

ON THE ELEMENTARY PROOF OF THE INVERSE ERDŐS-HEILBRONN PROBLEM

SHENGNING ZHANG

ABSTRACT. In this article, we studied the inverse Erdős-Heilbronn problem with the sumset from two components A and B that are not necessarily the same. We give a completely elementary proof for the problem in \mathbb{Z} and some partial results that contributes to the elementary proof of the problem in $\mathbb{Z}/p\mathbb{Z}$, avoiding the usage of the powerful polynomial method and the combinatorial Nullstellensatz.

1. INTRODUCTION

A basic object in Additive Number Theory is the sumset of sets A and B :

$$A + B = \{a + b : a \in A, b \in B\}.$$

A simple problem in Additive Number Theory is: Given two subsets A and B of sets of integers, what properties can we determined about $A + B$? A classic result is the Cauchy-Davenport Theorem proved by Cauchy [1] in 1813 and independently by Davenport [2] in 1935. Let p be a prime, if A and B are nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$, then the theorem asserts that

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

Similarly, we can define the restricted sumsets of sets A and B :

$$A \hat{+} B = \{a + b : a \in A, b \in B, a \neq b\}.$$

In 1964, P. Erdős and H. Heilbronn [3] conjectured that

$$|A \hat{+} A| \geq \min\{p, 2|A| - 3\},$$

where p is a prime and A is a nonempty subset of $\mathbb{Z}/p\mathbb{Z}$. The conjecture was then proved by J. A. Dias da Silva and Y. O. Hamidoune [4] in 1994 through the usage of methods from linear algebra. The more general case

$$|A \hat{+} B| \geq \min\{p, |A| + |B| - 3\}$$

was established and proved by N. Alon, Melvin B. Nathanson, and Imre Z. Ruzsa [5] in 1995 using the polynomial method.

These theorems above depict the properties of sumsets and restricted sumsets given the knowledge of the individual sets that make up the sumsets or restricted sumsets. Thus, one may consider the inverse directions of these problems and there indeed exists several beautiful results. In particular, Gy. Károlyi [6] points out the following inverse problem of the Erdős-Heilbronn conjecture:

Let sets $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ be nonempty sets such that $p \geq |A| + |B| - 2$, where p is a prime. Then $|A\hat{+}B| = |A| + |B| - 3$ if and only if $A = B$ and one of the following holds:

- (1) $|A| = 2$ or $|A| = 3$;
- (2) $|A| = 4$ and $A = \{a, a + d, c, c + d\}$;
- (3) $|A| \geq 5$ and A is an arithmetic progression.

This paper is motivated to give an elementary proof of the results. Firstly, the original proof of this statement [6] relies on the combinatorial Nullstellensatz and the polynomial method through the entire proof of the theorem. Inspired by [7], we believe that this should be unnecessary for such an elementary statement. Secondly, we hope to obtain a more explicit view to the structures of the sumsets in \mathbb{Z} and $\mathbb{Z}/p\mathbb{Z}$ by an elementary proof.

Our strategy is to first prove the inverse problem of the Erdős-Heilbronn conjecture for \mathbb{Z} , which is of independent interests. Our result generalizes Nathanson's proof [8], where the case $A = B$ is studied. In our work A and B are not necessarily the same. We then give some partial results for the elementary proof of the case in $\mathbb{Z}/p\mathbb{Z}$ through Theorem 5, Theorem 6 and Theorem 7.

2. NOTATIONS

To simplify our proofs, we will use the following notations throughout the rest of the paper:

- (1) Let G be the group \mathbb{Z} or $\mathbb{Z}/p\mathbb{Z}$. For nonempty finite sets $A, B \subseteq G$ with $|A|, |B| \geq 2$, note

$$A = \{a_1, a_2, \dots, a_m\} \quad (m = |A|)$$

and

$$B = \{b_1, b_2, \dots, b_n\} \quad (n = |B|).$$

If $G = \mathbb{Z}$, we always assume that $a_1 < a_2 < \dots < a_m$ and $b_1 < b_2 < \dots < b_n$; If $G = \mathbb{Z}/p\mathbb{Z}$, we identify it as set with $\{0, 1, 2, \dots, p-1\}$, and without the abuse of notation, we also assume $a_1 < a_2 < \dots < a_m$ and $b_1 < b_2 < \dots < b_n$;

- (2) For nonempty finite sets $A, B \subseteq G$ with $|A|, |B| \geq 2$, define the restricted sumset of A and B as $A\hat{+}B$. $A\hat{+}B = \{a + b : a \in A, b \in B, a \neq b\}$ if $G = \mathbb{Z}$ and $A\hat{+}B = \{a + b \pmod{p} : a \in A, b \in B, a \neq b\}$ if $G = \mathbb{Z}/p\mathbb{Z}$;

- (3) For nonempty finite sets $A, B \subseteq G$ with $|A|, |B| \geq 2$, if

$$|A\hat{+}B| = |A| + |B| - 3,$$

then we call the unordered pair (A, B) a critical pair;

- (4) For nonempty finite set $A \subseteq G$ with $|A| \geq 2$, if A can be written into the form $A = \{\tau + id : i = 0, 1, \dots, |A| - 1\}$ for some $\tau, d \in G$ with $d \neq 0$, then we call set A a standard set;

- (5) If sets A and B are both standard sets and $A = B$, then we call the unordered pair (A, B) a standard pair.
- (6) Suppose $m, n \in \mathbb{Z}_+ \cup \{0\}$ and p is a prime. Let $X \in \mathbb{Z}/p\mathbb{Z}$ be a nonempty set with $|X| \geq 2$. Suppose d is a given generator of $\mathbb{Z}/p\mathbb{Z}$. Then $[m, n]_d$ is called a gap with respect to d in X if $rd \notin X$ for $\forall r \in \{m, m+1, \dots, n\}$. The length of the gap $[m, n]_d$ is $(n - m + 1)$.

