ACTA ARITHMETICA
147.4 (2011)

An application of Tao's analytic method to restricted sumsets

by

Song Guo (Huaian)

1. Introduction. Let p be a prime, and A, B be finite subsets of $\mathbb{Z}_p$. Set

$$A + B = \{a + b : a \in A,\, b \in B\}, \tag{1}$$

$$A \dot{+} B = \{a + b : a \in A,\, b \in B,\, a \neq b\}. \tag{2}$$

The Cauchy–Davenport theorem [4] asserts that

$$|A + B| \geq \min\{p, |A| + |B| - 1\}. \tag{3}$$

A well-known result on restricted sumsets states that

$$|A \dot{+} A| \geq \min\{p, 2|A| - 3\}; \tag{4}$$

this was conjectured by P. Erdős and H. Heilbronn [6] in 1964 and confirmed by J. A. Dias da Silva and Y. O. Hamidoune [5] in 1994. In 1995-1996 N. Alon, M. B. Nathanson and I. Z. Ruzsa [2] proposed a polynomial method in this field and showed that if $|B| > |A| > 0$ then

$$|A \dot{+} B| \geq \min\{p, |A| + |B| - 2\}. \tag{5}$$

By the polynomial method, many interesting results have been obtained (cf. [1], [2], [3], [8], [9], [10], [11]).

In 2005, Terence Tao developed an analytic method for restricted sumsets and gave a simple proof of the Cauchy–Davenport theorem, applying a new form of the uncertainty principle for the Fourier transform. In [7] S. Guo and Z. Sun extended this method and gave a new proof of the Erdős–Heilbronn conjecture.

2010 *Mathematics Subject Classification*: Primary 11B75; Secondary 05A05, 11P99.
Key words and phrases: restricted sumsets, Fourier transform, uncertainty principle.

DOI: 10.4064/aa147-4-2

In this article we give a new application of Tao's method and obtain the following theorem which contains the inequalities (2)–(5).

THEOREM 1. *Let A and B be non-empty subsets of $\mathbb{Z}_p$ where p is an odd prime, and*

$$C = A +_S B = \{a + b : a \in A,\, b \in B,\, a - b \notin S\} \tag{6}$$

with $S \subsetneq \mathbb{Z}_p$. Then

$$|C| \geq \min\{p, |A| + |B| - |S| - r\}, \tag{7}$$

where

$$r = \begin{cases} 2 & \text{if } |A| = |B| \text{ and } |S| \equiv 1 \pmod 2, \\ 1 + \min\{\lfloor |S|/2 \rfloor, \big||A| - |B|\big|\} & \text{otherwise.} \end{cases} \tag{8}$$

In [7] the author and Z. Sun conjectured that $\min\{\lfloor |S|/2 \rfloor, \big||A| - |B|\big|\}$ can be eliminated, hence

$$r = \begin{cases} 2 & \text{if } |A| = |B| \text{ and } |S| \equiv 1 \pmod 2, \\ 1 & \text{otherwise.} \end{cases} \tag{9}$$

When $|S|$ is even, this conjecture was proposed by Q. Hou and Z. Sun in [8].

2. Proof of the main result. Without loss of generality, we let $|A| \leq |B|$ (note that $A +_S B = B +_{-S} A$). Set $m = |S|$. When $|A| = 1$ or $|A| + |B| \leq m + r$ or $m = 0$, (7) holds trivially. Assume that $|A| \geq 2$, $|A| + |B| \geq m + r + 1$ and $1 \leq m \leq p - 1$. For any $a, b \in \mathbb{Z}$, we let $[a, b] = \{x \in \mathbb{Z} : a \leq x \leq b\}$. For an assertion P we adopt Iverson's notation

$$[\![P]\!] = \begin{cases} 1 & \text{if } P \text{ holds,} \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

For any function $f : \mathbb{Z}_p \to \mathbb{C}$, we define its *support* $\operatorname{supp}(f)$ and its *Fourier transform* $\hat{f} : \mathbb{Z}_p \to \mathbb{C}$ as follows:

$$\operatorname{supp}(f) = \{x \in \mathbb{Z}_p : f(x) \neq 0\}, \tag{11}$$

$$\hat{f}(x) = \sum_{a \in \mathbb{Z}_p} f(a) e_p(ax), \qquad x \in \mathbb{Z}_p, \tag{12}$$

where $e_p(y) = e^{-2\pi i y/p}$ for $y \in \mathbb{Z}_p$.

