MULTIPLE SET ADDITION IN $\mathbb{Z}_p$

Tomasz Schoen[1]
Department of Discrete Mathematics, Adam Mickiewicz University, Poznań, Poland
schoen@amu.edu.pl

Received: 2/22/03, Revised: 10/6/03, Accepted: 11/1/03, Published: 11/5/03

Abstract

It is shown that there exists an absolute constant H such that for every $h > H$, every prime p, and every set $A \subseteq \mathbb{Z}_p$ such that $10 \leq |A| \leq p(\ln h)^{1/2}/(9h^{9/4})$ and $|hA| \leq h^{3/2}|A|/(8(\ln h)^{1/2})$, the set A is contained in an arithmetic progression modulo p of cardinality $\max_{1\leq j\leq h-1} \frac{|hA|-P_j(|A|)}{h-j} + 1$, where $P_j(n) = \frac{(j+1)j}{2}n - j^2 + 1$. This result can be viewed as a generalization of Freiman's "2.4-theorem".

1. Introduction

For a non-empty subset A of an additively written group and an integer $h \geq 2$ the h-sumset of A is defined as

$$hA = \{a_1 + \cdots + a_h : a_1, \ldots, a_h \in A\};$$

and by a sumset we mean a 2-sumset of A. The following well-known "2.4-theorem" of Freiman [2] describes the structure of sets $A \subseteq \mathbb{Z}_p$ with small sumsets.

Theorem 1 (Freiman). *Let A, $|A| \leq p/35$, be a subset of $\mathbb{Z}_p$ for some prime p. If*

$$|2A| \leq 2.4|A| - 3,$$

then A is contained in an arithmetic progression of $\mathbb{Z}_p$ with $|2A| - |A| + 1$ terms.

Freiman's proof goes roughly as follows. Since A has a small sumset, the characteristic function of A has a large non-zero Fourier coefficient. Hence A is dense in some arithmetic progression $P \subseteq \mathbb{Z}_p$ of length $(p-1)/2$. The set $A' = A \cap P$ is isomorphic (in the sense of Freiman) to a subset of integers, hence one can apply to A' Freiman's additive theorem for integers, and infer that A' is contained in an arithmetic progression of cardinality $|2A'| - |A'| + 1$. As a last step one shows that $A' = A$, otherwise we would have $|2A| > 2.4|A| - 3$.

[1]Research partially supported by KBN Grant 2 P03A 007 24

In this note we generalize Freiman's theorem to h summands, provided h is large. Our main result is as follows.

Theorem 2. *There is an absolute constant H such that for every $h > H$, every prime p, and every $A \subseteq \mathbb{Z}_p$ such that $10 \leq |A| \leq \frac{p(\ln h)^{1/2}}{9h^{9/4}}$ and*

$$|hA| \leq \frac{h^{3/2}}{8(\ln h)^{1/2}}|A|,$$

the set A is contained in an arithmetic progression of cardinality $\max_{1\leq j\leq h-1} \frac{|hA|-P_j(|A|)}{h-j} + 1$, *where* $P_j(n) = \frac{(j+1)j}{2}n - j^2 + 1$.

Our approach follows the main idea of Freiman's proof. First we observe that the absolute value of some Fourier coefficient of the characteristic function of A is very close to $|A|$. We use this fact to show the existence of a large subset A' of A contained in an arithmetic progression of cardinality roughly $p(\ln h/h)^{1/2}$. Then we apply a result of Lev (Theorem 3 below) to A' and some $h_0 > (h/\ln h)^{1/2}$ to prove that A' is, in fact, contained in a much shorter arithmetic progression. Finally we employ a well-known theorem of Cauchy-Davenport to infer that $A' = A$.

In order for our method to work we have to impose some restrictions on the sizes of A and hA. Thus, we assume that $h > H$, where the value of an absolute constant H can be explicitly computed. In our result Freiman's constant "2.4" is replaced by "$h^{3/2}/4(\ln h)^{1/2}$", although one can expect that, as in Theorem 3, the assertion holds for each A with $|hA| \leq \frac{(h+1)h}{2}|A| - h^2$.

2. Auxiliary results

In this section we recall some theorems and definitions used in the proof of our main result. First we state a consequence of [3, Corollary 1] . Here and below $L(A)$ denotes the cardinality of the shortest arithmetic progression containing A.

Theorem 3 (Lev [3]). *Let $h \geq 2$ and A be a finite subset of $\mathbb{Z}$, $|A| \geq 2$ such that $|hA| \leq \frac{(h+1)h}{2}|A| - h^2$. Then*

$$L(A) \leq \max_{1\leq j\leq h-1} \frac{|hA| - P_j(|A|)}{h-j} + 1,$$

where $P_j(n) = \frac{(j+1)j}{2}n - j^2 + 1$.