3. THE CASES OF \mathbb{Z} FOR $2 \leq |A| \leq 4$

Theorem 1. *Let finite sets $A, B \subseteq \mathbb{Z}$ be nonempty sets. If $|A| = 2$, then (A, B) is a critical pair if and only if $A = B$.*

Proof. We first consider the sufficiency of the conditions. If $A = B$, then assume that $A = B = \{a_1, a_2\}$. Thus,

$$|A \hat{+} B| = |\{a_1 + a_2\}| = 1 = |A| + |B| - 3.$$

For the necessity of the conditions, suppose $A = \{a_1, a_2\}$. If $a_2 \neq b_n$, due to $a_2 > a_1$ and $b_n = \max_{x \in B} \{x\}$, we have

$$a_2 + b_n \in (A \hat{+} B) \setminus (\{a_1\} \hat{+} B).$$

Together with

$$(\{a_1\} \hat{+} B) \cup \{a_2 + b_n\} \subseteq A \hat{+} B,$$

there is

$$|A \hat{+} B| \geq |(\{a_1\} \hat{+} B) \cup \{a_2 + b_n\}| = |B| - 1 + 1 > |A| + |B| - 3.$$

A contradiction! Therefore, $a_2 = b_n$.

Similarly, if $a_1 \neq b_1$, we have

$$a_1 + b_1 \in (A \hat{+} B) \setminus (\{a_2\} \hat{+} B),$$

because $a_1 < a_2$ and $b_1 = \min_{x \in B} \{x\}$. Thus, combining with

$$(\{a_2\} \hat{+} B) \cup \{a_1 + b_1\} \subseteq A \hat{+} B,$$

there is

$$|A \hat{+} B| \geq |(\{a_2\} \hat{+} B) \cup \{a_1 + b_1\}| = |B| - 1 + 1 > |A| + |B| - 3.$$

Consequently, $a_1 = b_1$.

Since $a_1, a_2 \in B$, $|\{a_1\} \hat{+} B| = |\{a_2\} \hat{+} B| = |B| - 1 = |A| + |B| - 3 = |A \hat{+} B|$. Thus, due to $\{a_1\} \hat{+} B, \{a_2\} \hat{+} B \subseteq A \hat{+} B$, there is $\{a_1\} \hat{+} B = \{a_2\} \hat{+} B = A \hat{+} B$. Now, because $a_1 \neq b_2$, we have $a_1 + b_2 \in \{a_1\} \hat{+} B = \{a_2\} \hat{+} B$. Therefore, $\exists b_i \in B$ ($i \in \mathbb{Z}_+$), such that $a_1 + b_2 = a_2 + b_i$. Notice that $a_2 > a_1$, so we must have $b_i < b_2$. According to the definition of B , $b_i = b_1$. Together with $a_1 = b_1$, we have $b_n = a_2 = b_2$. So, we have proven that $A = B$. □

Theorem 2. *Let finite sets $A, B \subseteq \mathbb{Z}$ be nonempty sets. If $|A| = 3$, then (A, B) is a critical pair if and only if $A = B$.*

Proof. Considering the sufficiency of the conditions, if $A = B$, we may assume that $A = B = \{a_1, a_2, a_3\}$, then

$$|A\hat{+}B| = |\{a_1 + a_2, a_1 + a_3, a_2 + a_3\}| = 3 = |A| + |B| - 3.$$

In order to prove the necessity of the conditions, we will first prove that $A \subseteq B$. If $a_1 \notin B$, then

$$|\{a_1\}\hat{+}B| = |B| = |A| + |B| - 3 = |A\hat{+}B|.$$

Since $\{a_1\}\hat{+}B \subseteq A\hat{+}B$ and $\{a_2, a_3\}\hat{+}B \subseteq A\hat{+}B$, we have

$$\{a_2, a_3\}\hat{+}B \subseteq \{a_1\}\hat{+}B = A\hat{+}B.$$

This indicates that for $\forall b_i \in B$ ($i \in \mathbb{Z}_+$) with $b_i \neq a_2$, $\exists b_j \in B$ ($j \in \mathbb{Z}_+$) such that $a_2 + b_i = a_1 + b_j$. Suppose $a_2 \neq b_n$, then $a_2 + b_n = a_1 + b_j$. However, for $\forall b_k \in B$ ($k \in \mathbb{Z}_+$), there is $a_2 + b_n > a_1 + b_k$. A contradiction! Thus, we must have $a_2 = b_n$. Notice that for $\forall b_k \in B$ ($k \in \mathbb{Z}_+$), there is $a_3 + b_n > a_1 + b_k$. Therefore, by applying the same argument, there is $a_3 = b_n$, which contradicts to $a_3 > a_2$. Consequently, we must have $a_1 \in B$.

If $a_3 \notin B$, then

$$|\{a_3\}\hat{+}B| = |B| = |A| + |B| - 3 = |A\hat{+}B|.$$

Since $\{a_3\}\hat{+}B \subseteq A\hat{+}B$ and $\{a_1, a_2\}\hat{+}B \subseteq A\hat{+}B$, we have

$$\{a_1, a_2\}\hat{+}B \subseteq \{a_3\}\hat{+}B = A\hat{+}B.$$

This indicates that for $\forall b_i \in B$ ($i \in \mathbb{Z}_+$) with $b_i \neq a_2$, $\exists b_j \in B$ ($j \in \mathbb{Z}_+$) such that $a_2 + b_i = a_3 + b_j$. Suppose $a_2 \neq b_1$, then $a_2 + b_1 = a_3 + b_j$. However, we know that for $\forall b_k \in B$ ($k \in \mathbb{Z}_+$), there is $a_2 + b_1 < a_3 + b_k$. A contradiction! Thus, we must have $a_2 = b_1$. Notice that for $\forall b_k \in B$ ($k \in \mathbb{Z}_+$), there is $a_1 + b_1 < a_2 + b_k$. Therefore, by applying the same argument, there is $a_1 = b_1$, which contradicts to $a_2 > a_1$. Consequently, we must have $a_3 \in B$.

If $a_2 \notin B$, then

$$|\{a_2\}\hat{+}B| = |B| = |A| + |B| - 3 = |A\hat{+}B|.$$

Since $\{a_2\}\hat{+}B \subseteq A\hat{+}B$ and $\{a_1, a_3\}\hat{+}B \subseteq A\hat{+}B$, we have

$$\{a_1, a_3\}\hat{+}B \subseteq \{a_2\}\hat{+}B = A\hat{+}B.$$

Through Theorem 2 we know that $|B| \geq 3$, for $|B| = 2$ indicates that $|A| = 2$. Thus, $b_{n-1} \notin \{b_1, b_n\}$. Using this condition, we have $a_3 + b_{n-1} \in A\hat{+}B = \{a_2\}\hat{+}B$. This implies that $\exists b_i \in B$ ($i \in \mathbb{Z}_+$) such that $a_3 + b_{n-1} = a_2 + b_j$. Since $a_3 > a_2$, there must be $b_j > b_{n-1}$. Thus, $b_j = b_n$. Together with $a_3 = b_n$, we have $a_2 = b_{n-1} \in B$. A contradiction! Therefore, $a_2 \in B$. Combining with the arguments above, we have $A \subseteq B$.