Tao obtained the following result in [12]:

LEMMA 1. *Let p be an odd prime. If $f : \mathbb{Z}_p \to \mathbb{C}$ is not identically zero, then*

$$|\operatorname{supp}(f)| + |\operatorname{supp}(\hat{f})| \geq p + 1. \tag{13}$$

Given two non-empty subsets A and B of $\mathbb{Z}_p$ with $|A| + |B| \geq p + 1$, we can find a function $f : \mathbb{Z}_p \to \mathbb{C}$ with $\operatorname{supp}(f) = A$ and $\operatorname{supp}(\hat{f}) = B$.

Note that inequality (13) was also discovered independently by András Biró.

Definition. A pair of sets $(\hat{A},\hat{B})$ is *m-good* if $\overline{0}\in\hat{A}$ and $\overline{p-m}\in\hat{B}$, and there is no $t\in[0,m-1]$ such that $\overline{t-m}\in\hat{A}$ and $\overline{-t}\in\hat{B}$.

Definition. For a pair $(\hat{A},\hat{B})$ we put

$$(\hat{A},\hat{B})_m=\bigcup_{t=0}^{m}((\hat{A}-\overline{t})\cap(\hat{B}+\overline{t-m})).$$

Lemma 2. *Let A,B,C be as in Theorem 1 and $\hat{A},\hat{B}$ be subsets of $\mathbb{Z}_p$ with $|\hat{A}|\geq p+1-|A|$ and $|\hat{B}|\geq p+1-|B|$. If $(\hat{A},\hat{B})$ is m-good, then $|C|\geq p+1-|(\hat{A},\hat{B})_m|$.*

Proof. By Lemma 1 there are functions $f,g:\mathbb{Z}_p\to\mathbb{C}$ such that $\operatorname{supp}(f)=A$, $\operatorname{supp}(\hat{f})=\hat{A}$, $\operatorname{supp}(g)=B$ and $\operatorname{supp}(\hat{g})=\hat{B}$. Now we define a function $F:\mathbb{Z}_p\to\mathbb{C}$ by

$$F(x)=\sum_{a\in\mathbb{Z}_p}f(a)g(x-a)\prod_{d\in S}(e_p(x-a)-e_p(a-d)),\tag{14}$$

as in [7]. For each $x\in\operatorname{supp}(F)$, there exists $a\in\operatorname{supp}(f)$ with $x-a\in\operatorname{supp}(g)$ and $d:=a-(x-a)\notin S$, hence $x=a+(x-a)\in C$. Therefore

$$\operatorname{supp}(F)\subseteq C.\tag{15}$$

For any $x\in\mathbb{Z}$ we have

$$\hat{F}(x)=\sum_{b\in\mathbb{Z}_p}F(b)e_p(bx)=\sum_{a\in\mathbb{Z}_p}\sum_{b\in\mathbb{Z}_p}f(a)g(b-a)e_p(bx)P(a,b),$$

where

$$\begin{aligned}P(a,b)&=\prod_{d\in S}(e_p(b-a)-e_p(a-d))\\&=\sum_{T\subseteq S}(-1)^{|T|}e_p\left((|S|-|T|)(b-a)\right)e_p\Big(|T|a-\sum_{d\in T}d\Big).\end{aligned}$$

Therefore

$$\begin{aligned}\hat{F}(x)&=\sum_{T\subseteq S}(-1)^{|T|}e_p\Big(-\sum_{d\in T}d\Big)\sum_{a\in\mathbb{Z}_p}f(a)e_p(ax+|T|a)\\&\quad\times\sum_{b\in\mathbb{Z}_p}g(b-a)e_p\left((b-a)x+(|S|-|T|)(b-a)\right)\\&=\sum_{T\subseteq S}(-1)^{|T|}e_p\Big(-\sum_{d\in T}d\Big)\hat{f}(x+\overline{|T|})\hat{g}(x+\overline{m-|T|}).\end{aligned}$$

By the definition of m-good pair we have

$$\hat{F}(\overline{p-m}) = (-1)^m e_p\Big(-\sum_{d\in S} d\Big)\hat{f}(\overline{0})\hat{g}(\overline{p-m}) \neq 0,$$

so $\hat{F}$ is not identically zero.