Remark 1. The estimate of Theorem 3 is tight, as shows the following example given in [3]. Let $\ell \geq n-1,\ A = \{0,\ldots,n-2\} \cup \{\ell\}$ and put $k = \lceil \frac{\ell-1}{n-2} \rceil - 1$. If $h > \frac{\ell-1}{n-2}$ then it is easily seen that $|hA| = P_k(n) + (h-k)l < P_h(n)$ and

$$\max_{1\le j\le h-1} \frac{|hA| - P_j(n)}{h-j} + 1 = \ell + 1 = L(A),$$

maximum is attained for $j = k$.

Remark 2. Note that under the assumptions of Theorem 3 we have

$$L(A) \le \frac{2|hA|}{h} + 1.$$

Indeed, suppose that the maximum is attained for j_0. If $j_0 \le h/2$ then the inequality follows immediately. Assume that $j_0 > h/2$ and

$$\frac{|hA| - P_{j_0}(|A|)}{h - j_0} > \frac{2|hA|}{h}.$$

Then we have

$$|hA| > \frac{h}{2j_0 - h} P_{j_0}(|A|) \ge \min_{h/2<j\le h} \frac{h}{2j-h} P_j(|A|).$$

Since $\frac{h}{2j-h}P_j(n)$ is a strictly decreasing function of j it follows that

$$|hA| > P_h(|A|) > \frac{(h+1)h}{2}|A| - h^2,$$

contradicting the assumptions of Theorem 3.

Theorem 4 (Cauchy-Davenport). *Let p be a prime number and let A be a nonempty subset of $\mathbb{Z}_p$. Then, for every integer $h \ge 2$,*

$$|hA| \ge \min(p, h|A| - h + 1).$$

We will also need the following straightforward consequence of Theorem 4.

Corollary 1. *Let p be a prime number and let A be a nonempty subset of $\mathbb{Z}_p$ such that $|hA| < p$. Then, for every integers $h \ge h_1 \ge 2$,*

$$|h_1A| < \lfloor h/h_1 \rfloor^{-1} |hA| + 1.$$

Proof. By Cauchy-Davenport theorem, we have

$$|hA| \ge |\lfloor h/h_1 \rfloor (h_1A)| \ge \lfloor h/h_1\rfloor |h_1A| - \lfloor h/h_1 \rfloor + 1. \qquad \square$$

Let G and H be abelian groups and let $A \subseteq G$ and $B \subseteq H$. We say that a mapping $\phi : A \to B$ is a Freiman's isomorphism of order h (briefly, F_h-isomorphism), if for every $a_1, \ldots, a_h, a'_1, \ldots, a'_h \in A$ the equation

$$a_1 + \cdots + a_h = a'_1 + \cdots + a'_h$$

holds if and only if

$$\phi(a_1) + \cdots + \phi(a_h) = \phi(a'_1) + \cdots + \phi(a'_h)$$

holds. In particular F_h-isomorphisms preserve the size of h-sumsets.

3. Proof of the main theorem

For a set $S \subseteq \mathbb{Z}_p$ let $\{\hat{S}(r)\}_{r\in\mathbb{Z}_p}$ denote the Fourier coefficients of the indicator function of S $\ (\hat{S}(r) = \sum_{s\in S} e^{2\pi i r s/p}\ )$. It is easy to see that $|\hat{S}(0)| = |S|$. We recall also Parseval formula

$$\sum_{r=0}^{p-1} |\hat{S}(r)|^2 = |S|p.$$

By the definition all sums $a_1 + \cdots + a_h,\ a_1, \ldots, a_h \in A$ belong to the set hA, hence

$$\sum_{r=0}^{p-1} \hat{A}(r)^h (\hat{hA})(-r) = |A|^h p$$

and

$$\sum_{r=1}^{p-1} \hat{A}(r)^h (\hat{hA})(-r) = |A|^h p - |A|^h |hA| \geq |A|^h p/2.$$

Put $M = \max_{r\neq 0} |\hat{A}(r)|$. By Cauchy-Schwarz inequality and Parseval formula we have

$$\begin{aligned}
|A|^h p/2 &\leq \sum_{r=1}^{p-1} |\hat{A}(r)|^h |(\hat{hA})(-r)| \leq M^{h-1} \sum_{r=1}^{p-1} |\hat{A}(r)||(\hat{hA})(-r)| \\
&\leq M^{h-1} \Big(\sum_{r=1}^{p-1} |\hat{A}(r)|^2\Big)^{1/2} \Big(\sum_{r=1}^{p-1} |(\hat{hA})(-r)|^2\Big)^{1/2} \\
&< M^{h-1} |A|^{1/2} |hA|^{1/2} p.
\end{aligned}$$