Suppose $a_1 \neq b_1$, then $a_1 + b_1 \in (A\hat{+}B) \setminus (\{a_3\}\hat{+}B)$, for $a_1 < a_3$ and $b_1 = \min_{x \in B} \{x\}$. Thus, $a_2 = b_1$, or else we can get $a_2 + b_1 \in (A\hat{+}B) \setminus (\{a_3\}\hat{+}B)$ with

the same argument above. Apparently, $(\{a_3\}\hat{+}B) \cup \{a_1 + b_1, a_2 + b_1\} \subseteq A\hat{+}B$. However, because (A, B) is a critical pair,

$$\begin{aligned} |(\{a_3\}\hat{+}B) \cup \{a_1 + b_1, a_2 + b_1\}| &= |\{a_1\}\hat{+}B| + |\{a_1 + b_1, a_2 + b_1\}| \\ &= (|B| - 1) + 2 \\ &= |A| + |B| - 2 \\ &= |A\hat{+}B| + 1 \end{aligned}$$

leads to a contradiction! Therefore, $a_1 = b_1$.

Suppose $a_3 \neq b_n$, then $a_3 + b_n \in A\hat{+}B \setminus \{a_1\}\hat{+}B$, for $a_1 < a_3$ and $b_n = \max_{x \in B} \{x\}$. So, $a_2 = b_n$, or else we can get $a_2 + b_n \in (A\hat{+}B) \setminus (\{a_1\}\hat{+}B)$ with the same argument above. Apparently, $(\{a_1\}\hat{+}B) \cup \{a_2 + b_n, a_3 + b_n\} \subseteq A\hat{+}B$. However, because (A, B) is a critical pair,

$$\begin{aligned} |(\{a_1\}\hat{+}B) \cup \{a_2 + b_n, a_3 + b_n\}| &= |\{a_1\}\hat{+}B| + |\{a_2 + b_n, a_3 + b_n\}| \\ &= (|B| - 1) + 2 \\ &= |A| + |B| - 2 \\ &= |A\hat{+}B| + 1 \end{aligned}$$

leads to a contradiction! Therefore, $a_3 = b_n$.

Since $a_1 \in B$, we have $|\{a_1\}\hat{+}B| = |B| - 1$. Due to $b_{n-1} \notin \{b_1, b_n\} = \{a_1, a_3\}$, $a_1 < b_{n-1}$. So, $a_1 + b_n < a_3 + b_{n-1}$. Therefore, $a_3 + b_{n-1} \in (A\hat{+}B) \setminus (\{a_1\}\hat{+}B)$. Consequently,

$$|\{a_3 + b_{n-1}\} \cup (\{a_1\}\hat{+}B)| = |B| = |A| + |B| - 3 = |A\hat{+}B|.$$

Since $(\{a_3 + b_{n-1}\} \cup (\{a_1\}\hat{+}B)) \subseteq A\hat{+}B$, we have $\{a_3 + b_{n-1}\} \cup (\{a_1\}\hat{+}B) = A\hat{+}B$. Apparently, $a_2 + b_n \in (A\hat{+}B) \setminus (\{a_1\}\hat{+}B)$. With the same argument, there is $\{a_2 + b_n\} \cup (\{a_1\}\hat{+}B) = A\hat{+}B$. This together with the previous argument above leads to

$$\{a_3 + b_{n-1}\} \cup (\{a_1\}\hat{+}B) = \{a_2 + b_n\} \cup (\{a_1\}\hat{+}B).$$

Thus, $a_3 + b_{n-1} = a_2 + b_n$, indicating that $a_2 = b_{n-1}$.

Suppose $|B| \geq 4$, then $\exists b_{n-2} \in B \setminus \{b_1, b_{n-1}, b_n\}$. If $a_3 + b_{n-2} \in \{a_1\}\hat{+}B$, then $\exists b_i \in B \setminus \{a_1\}$ ($i \in \mathbb{Z}_+$) such that $a_1 + b_i = a_3 + b_{n-2}$. Since $a_1 < a_3$, we must have $b_i > b_{n-2}$. Thus, $b_i = b_n$. This leads to $a_2 = b_{n-2}$. A contradiction! Therefore, $a_3 + b_{n-2} \notin \{a_1\}\hat{+}B$. Combining

$$\{a_3 + b_{n-2}\} \cup (\{a_1\}\hat{+}B) \subseteq A\hat{+}B$$

with

$$|\{a_3 + b_{n-2}\} \cup (\{a_1\}\hat{+}B)| = |B| = |A\hat{+}B|,$$

we have $\{a_3 + b_{n-2}\} \cup (\{a_1\}\hat{+}B) = A\hat{+}B$. Recalling that

$$\{a_2 + b_n\} \cup (\{a_1\}\hat{+}B) = A\hat{+}B,$$

we can get $a_2 + b_n = a_3 + b_{n-2}$. Thus, $a_2 = b_{n-2}$, which is not possible! Therefore, $|B| = 3$. This implies that $A = B$. □

Theorem 3. *Let finite sets $A, B \subseteq \mathbb{Z}$ be nonempty sets. If $|A| = 4$, then (A, B) is a critical pair if and only if $A = B$ and $A = \{a, c, a + d, c + d\}$.*

Proof. We first consider the sufficiency of the conditions. If $A = B$ and $A = \{a, a + d, c, c + d\}$, then we have

$$|A \hat{+} B| = |\{a + c, 2a + c, 2c + d, a + c + d, a + c + 2d\}| = 5 = |A| + |B| - 3.$$

Now, consider the necessity of conditions. Apparently,

$$|(\{a_4\} \hat{+} B) \cup (\{b_1\} \hat{+} A)| = |\{a_4\} \hat{+} B| + |\{b_1\} \hat{+} A| - |(\{a_4\} \hat{+} B) \cap (\{b_1\} \hat{+} A)|.$$

Noticing that $(\{a_4\} \hat{+} B) \cap (\{b_1\} \hat{+} A) = \{a_4 + b_1\}$, we have

$$|(\{a_4\} \hat{+} B) \cup (\{b_1\} \hat{+} A)| \geq (|A| - 1) + (|B| - 1) - 1 = |A \hat{+} B|.$$