Suppose that $x \in \operatorname{supp}(\hat{F})$. Then there is a subset T of S with $|T| = t$ such that $x + \bar{t} \in \hat{A} = \operatorname{supp}(\hat{f})$ and $x + \overline{m-t} \in \hat{B} = \operatorname{supp}(\hat{g})$, hence $x \in (\hat{A}, \hat{B})_m$. Thus $\operatorname{supp}(\hat{F}) \subseteq (\hat{A}, \hat{B})_m$. By Lemma 1, we have

$$|C| \geq |\operatorname{supp}(F)| \geq p + 1 - \operatorname{supp}(\hat{F}) \geq p + 1 - |(\hat{A}, \hat{B})_m|. \ \blacksquare$$

Below we construct a suitable m-good pair $(\hat{A}, \hat{B})$ so that $|[\hat{A}, \hat{B}]_m|$ is small and hence $|C|$ is large. All the cases needed to be proved are listed in the following table.

The hypothesis on the cardinality of A and B	r	Proof
$\lvert A\rvert + \lvert B\rvert \leq m + r$ or $\lvert A\rvert = 1$ or $m = 0$	–	Trivial
$\lvert A\rvert + \lvert B\rvert \geq p - m + 1$	–	Lemma 3
$\lvert A\rvert = \lvert B\rvert \leq (p-m)/2$ and $m \equiv 1 \pmod 2$	2	Lemma 4
$2\lvert A\rvert \leq m$ and $[\![2 \nmid m]\!] \leq n = \lvert B\rvert - \lvert A\rvert \leq \lfloor m/2 \rfloor$	$n+1$	Trivial
$m + 1 \leq 2\lvert A\rvert \leq \lvert A\rvert + \lvert B\rvert \leq p - m$		
and $[\![2 \nmid m]\!] \leq n = \lvert B\rvert - \lvert A\rvert \leq \lfloor m/2 \rfloor$	$n+1$	Lemma 5
$m + r \leq \lvert A\rvert + \lvert B\rvert \leq p - m$ and $\lvert B\rvert - \lvert A\rvert \geq (m+1)/2$	$\lfloor m/2 \rfloor + 1$	Lemma 6

We note that $|A| + |B| - m - r = 2|A| - m - 1 \leq 0$ when $2|A| \leq m$ and $[\![2 \nmid m]\!] \leq n \leq \lfloor m/2 \rfloor$.

Lemma 3. *Suppose that* $|A| + |B| \geq p - m + 1$. *Let* $\hat{A} = \{\overline{2i} : i = 0, 1, \ldots, k-1\}$ *with* $k = p+1-|A|$ *and* $\hat{B} = \{\overline{p-m-2j} : j = 0, 1, \ldots, l-1\}$ *with* $l = k + 1 - |B|$. *Then* $(\hat{A}, \hat{B})$ *is* m*-good with* $|(\hat{A}, \hat{B})_m| = 1$.

Proof. Let $x \in (\hat{A}, \hat{B})_m$. Suppose that $t \in [0, m]$, $x + \bar{t} \in \hat{A}$ and $x + \overline{m-t} \in \hat{B}$. Then there are $i \in [0, k-1]$ and $j \in [0, l-1]$ such that $x + t \equiv 2i \pmod p$ and $x + m - t \equiv p - m - 2j \pmod p$. Thus $2i - t \equiv x \equiv p - 2m - 2j + t \pmod p$ and hence $2(i + j + m - t) \equiv 0 \pmod p$. Since $k+l = 2p+2-|A|-|B| \leq p-m+1$ and $0 \leq i+j+m-t \leq k+l+m-2 \leq p-1$, we must have $i + j + m - t = 0$ and hence $i = j = 0$ and $t = m$.

In view of the above, $(\hat{A}, \hat{B})$ is m-good with $(\hat{A}, \hat{B})_m = \{p - m\}$. $\blacksquare$

Lemma 4. *Suppose that* $|A| = |B| \leq (p-m)/2$ *and* $m \equiv 1 \pmod 2$. *Let* $\hat{A} = \{\overline{2i} : i = 0, 1, \ldots, k-1\}$ *with* $k = p + 2 - |A|$ *and* $\hat{B} = \hat{A} \setminus \{\overline{0}\}$. *Then* $(\hat{A}, \hat{B})$ *is* m*-good with* $|(\hat{A}, \hat{B})_m| \leq 2k - 1 + m - p$.

