseteq[1,4p^h-2]\colon \sum_{i\in I}a_i\equiv\sum_{i\in I}b_i\equiv 0 \pmod{p^h}\}$. Then

$$|\{I\in\mathcal{I}\colon |I|=p^h\}|\equiv|\{I\in\mathcal{I}\colon |I|=3p^h\}|+2 \pmod{p}.$$

(ii) Suppose that

$$\sum_{\substack{I,J\subseteq[1,4p^h-3]\\ |I|=|J|=p^h-1,\ I\cap J=\emptyset}}\Big(\prod_{i\in I}a_i\Big)\Big(\prod_{j\in J}b_j\Big)\not\equiv 2 \pmod{p}.$$

Then there exists an $I\subseteq[1,4p^h-3]$ with $|I|=p^h$ such that $\sum_{i\in I}a_i\equiv\sum_{i\in I}b_i\equiv 0 \pmod{p^h}$.

# Reiher's work

In his paper "*On Kemnitz's conjecture concerning lattice points in the plane*" written in Nov. 2003, C. Reiher, completely proved the Kemnitz conjecture which had been open for 20 years! This work represents one of the most important achievements in the theory of zero-sums.

Reiher's paper has 4 pages. Pages 1–3 are devoted to 5 sophisticated corollaries to the Chevalley-Warning theorem which are needed later. Actually this can be significantly simplified by using our Theorem 1(i) with $a_{4p-2} = b_{4p-2} = 0$.

**A Consequence of Theorem 1(i)** Let $p$ be a prime and let $h > 0$ be an integer. Let $a_i, b_i \in \mathbb{Z}$ for $i = 1, \ldots, 4p^h - 3$. Set $\mathcal{I} = \{I \subseteq [1, 4p^h - 3]\colon \sum_{i\in I} a_i \equiv \sum_{i\in I} b_i \equiv 0 \pmod{p^h}\}$. Then

$$\begin{aligned}&|\{I \in \mathcal{I}\colon |I| = p^h\}| + |\{I \in \mathcal{I}\colon |I| = p^h - 1\}|\\ \equiv&|\{I \in \mathcal{I}\colon |I| = 3p^h\}| + |\{I \in \mathcal{I}\colon |I| = 3p^h - 1\}| + 2 \pmod{p}.\end{aligned}$$

# Reiher's Lemma

On the last page of his paper, C. Reiher provided a key lemma which is obtained by a combinatorial method rather than an algebraic method.

**Reiher's Lemma**. Let $p$ be a prime and let $a_i, b_i \in \mathbb{Z}$ for $i = 1, \ldots, 4p-3$. Set

$$\mathcal{I} = \left\{ I \subseteq [1, 4p-3] \colon \sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \pmod{p} \right\}.$$

Then, either $\{I \in \mathcal{I} \colon |I| = p\} \neq \emptyset$ or

$$|\{I \in \mathcal{I} \colon |I| = p-1\}| \equiv |\{I \in \mathcal{I} \colon |I| = 3p-1\}| \pmod{p}.$$

# An Observation

For $J \subseteq [1, 4p-3]$ and $n = 1, 2, \ldots$ let

$$(n, J) := \left|\left\{I \subseteq J\colon |I| = n \ \&\ \sum_{i\in I} a_i \equiv \sum_{i\in I} b_i \equiv 0 \pmod{p}\right\}\right|.$$

**Observation.** We have

$$|J| \in \{3p-1, 3p-2\} \Rightarrow (2p, J) \equiv (p, J) - 1 \pmod{p}.$$

In fact, by the polynomial formula we mentioned before,

$$\sum_{I\subseteq J}(-1)^{|J|-|I|}(1-|I|^{p-1})\left(1-\left(\sum_{i\in I} a_i\right)^{p-1}\right)\left(1-\left(\sum_{i\in I} b_i\right)^{p-1}\right)$$

$$=\left[\prod_{j\in J} x_j\right]\left(1-\left(\sum_{j\in J} x_j\right)^{p-1}\right)\left(1-\left(\sum_{j\in J} a_j x_j\right)^{p-1}\right)$$

$$\times\left(1-\left(\sum_{j\in J} b_j x_j\right)^{p-1}\right)$$

$=0.$

# Sketch of the proof

Thus

$$\sum_{\substack{I\subseteq J,\ |I|\in\{0,p,2p\} \\ \sum_{i\in I} a_i\equiv\sum_{i\in I} b_i\equiv 0 \pmod p}} (-1)^{|I|} \equiv 0 \pmod p,$$

that is, $(0,J)-(p,J)+(2p,J)=0$.

*Sketch of the Proof.* Assume that $\{I\in\mathcal{I}\colon |I|=p\}=\emptyset$, i.e., $(p,J)=0$ for any $J\subseteq[1,4p-3]$. Let $N$ denote the number of partitions $[1,4p-3]=I_1\cup I_2\cup I_3$ satisfying

$$|I_1|=p-1,\ \ |I_2|=p-2,\ \ |I_3|=2p$$

and furthermore

$$\sum_{i\in I_1} a_i\equiv\sum_{i\in I_1} b_i\equiv 0 \pmod p,\quad \sum_{i\in I_3} a_i\equiv\sum_{i\in I_3} b_i\equiv 0 \pmod p$$

(and hence $\sum_{i\in[1,4p-3]\setminus I_2} a_i\equiv\sum_{i\in[1,4p-3]\setminus I_2} b_i\equiv 0 \pmod p$).

We count $N$ in two ways.

# Continue the proof

Observe that

$$N = \sum_{I_1} (2p, [1, 4p-3] \backslash I_1) \equiv \sum_{I_1} (-1) = -(p-1, [1, 4p-3]) \pmod{p}.$$

On the other hand,

$$\begin{aligned} N &= \sum_{I_2} (2p, [1, 4p-3] \setminus I_2) \\ &\equiv \sum_{[1,4p-3] \backslash I_2} (-1) = -(3p-1, [1, 4p-3]) \pmod{p}. \end{aligned}$$

So we have the congruence
$(p-1, [1, 4p-3]) \equiv (3p-1, [1, 4p-3]) \pmod{p}$.

*Remark*. The prime power version of Reiher's Lemma also holds.

# Conclusion

Combining Reiher's Lemma, the Alon-Dubiner lemma and the above consequence of Theorem 1(i), we immediately obtain the following result of Reiher [Ramanujan J. 2007].

**Kemnitz-Reiher Theorem**. The Kemnitz conjecture is true, that is, any sequence of elements in $\mathbb{Z}_n \oplus \mathbb{Z}_n$ with length at least $4n - 3$ contains a zero-sum sequence of length $n$.

What does Reiher's solution teach us? When we apply a powerful algebraic method in combinatorics, we should also realize its disadvantage and should not forget combinatorial methods. **A combination of algebraic methods and combinatorial methods might be more powerful!**

By the way, Sun [Israel J. Math. 2009] established connections of the EGZ theorem, Olson's theorem and the Alon-Dubiner lemma to covering systems of $\mathbb{Z}$ by residue classes. But it seems that the Kemnitz-Reiher theorem cannot be connected with covers of $\mathbb{Z}$.

# Open Problem

How to determine $s(\mathbb{Z}_n^d)$?

*In particular,*

how to prove $s(\mathbb{Z}_p^3) = 9p - 8$ for odd prime $p$?

Thank you!