Since $(\{a_4\} \hat{+} B) \cup (\{b_1\} \hat{+} A) \subseteq A \hat{+} B$, there is $(\{a_4\} \hat{+} B) \cup (\{b_1\} \hat{+} A) = A \hat{+} B$. Thus, $|\{a_4\} \hat{+} B| = |B| - 1$ and $|\{b_1\} \hat{+} A| = |A| - 1$. This gives us $a_4 \in B$ and $b_1 \in A$. Using the same argument, we have $(\{a_1\} \hat{+} B) \cup (\{b_n\} \hat{+} A) = A \hat{+} B$, $a_1 \in B$ and $b_n \in A$. Through the definition of a_1, a_4, b_1 and b_n , there must be $a_1 = b_1$ and $a_4 = b_n$. Then, there are

$$\begin{aligned} A \hat{+} B &= (\{a_4\} \hat{+} B) \cup (\{b_1\} \hat{+} A) \\ &= \{a_4 + b_1, a_4 + b_2, \dots, a_4 + b_{n-1}\} \cup \{b_1 + a_2, b_1 + a_3\} \\ &= \{a_4 + b_1, a_4 + b_2, \dots, a_4 + b_{n-1}\} \cup \{a_1 + a_2, a_1 + a_3\} \end{aligned}$$

and

$$\begin{aligned} A \hat{+} B &= (\{a_1\} \hat{+} B) \cup (\{b_n\} \hat{+} A) \\ &= \{a_1 + b_2, a_1 + b_3, \dots, a_1 + b_n\} \cup \{b_n + a_2, b_n + a_3\}. \end{aligned}$$

Rearrange the elements in $A \hat{+} B$, and then we have

$$\begin{aligned} A \hat{+} B &= \{a_1 + a_2, a_1 + a_3, a_4 + b_1, a_4 + b_2, \dots, a_4 + b_{n-1}\} \\ &= \{a_1 + b_2, a_1 + b_3, \dots, a_1 + b_n, a_2 + b_n, a_3 + b_n\}. \end{aligned}$$

Notice that $a_1 + a_2 < a_1 + a_3 < \dots < a_4 + b_{n-1}$ and $a_1 + b_2 < a_1 + b_3 < \dots < a_3 + b_n$, then there must be $a_4 + b_{n-1} = a_3 + b_n$ and $a_1 + a_2 = a_1 + b_2$. So, we can get $a_2 = b_2$, which further indicates that $a_3 = b_3$. What's more, $a_4 = b_n$ shows that $a_3 = b_{n-1}$. As a result, $b_3 = b_{n-1}$. Therefore,

$$A = \{a_1, a_2, a_3, a_4\} = \{b_1, b_2, b_3, b_4\} = B.$$

It's now easy for us to find that $A \hat{+} B = \{a_1 + a_4, a_2 + a_4, a_3 + a_4, a_1 + a_2, a_1 + a_3\}$. Since we also have $a_2 + a_3 \in A \hat{+} B$, it's apparent that $a_2 + a_3 = a_1 + a_4$. This means $a_3 - a_1 = a_4 - a_2$. By letting $a_3 - a_1 = d$, $a_1 = a$ and $a_2 = c$, we have $A = \{a, c, a + d, c + d\}$, which completes the proof. \square

4. THE CASES OF \mathbb{Z} FOR $|A| \geq 5$

Theorem 4. *Let sets $A, B \subseteq \mathbb{Z}$ be nonempty sets. If $|A| \geq 5$, then (A, B) is a critical pair if and only if (A, B) is a standard pair.*

Proof. We still first consider the sufficiency of the conditions. Since (A, B) is a standard pair, we may assume that

$$A = B = \{a_1, a_2, \dots, a_m\} = \{a + id : i = 0, 1, \dots, m-1\}$$

for some $a, d \in \mathbb{Z}_+$. Define $A' = B' = \{id : i = 0, 1, \dots, m-1\}$. For $\forall x+y \in A \hat{+} B$, there is $(x-a) + (y-a) \in A' \hat{+} B'$. Similarly, for $\forall u+w \in A' \hat{+} B'$, there is $(u+a) + (w+a) \in A \hat{+} B$. So, $|A \hat{+} B| = |A' \hat{+} B'|$. Now, according to the definition of sumset and restricted sumset, we have

$$A' \hat{+} B' \subseteq A' + B'$$

and

$$|A' + B'| = |\{id : i = 0, 1, \dots, 2m-2\}| = |A'| + |B'| - 1 \geq |A' \hat{+} B'|.$$

Apparently, there are $0 \notin A' \hat{+} B'$ and $(2m-2)d \notin A' \hat{+} B'$. Thus, $A' \hat{+} B' \subseteq \{id : i = 1, \dots, 2m-3\}$. For $\forall x \in [1, m-1] \cap \mathbb{Z}$, we can choose $0 \in A'$ and $xd \in B'$. Since $0 \neq xd$, we have $xd = 0 + xd \in A' \hat{+} B'$. For $\forall x \in [m, 2m-3] \cap \mathbb{Z}$, we can choose $(m-1)d \in A'$ and $(x-m+1)d \in B'$. Since $x \in [m, 2m-3] \cap \mathbb{Z}$,

$$(x-m+1)d < (m-1)d.$$

Therefore, we have $xd = (m-1)d + (x-m+1)d \in A' \hat{+} B'$. So, for $\forall x \in [1, 2m-3]$, $xd \in A' \hat{+} B'$. Combining with $A' \hat{+} B' \subseteq \{id : i = 1, \dots, 2m-3\}$, we have $A' \hat{+} B' = \{id : i = 1, \dots, 2m-3\}$. As a result,

$$|A \hat{+} B| = |A' \hat{+} B'| = |\{id : i = 1, \dots, 2m-3\}| = 2m-3 = |A| + |B| - 3.$$

To prove the necessity of the conditions, let's consider the following lemmas.