Proof. Since

$$2k - 2 = 2p + 2 - 2|A| \geq p + m - 2 \geq p - m,$$

we have $\overline{p-m} \in \hat{B}$. Let $x \in [p-m, p-1]$ with $\overline{x} \in \hat{A}$. Then $x \equiv 0 \pmod 2$. For any $t \in [0, m-1]$, we have

$$\overline{p-m+t} \in \hat{A} \ \Rightarrow\ t \equiv 0 \pmod 2,$$
$$\overline{p-m+m-t} \in \hat{B} \ \Rightarrow\ t \equiv 1 \pmod 2.$$

Thus $(\hat{A}, \hat{B})$ is m-good.

Observe that $2k-2-p = p+2-2|A| \le p-m$. Then for any $x \in [\max\{0, 2k-1-p\}, p-1]$ with $\overline{x} \in \hat{A}$, we must have $x \equiv 0 \pmod 2$. Let $x \in [\max\{0, 2k-1-p\}, p-m-1]$ and $t \in [0, m]$. Clearly

$$\overline{x+t} \in \hat{A} \ \Rightarrow\ x+t \equiv 0 \pmod 2,$$
$$\overline{x+m-t} \in \hat{B} \ \Rightarrow\ x+m-t \equiv 0 \pmod 2.$$

Recalling $m \equiv 1 \pmod 2$, we have

$$(\hat{A}, \hat{B})_m \cap \{\overline{x} :\ x \in [\max\{0, 2k-1-p\}, p-m-1]\} = \emptyset. \tag{16}$$

Suppose that $2k-1-p < 0$. By the definition of $\hat{A}$,

$$\hat{A} \cap \{\overline{x} : x \in [2k-1, p-1]\} = \emptyset.$$

For any $x \in [2k-1, p-1]$ and $t \in [0, m]$, we have $x+t, x+m-t \in [2k-1, p+m-1]$. If $\overline{x+t} \in \hat{A}$, then $p \le x+t \le p+m-1$ and $x+t-p \equiv 0 \pmod 2$. For $\overline{x+m-t} \in \hat{B}$, we have $p \le x+m-t \le p+m-1$ and $x+m-t-p \equiv 0 \pmod 2$. Thus $\overline{x} \notin (\hat{A}, \hat{B})_m$ since $m \equiv 1 \pmod 2$. So we have

$$(\hat{A}, \hat{B})_m \cap \{\overline{x} :\ x \in [2k-1, p-1]\} = \emptyset. \tag{17}$$

Combining (16) and (17), we obtain

$$(\hat{A}, \hat{B})_m \cap \{\overline{x} :\ x \in [2k-1-p, p-m-1]\} = \emptyset.$$

Therefore

$$|(\hat{A}, \hat{B})_m| \le p - (p-m-1-(2k-2-p)) \le 2k-1+m-p. \ \blacksquare$$

Lemma 5. *Suppose that $m+1 \le 2|A| \le |A|+|B| \le p-m$. Set $k = p+1-|A|$, $l = p+1-|B|$ and $n = k-l$. Suppose that $[\![2 \nmid m]\!] \le n \le \lfloor m/2 \rfloor$. Let $\hat{A} = \{\overline{2i} : i = 0, 1, \ldots, k-1\}$ and*

$$\hat{B} = \{\overline{x} : x \in [1, 2k-1-p]\}$$
$$\cup \{\overline{x} : x \equiv p-m \pmod 2\ \&\ x \in [2k-p, p+1+2l-2k]\}.$$

Then $(\hat{A}, \hat{B})$ is m-good with $|(\hat{A}, \hat{B})_m| \le 2k+m-p$.

Proof. Note that

$$|\hat{B}| = 2k-1-p + \frac{p + [\![2 \nmid m]\!] + 2l - 2k - (2k-p-1-[\![2 \mid m]\!])}{2} = l.$$

Since $k-l \le \lfloor m/2 \rfloor$, we have $p-m \le p+1+2l-2k$ and hence $\overline{p-m} \in \hat{B}$.

Clearly,

$$m+1 \le p+1-(|A|+|B|) \le p+1-2|A| = 2k-1-p \le p-m.$$

For any $t \in [0, m-1]$, we have

$$\overline{p-m+t} \in \hat{A} \;\Rightarrow\; p-m+t \equiv 0 \pmod 2,$$
$$\overline{p-m+m-t} \in \hat{B} \;\Rightarrow\; m-t \equiv 0 \pmod 2.$$

Thus $(\hat{A}, \hat{B})$ is m-good.

If $x \in [2k-p, p-m-1]$ and $t \in [0, m]$, then $x+t, x+m-t \in [2k-p, p-1]$, hence

$$\overline{x+t} \in \hat{A} \;\Rightarrow\; x+t \equiv 0 \pmod 2,$$
$$\overline{x+m-t} \in \hat{B} \;\Rightarrow\; x+m-t \equiv p-m \pmod 2,$$

thus $\overline{x} \notin [\hat{A}, \hat{B}]_m$. So

$$(\hat{A}, \hat{B})_m \cap \{\overline{x} : x \in [2k-p, p-m-1]\} = \emptyset,$$

and hence

$$|(\hat{A}, \hat{B})_m| \le p - (p-m-1-(2k-p-1)) \le 2k+m-p. \;\blacksquare$$

Lemma 6. *Suppose that* $m + \lfloor m/2 \rfloor + 1 \le |A| + |B| \le p - m$ *and* $|B| - |A| \ge (m+1)/2$. *Set* $k = p+1-|A|$ *and* $l = p+1-|B|$. *Let* $\hat{A} = \{\overline{2i} : i = 0, 1, \ldots, k-1\}$ *and*

$$\hat{B} = \begin{cases} \{\overline{x} : x \in [p-m-l+1, p-m]\} & \text{if } k \ge p - \lfloor m/2 \rfloor, \\ \{\overline{p-m-2i} : i = 0, 1, \ldots, l-1\} & \text{if } \max\{2, l\} \le p-k-\lfloor m/2 \rfloor + 1, \\ \{\overline{x} : x \in [2k-p, p-m] \text{ and } x \equiv p-m \pmod 2\} & \\ \qquad \cup \{\overline{x} : x \in [k-l-\lfloor (m-1)/2 \rfloor, 2k-1-p]\} & \text{otherwise.} \end{cases}$$

Then $(\hat{A}, \hat{B})$ *is* m-*good with* $|(\hat{A}, \hat{B})_m| \le k+l+\lfloor 3m/2 \rfloor - p$.

Proof. Note that if $l > p-k-\lfloor m/2 \rfloor + 1$, then

$$|B| = \frac{p-m-(2k-p-1-[\![2 \mid m]\!])}{2} + 2k-p-\left(k-l-\left\lfloor \frac{m-1}{2} \right\rfloor\right) = l.$$

For any $t \in [0, m-1]$, $\overline{p-m+m-t} = \overline{p-t} \notin \hat{B}$. So $(\hat{A}, \hat{B})$ is m-good.

Case 1: $k \ge p - \lfloor m/2 \rfloor$. For any $x \in \mathbb{Z}_p$ and $t \in [0, m]$ with $\overline{x+m-t} \in \hat{B}$, we must have $x \in [p-2m-l+1, p-m]$. Thus $(\hat{A}, \hat{B})_m \subseteq [p-2m-l+1, p-m]$. As $k \ge p - \lfloor m/2 \rfloor$, we obtain

$$|(\hat{A}, \hat{B})_m| \le p-m-(p-2m-l+1)+1 = m+l \le k+l+\lfloor 3m/2 \rfloor - p.$$

Case 2: $\max\{2, l\} \le p-k-\lfloor m/2 \rfloor + 1$. For any $x \in [1-m, p-2m-2l+1]$ and $t \in [0, m]$, we have

$$1-m \le x+m-t \le p-m-2l+1,$$

so $\overline{x+m-t} \notin \hat{B}$ and hence $\overline{x} \notin (\hat{A}, \hat{B})_m$.

For any $x \in [2k-p-1, p-m-1]$ and $t \in [0,m]$, clearly

$$2k-p-1 \le x+t, x+m-t \le p-1,$$

hence

$$\overline{x+t} \in \hat{A} \;\Rightarrow\; x+t \equiv 0 \pmod 2,$$
$$\overline{x+m-t} \in \hat{B} \;\Rightarrow\; x+m-t \equiv p-m \pmod 2,$$

thus $\overline{x} \notin (\hat{A},\hat{B})_m$ since $2 \nmid p$.