Lemma 1. *If finite sets $A, B \subseteq \mathbb{Z}$ are nonempty sets, then $|A+B| \geq |A| + |B| - 1$.*

Proof. Since A and B are finite sets, define the element with the largest absolute value in A as a_x and the element with the largest absolute value in B as b_y . Apparently, $\exists p$ such that p is a prime number and $p > \max\{a_m, b_n, |a_x| + |b_y|, |A| + |B| - 1\}$. Thus, applying the Cauchy-Davenport theorem in $\mathbb{Z}/p\mathbb{Z}$ [1], we have $|A+B| \geq \min\{p, |A| + |B| - 1\} = |A| + |B| - 1$. □

Lemma 2. *If finite sets $A, B \subseteq \mathbb{Z}$ are nonempty sets, then $|A \hat{+} B| \geq |A| + |B| - 3$.*

Proof. Similar with Lemma 1, since A and B are finite sets, define the element with the largest absolute value in A as a_x and the element with the largest absolute value in B as b_y . Apparently, $\exists p$ such that p is a prime number and $p > \max\{a_m, b_n, |a_x| + |b_y|, |A| + |B| - 3\}$. Thus, applying the general case of the Erdős-Heilbronn conjecture in $\mathbb{Z}/p\mathbb{Z}$ [5], we have $|A+B| \geq \min\{p, |A| + |B| - 3\} = |A| + |B| - 3$. □

Lemma 3. *(A, B) is a critical pair and $|A| \geq 5$. If $B \subseteq A$, then $a_m = b_n$ and (X, Y) is also a critical pair, where $X = A \setminus \{a_m\}$ and $Y = B \setminus \{a_n\}$.*

Proof. Since $B \subseteq A$, we have $a_m \geq b_n$. Notice that $(A \hat{+} \{b_1\}) \cap (\{a_m\} \hat{+} B) = \{a_m + b_1\}$. Since

$$(A \hat{+} \{b_1\}) \cup (\{a_m\} \hat{+} B) \subseteq A \hat{+} B,$$

we have

$$|A \hat{+} B| \geq |(A \hat{+} \{b_1\}) \cup (\{a_m\} \hat{+} B)| = |A \hat{+} \{b_1\}| + |\{a_m\} \hat{+} B| - 1.$$

If $a_m > b_n$, then $a_m \notin B$. Thus,

$$|A \hat{+} \{b_1\}| + |\{a_m\} \hat{+} B| - 1 = (|A| - 1) + |B| - 1 = |A| + |B| - 2.$$

A contradiction! Therefore, $a_m = b_n$.

Apparently,

$$\begin{aligned} |(X \hat{+} Y) \cap (\{a_m\} \hat{+} A)| &= |(X \hat{+} Y) \cap ((\{a_m\} \hat{+} A) \setminus \{a_{m-1} + a_m\})| \\ &\leq |(\{a_m\} \hat{+} A) \setminus \{a_{m-1} + a_m\}| \\ &= |A| - 2. \end{aligned}$$

Now, because $B \subseteq A$, we have $A \hat{+} B = (X \hat{+} Y) \cup (\{a_m\} \hat{+} A)$. Thus, according to Lemma 2,

$$\begin{aligned} |(X \hat{+} Y) \cap (\{a_m\} \hat{+} A)| &= |X \hat{+} Y| + |\{a_m\} \hat{+} A| - |(X \hat{+} Y) \cup (\{a_m\} \hat{+} A)| \\ &= |X \hat{+} Y| + |\{a_m\} \hat{+} A| - |A \hat{+} B| \\ &\geq (|X| + |Y| - 3) + (|A| - 1) - (|A| + |B| - 3) \\ &= |A| - 3. \end{aligned}$$

Thus, $|(X \hat{+} Y) \cap (\{a_m\} \hat{+} A)| \in \{|A| - 2, |A| - 3\}$.

If $|(X \hat{+} Y) \cap (\{a_m\} \hat{+} A)| = |A| - 2$, then

$$(X \hat{+} Y) \cap (\{a_m\} \hat{+} A) = (\{a_m\} \hat{+} A) \setminus \{a_{m-1} + a_m\}.$$

This implies that for $\forall a_i \in X \setminus \{a_{m-1}\}$ ($i \in \mathbb{Z}_+$), $\exists x \in X$ and $\exists y \in Y$ with $x \neq y$ such that $a_m + a_i = x + y$. By taking $a_i = a_{m-2}$, we have

$$a_m + a_{m-2} = x + y.$$

Since $a_m > \max\{x, y\}$, then we must have $x > a_{m-2}$ and $y > a_{m-2}$. Thus, $x = y = a_{m-1}$. A contradiction! Consequently, $|(X \hat{+} Y) \cap (\{a_m\} \hat{+} A)| = |A| - 3$.

Through the following computation,

$$\begin{aligned} |X \hat{+} Y| &= |(X \hat{+} Y) \cup (\{a_m\} \hat{+} A)| - |\{a_m\} \hat{+} A| + |(X \hat{+} Y) \cap (\{a_m\} \hat{+} A)| \\ &= |A \hat{+} B| - (|A| - 1) + (|A| - 3) \\ &= (|A| + |B| - 3) - (|A| - 1) + (|A| - 3) \\ &= (|A| - 1) + (|B| - 1) - 3 \\ &= |X| + |Y| - 3, \end{aligned}$$

we complete the proof that (X, Y) is a critical pair. □

Lemma 4. (A, B) is a critical pair and $|A| \geq 5$. If $B \subseteq A$, then (A, B) is a standard pair.

Proof. Let's use induction on $|A|$ to prove Lemma 4.

When $|A| = 5$, define $X = A \setminus \{a_5\}$ and $Y = B \setminus \{b_n\}$. According to Lemma 3, $a_5 = b_n$ and (X, Y) is a critical pair. Since $|X| = 4$, according to Theorem 3, we have $X = Y = \{a_1, a_2, a_3, a_4\}$ and $X \hat{+} Y = \{a_1 + a_4, a_2 + a_4, a_3 + a_4, a_1 + a_2, a_1 + a_3\}$. Apparently, $A = B = \{a_1, a_2, a_3, a_4, a_5\}$. From the proof of Lemma 3, we know that

$$|(X \hat{+} Y) \cap (a_5 \hat{+} A)| = |A| - 3 = 2.$$

It's easy for us to observe that $a_2 + a_4 = a_5 + a_1$ and $a_3 + a_4 = a_5 + a_2$. By the proof of Theorem 3, we also have $a_2 + a_3 = a_1 + a_4$. Consequently,

$$a_5 - a_4 = a_4 - a_3 = a_3 - a_2 = a_2 - a_1.$$

Thus, (A, B) is a standard pair.

Now, suppose Lemma 4 is true for $|A| \leq m - 1$ ($m \in \mathbb{Z}, m > 5$). Let's consider the case when $|A| = m$. Note $A' = A \setminus \{a_m\}$ and $B' = B \setminus \{b_n\}$, then (A', B') is a critical pair and $a_m = b_n$ according to Lemma 3. Thus, by the induction hypothesis, (A', B') is a standard pair. Without loss of generality, for some $\tau, d \in \mathbb{Z}$, we may assume that

$$A' = B' = \{\tau, \tau + d, \tau + 2d, \dots, \tau + (m - 2)d\}$$

with $\tau < \tau + d < \tau + 2d < \dots < \tau + (m - 2)d$.

From the proof of Lemma 3, we know that

$$|(A' \hat{+} B') \cap (a_m \hat{+} A)| = |A| - 3 = |a_m \hat{+} A| - 2.$$

Thus, for $\forall u \in A' \setminus \{\tau + (m - 3)d, \tau + (m - 2)d\}$, $\exists v \in A', w \in B'$ such that

$$a_m + u = v + w.$$

When $u = \tau + (m - 4)d$, $\max\{v, w\} \geq \tau + (m - 3)d$. Without loss of generality, assume that $v \geq w$. Thus, $v \in \{\tau + (m - 3)d, \tau + (m - 2)d\}$.

If $v = \tau + (m - 3)d$, then $a_m = w + d$. From the definition of a_m , we know that $a_m > \tau + (m - 2)d$. Because $w \leq \tau + (m - 2)d$, we must have $w = \tau + (m - 2)d$. Consequently, $a_m = \tau + (m - 1)d = b_n$.

If $v = \tau + (m - 2)d$, then $a_m = w + 2d$. According to the definition of a_m , we know that $a_m > \tau + (m - 2)d$. Thus, since $w \leq \tau + (m - 2)d$, $w \in \{\tau + (m - 3)d, \tau + (m - 2)d\}$. Note that $w \neq v$, then there must be $w = \tau + (m - 3)d$. Therefore, $a_m = \tau + (m - 1)d = b_n$.

As a result, we always have

$$A = B = \{\tau, \tau + d, \tau + 2d, \dots, \tau + (m - 2)d, \tau + (m - 1)d\}$$

with $\tau < \tau + d < \tau + 2d < \dots < \tau + (m - 2)d < \tau + (m - 1)d$. This completes our induction. \square

Lemma 5. Let finite sets $A, B \subseteq \mathbb{Z}$ be nonempty sets. If $|A|, |B| \geq 2$ and $B \not\subseteq A$, then $|A \hat{+} B| \geq |A| + |B| - 2$.

Proof. Suppose $B \subsetneq A$, according to Lemma 2, we have

$$|A \hat{+} B| \geq |A| + |B| - 3.$$

According to Lemma 4, if $|A \hat{+} B| = |A| + |B| - 3$, then $A = B$. However, this contradicts with $B \subsetneq A$. Thus,

$$|A \hat{+} B| > |A| + |B| - 3.$$

Therefore, we have $|A \hat{+} B| \geq |A| + |B| - 2$. \square

Lemma 6. *Let finite sets $A, B \subseteq \mathbb{Z}$ be nonempty sets. If $|A|, |B| \geq 2$ and $A \neq B$, then $|A \hat{+} B| \geq |A| + |B| - 2$.*

Proof. Using Lemma 5, we only need to consider the case when $A \neq B$ and $B \not\subseteq A$. Without loss of generality, assume $|A| \geq |B|$. If $|A \cup B| = 0$, then according to Lemma 1, we have

$$|A \hat{+} B| = |A + B| \geq |A| + |B| - 1 > |A| + |B| - 2.$$

If $|A \cup B| = 1$, then note $X = A \cup B$. According to Lemma 1, we have

$$|A \hat{+} B| \geq |A \hat{+} (B \setminus X)| = |A + (B \setminus X)| \geq |A| + |B \setminus X| - 1 \geq |A| + |B| - 2.$$

Thus, we only need to consider the case when $|A \cup B| \geq 2$. Since $B \not\subseteq A$, we have $A \cap B \subsetneq A \cup B$. Moreover, $A \cap B, A \cup B \in \mathbb{Z}$ and $|A \cup B| \geq 2$. Thus, according to Lemma 5, we have

$$|(A \cup B) \hat{+} (A \cap B)| \geq |A \cup B| + |A \cap B| - 2 = |A| + |B| - 2.$$

Notice that for any $x \neq y$ with $x \in A \cup B$ and $y \in A \cap B$, if $x \in A$, then $y \in B$. Thus, $x + y \in A \hat{+} B$. Similarly, if $x \in B$, then $y \in A$ and thus $x + y \in A \hat{+} B$. As a result,

$$(A \cup B) \hat{+} (A \cap B) \subseteq A \hat{+} B.$$

Therefore, $|A \hat{+} B| \geq |(A \cup B) \hat{+} (A \cap B)| \geq |A| + |B| - 2$. \square

Back to the main problem, if (A, B) is a critical pair, Lemma 6 indicates that $A = B$. Thus, we have $B \subseteq A$. According to Lemma 4, (A, B) is a standard pair when $|A| \geq 5$. This finishes our proof for the sufficiency of the conditions. \square

5. PARTIAL RESULTS IN $\mathbb{Z}/p\mathbb{Z}$

Theorem 5. *Let sets $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ be nonempty sets such that $p \geq |A| + |B| - 2$ and $a_m + b_n < p$. Then $|A \hat{+} B| = |A| + |B| - 3$ if and only if $A = B$ and one of the following holds:*

- (1) $|A| = 2$ or $|A| = 3$;
- (2) $|A| = 4$ and $A = \{a, a + d, c, c + d\}$;
- (3) $|A| \geq 5$ and A is an arithmetic progression.

Proof. Since $a_m + b_n < p$, we have $a + b < p$ for $\forall a \in A, b \in B$. This leads to

$$\{a + b : a \in A, b \in B, a \neq b\} = \{a + b \pmod{p} : a \in A, b \in B, a \neq b\}.$$

This equation here indicates that the proof is equivalent to the case in \mathbb{Z} , which we have completed. \square

Theorem 6. *Let sets $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ be nonempty sets such that $p \geq |A| + |B|$, where p is a prime. Suppose $|A| \geq 5$ and (A, B) is a critical pair. Given d as an arbitrary generator of $\mathbb{Z}/p\mathbb{Z}$, then length of the longest gap in B with respect to d is not less than $|A|$.*

Proof. Let $A = \{\tau + id : i = 0, 1, \dots, |A| - 1\}$ and $B = \{x_i d : i = 0, 1, \dots, |B| - 1\}$, where $\tau \in \mathbb{Z}/p\mathbb{Z}$ and $x_i \in \mathbb{Z}_+ \cup \{0\}$. Define the length of the longest gap in B with respect to d as t and suppose $t \leq |A| - 1$.