In view of the above,

$$(\hat{A},\hat{B})_m \cap \{\overline{x} : x \in [2k-p-1, p-m-1] \cup [1-m, p-2m-2l+1]\} = \emptyset.$$

Thus

$$|(\hat{A},\hat{B})_m| \le p-(3p-2m-2k-2l+2) = 2k+2l+2m-2p-2.$$

Recall that $l \le p-k-\lfloor m/2 \rfloor + 1$, so we have

$$|(\hat{A},\hat{B})_m| \le k+l+2m-2p-2+p-\lfloor m/2\rfloor+1 \le k+l+\lfloor 3m/2\rfloor - p.$$

Case 3: $l > p-k-\lfloor m/2\rfloor+1 \ge 2$. If $x \in [1-m, k-l-\lfloor (m-1)/2\rfloor - m-1]$ and $t \in [0,m]$, then $\overline{x+m-t} \notin \hat{B}$ and hence $\overline{x} \notin (\hat{A},\hat{B})_m$. For any $x \in [2k-p, p-m-1]$ and $t \in [0,m]$, clearly

$$2k-p \le x+t, x+m-t \le p-1,$$

hence

$$\overline{x+t} \in \hat{A} \;\Rightarrow\; x+t \equiv 0 \pmod 2,$$
$$\overline{x+m-t} \in \hat{B} \;\Rightarrow\; x+m-t \equiv p-m \pmod 2,$$

thus $\overline{x} \notin (\hat{A},\hat{B})_m$. If $x = 2k-p-1$ and $t \in [0,m]$, then

$$\overline{x+m-t} \in \hat{B} \Rightarrow m-t = 0 \Rightarrow t = m,$$

and hence

$$\overline{x+t} \in \hat{A} \;\Rightarrow\; 2k-p-1+m \equiv 0 \pmod 2.$$

Therefore $\overline{2k-p-1} \in (\hat{A},\hat{B})_m$ if and only if $2 \mid m$.

In view of the above,

$$(\hat{A},\hat{B})_m \cap \left\{\overline{x} : x \in \left[1-m, k-l-\frac{3m+[\![2\nmid m]\!]}{2}\right] \cup [2k-p-[\![2\nmid m]\!], p-m-1]\right\} = \emptyset.$$

Thus

$$|(\hat{A},\hat{B})_m| \le p-(2p-k-l-\lfloor 3m/2\rfloor) = k+l+\lfloor 3m/2\rfloor - p.$$

We are done. ∎

Combining the above lemmas we immediately obtain the desired results of Theorem 1.

Acknowledgments. I would like to thank the referee and my supervisor Professor Zhi-Wei Sun for many helpful suggestions.

The author is supported by Natural Science Research Project of Ordinary Universities in Jiangsu Province of China (grant 08KJB110002) and the National Natural Science Foundation of China (grants 10911078 and 11001098).

References

[1] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. 8 (1999), 7–29.

[2] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *The polynomial method and restricted sums of congruence classes*, J. Number Theory 56 (1996), 404–417.

[3] H. Q. Cao and Z. W. Sun, *On sums of distinct representatives*, Acta Arith. 87 (1998), 159–169.

[4] H. Davenport, *On the addition of residue classes*, J. London Math. Soc. 10 (1935), 30–32.

[5] 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.

[6] P. Erdős and H. Heilbronn, *On the addition of residue classes mod* p, Acta Arith. 9 (1964), 149–159.

[7] S. Guo and Z. W. Sun, *A variant of Tao's method with application to restricted sumsets*, J. Number Theory 129 (2009), 434–438.

[8] Q. H. Hou and Z. W. Sun, *Restricted sums in a field*, Acta Arith. 102 (2002), 239–249.

[9] J. X. Liu and Z. W. Sun, *Sums of subsets with polynomial restrictions*, J. Number Theory 97 (2002), 301–304.

[10] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math. 165, Springer, New York, 1996.

[11] H. Pan and Z. W. Sun, *A lower bound for* $|\{a+b : a \in A,\ b \in B,\ P(a,b) \neq 0\}|$, J. Combin. Theory Ser. A 100 (2002), 387–393.

[12] T. Tao, *An uncertainty principle for cyclic groups of prime order*, Math. Res. Lett. 12 (2005), 121–127.

Song Guo
School of Mathematical Science
Huaiyin Normal University
Huaian 223300, People's Republic of China
E-mail: guosong77@hytc.edu.cn

Received on 10.8.2009
and in revised form on 6.4.2010 (6116)