Without loss of generality, assume $\tau = 0$, or else use

$$A' = \{id : i = 0, 1, \dots, |A| - 1\}$$

and

$$B' = \{x_i d - \tau : i = 0, 1, \dots, |B| - 1\}$$

to represent A and B . Since $0 \in A$, apparently $B \setminus \{0\} \subseteq A + B$.

Define sets $B_i \subseteq B$ as the following:

$$B_i = \{m_i d, (m_i + 1)d, \dots, \widehat{m}_i d\} \quad (m_i \leq \widehat{m}_i),$$

where $m_{i+1} - \widehat{m}_i \geq 1$. By definition, we can get a partition of B , where I a finite set of positive integers and $B = \sqcup_{i \in I} B_i$. Note $\mathfrak{B}_1 = \{B_i : \widehat{m}_i > t\}$ and $\mathfrak{B}_2 = \{B_i : \widehat{m}_i \leq t\} = \{B_1, B_2, \dots, B_k\}$ ($1 \leq k \leq |B|$).

We first claim that for $\forall g \in \mathbb{Z}_+ \cup \{0\}$, $gd \in A + B$ if there $\exists j \in I$ such that $\widehat{m}_j < g < m_{j+1}$ and $\widehat{m}_j > \widehat{m}_k$.

In particular, if $0 \leq g < m_1$ then $gd \in A + B$. Observing that $g - \widehat{m}_j < m_{j+1} - \widehat{m}_j \leq t + 1 \leq |A|$, we have $g - \widehat{m}_j \leq |A| - 1$ and thus $(g - \widehat{m}_j)d \in A$. Since $\widehat{m}_j > \widehat{m}_k$, $\widehat{m}_j > t \geq g - \widehat{m}_j$. Then $gd = (g - \widehat{m}_j)d + \widehat{m}_j d \in A + B$.

We now proof that for $\forall xd \in A$, if $x \neq 2\widehat{m}_i$ ($i = 1, 2, \dots, k$), then $xd \in A + B$.

To prove this claim, assume that $\widehat{m}_i < x < m_{i+1}$ for some $i \in I$. Again

$$xd = (x - \widehat{m}_j)d + \widehat{m}_j d \in A + B,$$

unless $(x - \widehat{m}_j)d = \widehat{m}_j d$, which indicates $x = 2\widehat{m}_j$.

For $i = 1, 2, \dots, k$, if $|B_i| \geq 2$, then $2\widehat{m}_i d \in A + B$, because $(\widehat{m}_i - 1)d \in B$ and $2\widehat{m}_i d = (\widehat{m}_i + 1)d + (\widehat{m}_i - 1)d$.

For $i = 1, 2, \dots, k$, if there exists \widehat{m}_{i-1} and m_{i+1} such that $\widehat{m}_{i-1} < \widehat{m}_i < m_{i+1}$, then we claim that $2\widehat{m}_i d \in A + B$.

Note that $0 \leq \widehat{m}_{i-1} < \widehat{m}_i < m_{i+1}$. If $2\widehat{m}_i d \notin A + B$, then $2\widehat{m}_i < m_{i+1}$. Therefore,

$$m_{i+1} - \widehat{m}_i > \widehat{m}_i \geq \widehat{m}_i - \widehat{m}_{i-1}.$$

So, $2\widehat{m}_i - \widehat{m}_{i-1} < m_{i+1} \leq \widehat{m}_{i+1} \leq t \leq |A| - 1$. Thus, $(2\widehat{m}_i - \widehat{m}_{i-1})d \in A$. This further leads to $2\widehat{m}_i d = (2\widehat{m}_i - \widehat{m}_{i-1})d + \widehat{m}_{i-1} d \in A + B$.

Combining all these claims, we find the only possible elements in $\mathbb{Z}/p\mathbb{Z}$ that are not in $A\hat{+}B$:

- (1) \widehat{m}_1 , if $\widehat{m}_1 = 0$;
- (2) $2\widehat{m}_1$;
- (3) $2\widehat{m}_k$.

Apparently, the first two cases can not happen together at the same time unless $\widehat{m}_1 = 2\widehat{m}_1 = 0$. So, at most two elements in $\mathbb{Z}/p\mathbb{Z}$ are not in $A\hat{+}B$. This gives $|A\hat{+}B| \geq p - 2 \geq |A| + |B| - 2$. A contradiction! Thus, we must have $t \geq |A|$. \square

Theorem 7. *Let sets $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ be nonempty sets such that $p \geq |A| + |B|$, where p is a prime. Suppose $|A| \geq 5$ and (A, B) is a critical pair. If A is a standard set, then (A, B) is a standard pair.*

Proof. Define A and B in the same way as in Theorem 6. According to Theorem 6, the length of the largest gap in B with respect to d is not less than $|A|$. Denote the largest gap as $[u, v]_d$, then $(u - 1)d \in B$. $A = \{id : i = 0, 1, \dots, |A| - 1\}$ gives

$$\{(u - 1)d\}\hat{+}A = \{(u - 1 + i)d : i = 0, 1, \dots, |A| - 1\} \subseteq A\hat{+}B.$$

Since $0 \in A$, $\{0\}\hat{+}B \subseteq A\hat{+}B$. According to the definition of u , we know that

$$(\{(u - 1)d\}\hat{+}A) \cap (\{0\}\hat{+}B) = \{(u - 1)d\}.$$

Observing that

$$\begin{aligned} |A\hat{+}B| &= |A| + |B| - 3 \\ &\geq |(\{(u - 1)d\}\hat{+}A) \cup (\{0\}\hat{+}B)| \\ &= |(\{(u - 1)d\}\hat{+}A)| + |(\{0\}\hat{+}B)| - 1 \\ &\geq (|A| - 1) + (|B| - 1) - 1 \\ &= |A| + |B| - 3, \end{aligned}$$

all equalities must hold. Therefore, $\{(u - 1)d\} \in A$, $0 \in B$ and

$$(5.1) \quad A\hat{+}B = (\{(u - 1)d\}\hat{+}A) \cup (\{0\}\hat{+}B).$$

Define $X = (\{(u - 1)d\}\hat{+}A) \cup (\{0\}\hat{+}B)$. We can prove that $(w + 1)d \in B$ for $\forall wd \in B$ with $w \neq 1$ and $w \neq (u - 1)$. If not, $(w + 1)d \in (A\hat{+}B) \setminus X$, which is not possible. Applying this argument, we get $d \in B$, for $0 \in B$. Similarly, consider $0 + 2d$, then $0 + 2d = 2d \in B$. So we have $xd \in B$ for $\forall x \notin [u, v]_d$ by repeating the previous argument. In particular, B is a standard set and $B = \{b + td : t = 0, 1, \dots, |B| - 1\}$.

Now, we can apply a similar argument as [7] to prove that (A, B) is a standard pair. We have $A\hat{+}B = \{sd + (b + td) : 0 \leq s \leq |A| - 1, 0 \leq t \leq |B| - 1, sd \neq b + td\}$. Since $sd + (b + td) = (s \pm 1)d + b + (t \mp 1)d$, then even if $sd = b + td$, we have the sum be written into the sum of two distinct elements from A and B unless $s = t = 0$ or $s = |A| - 1$ and $t = |B| - 1$. Therefore, $A\hat{+}B = A + B$ unless $b = 0$ or $(|A| - 1)d = b + (|B| - 1)d$. By putting $b' = b + (|B| - 1)d$ and forming the arithmetic progression with the common difference $d' = -d$, we can

reduce the second case to the first one. So, $A \hat{+} B = A + B$ unless $b = 0$. Since $A + B \geq \min\{p, |A| + |B| - 1\} > |A| + |B| - 3$, we must have $b = 0$.

Thus, we can write

$$A \hat{+} B = \{sd + td \pmod p : sd \in A, td \in B, sd \neq td\}.$$

If $sd = td$ for $s \neq t$ (say without the loss of generality that $s > t$), then

$$(s - t)d \equiv 0 \pmod p.$$

Because $d \not\equiv 0 \pmod p$, $p \mid (s - t)$. By our definition for p ,

$$|A| \geq (s - t) \geq p > |A| + |B| > |A|,$$

which is a contradiction. We now must conclude that $sd = td$ implies $s = t$.

Again, for the case where $sd = td$, we can write

$$sd + td = (s \pm 1)d + (t \mp 1)d,$$

unless $s, t = 0$ or $s = t = |A| - 1 = |B| - 1$. However, if $|A| \neq |B|$, then we only get the case $s = t = 0$, which means that

$$|A \hat{+} B| \geq |A + (B \setminus \{0\})| \geq |A| + (|B| - 1) - 1 = |A| + |B| - 2,$$

which is also a contradiction. Therefore, we must have $|A| = |B|$ and this completes the proof. \square

6. CONCLUDING REMARKS & FURTHER THOUGHTS

We have given an elegant and completely elementary proof for the inverse Erdős-Heilbronn problem in \mathbb{Z} and give some partial results on the elementary proof for the inverse Erdős-Heilbronn problem in $\mathbb{Z}/p\mathbb{Z}$. Our strategies in \mathbb{Z} need to be further improved to apply to $\mathbb{Z}/p\mathbb{Z}$, for we are considering the equations under the meaning of module p in $\mathbb{Z}/p\mathbb{Z}$.

For Theorem 5, we add the technical condition of $a_m + b_n < p$ in order to apply the theorems that we have obtained in \mathbb{Z} to $\mathbb{Z}/p\mathbb{Z}$. For Theorem 6 and Theorem 7, we drop this technical condition and ask $p \geq |A| + |B|$ instead of $p \geq |A| + |B| - 2$ in the case of \mathbb{Z} to complete the proof of our results.

Through Theorem 7, we improve Theorem 5.1 in [7], which gives an elementary proof of the inverse Erdős-Heilbronn problem in $\mathbb{Z}/n\mathbb{Z}$ under the condition that elements in sets A and B for arithmetic progressions with the same common difference, by giving an elementary proof in $\mathbb{Z}/p\mathbb{Z}$ that only requires $p \geq |A| + |B|$ and A to be a standard set.

Moreover, we may very likely guess that an elementary proof in $\mathbb{Z}/p\mathbb{Z}$ can be achieved through an analogy of Vosper's elementary proof [9] on the inverse Cauchy-Davenport problem.

In addition, through of elementary proof in the case of \mathbb{Z} , we give an explicit description of $A \hat{+} B$ as the union of $(a_{max} \hat{+} B) \cup (A \hat{+} b_{min})$, so we may expect in general, when $|A \hat{+} B|$ is close to $|A| + |B|$ in \mathbb{Z} , $A \hat{+} B$ could almost be written as

a union of such copies. Similar results may very possibly be found in $\mathbb{Z}/p\mathbb{Z}$ if a completely elementary proof is found as hinted by (5.1).

REFERENCES

- [1] A.L. Cauchy, *Recherches sur les nombres*, J. École polytech, **9** (1813) 99–116.
- [2] H. Davenport, *On the addition of residue classes*, Journal of the London Mathematical Society, **10** (1935) 30–32.
- [3] P. Erdős and H. Heilbronn, *On the addition of residue classes modulo p* , Acta Arith., **9** (1964) 149–159.
- [4] J.A. Dias da Silva and Y.O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc., **26** (1994) 140–146.
- [5] N. Alon, M.B. Nathanson, and I. Ruzsa, *Adding distinct congruence classes modulo a prime*, American Mathematical Monthly, **102** (1995) 250–255.
- [6] Gy. Károlyi, *Restricted set addition: The exceptional case of the Erdős-Heilbronn conjecture*, Journal of Combinatorial Theory A, **116** (2009) 741–746.
- [7] S.M. Jayasuriya, S.D. Reich, and J.P. Wheeler, *On the inverse Erdős-Heilbronn problem for restricted set addition in finite groups*, <https://arxiv.org/pdf/1210.6509.pdf>.
- [8] M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics 165, Springer (1996).
- [9] A.G. Vosper, *The Critical Pairs of Subsets of a Group of Prime Order*, Journal of the London Mathematical Society, **31** (1956) 200–205.

THE EXPERIMENTAL HIGH SCHOOL ATTACHED TO BEIJING NORMAL UNIVERSITY, 1#, ZHONGJINGJI
DAO, XICHENG DISTRICT, BEIJING, CHINA, 100032.
Email address: Leo176637@hotmail.com