Thus,

$$\begin{aligned}
M &> \Big(\frac{|A|}{4|hA|}\Big)^{\frac{1}{2(h-1)}} |A| \geq (h^{-3/2})^{\frac{1}{2(h-1)}} |A| \\
&= \exp\Big(-\frac{3}{4}\frac{\ln h}{h-1}\Big)|A| > \Big(1 - \frac{3}{4}\frac{\ln h}{h-1}\Big)|A| \\
&> \Big(1 - \frac{\ln h}{h}\Big)|A|. \qquad (1)
\end{aligned}$$

Let $r_0 \in \mathbb{Z}_p \setminus \{0\}$ be an element with $|\hat{A}(r_0)| = M$. Put $\gamma = \arg \hat{A}(r_0),\ \alpha = \arccos\Big(1 - \frac{2\ln h}{h}\Big)$, so that $\alpha \leq \pi\big(\frac{\ln h}{2h}\big)^{1/2}$. Define

$$B = \Big\{r_0 a\colon a \in A \text{ and } d\big(\gamma - 2\pi\frac{(r_0 a)_p}{p}\big) \leq \alpha\Big\},$$

where $(r_0a)_p$ stands for the least non-negative integer congruent to r_0a modulo p and $d(x)$ denotes the distance of x from the nearest number of the form $2\pi k,\ k\in\mathbb{Z}$. It follows that

$$|\hat{A}(r_0)|\le |B|+(\cos\alpha)(|A|-|B|),$$

and by (1)

$$|B|\ge \frac{1-\frac{\ln h}{h}-\cos\alpha}{1-\cos\alpha}|A|=|A|/2. \tag{2}$$

Observe that B is F_{h_0}-isomorphic to a subset of integers, where $h_0=\lfloor 2\pi/\alpha\rfloor$. Then $h_0\ge 2\left(\frac{h}{\ln h}\right)^{1/2}$ and by Corollary 1, (1), and (2), we get

$$\begin{aligned}|h_0B| &\le \frac{|hB|}{\lfloor h/h_0\rfloor}+1\le \frac{2h_0|hA|}{h}+1\le \frac{h_0h^{1/2}|A|}{4(\ln h)^{1/2}}+1\\ &\le \frac{h_0h^{1/2}|B|}{2(\ln h)^{1/2}}+1\le \frac{h_0^2}{4}|B|+1\\ &< \frac{(h_0+1)h_0|B|}{2}-h_0^2+1.\end{aligned}$$

Thus, one can apply Theorem 3 to the set B, so that B is contained in an arithmetic progression in $\mathbb{Z}_p$ of size

$$\begin{aligned}\max_{1\le j\le h_0-1}\frac{|h_0B|-P_j(|B|)}{h_0-j}+1 &\le \frac{2|h_0B|}{h_0}+1\le \frac{2|hB|}{h_0\lfloor h/h_0\rfloor}+2\\ &\le \frac{4|hA|}{h}+2\le \frac{h^{1/2}|A|}{2(\ln h)^{1/2}}+2\\ &\le \frac{p}{2h^{7/4}}.\end{aligned} \tag{3}$$

Let A_1 be any subset of A of the maximum cardinality, contained in an arithmetic progression of cardinality $\lfloor p/h\rfloor$. From (2) and (3) it follows that $|A_1|\ge |A|/2$. An argument analogous to that used in (3) shows that A_1 is contained in an arithmetic progression of size at most $p/(2h^{7/4})$. Without loss of generality we may assume that A_1 is a subset of the arithmetic progression with the common difference 1 centered at 0 that means $\|a\|\le p/(4h^{7/4})$ for every $a\in A_1$, where $\|x\|=\min\big((x)_p,(p-x)_p\big)$. If $a_0\in A\setminus A_1$, then

$$\|ka_0\|\le \frac{p}{2h},$$

for some $k\in\mathbb{N}$. Let k be the smallest number with this property. Observe that if $k\le h^{3/4}$, then for every $a\in A_1$

$$\|ka\|\le k\|a\|\le h^{3/4}\frac{p}{4h^{7/4}}<\frac{p}{2h},$$

so the set $A_1\cup\{a_0\}$ is contained in an arithmetic progression of size at most p/h and the common difference k^{-1} (the multiplicative inverse of k in $\mathbb{Z}_p$), contradicting the maximality of A_1. Hence we may assume that $k \geq h^{3/4}$. Put $\ell = \lfloor h^{3/4} \rfloor$. Then, the elements $a_0, 2a_0, \ldots, \ell a_0$ are well-spaced:

$$\|ia_0 - ja_0\| = \|(i-j)a_0\| \geq \frac{p}{2h},$$

for all $i \neq j,\ i,j \in \{1, \ldots, \ell\}$. Consequently, the sets

$$\ell A_1, a_0 + (\ell-1)A_1, \ldots, (\ell-1)a_0 + A_1 \tag{4}$$

are pairwise disjoint. Indeed, if $(ia_0 + (\ell - i)A_1) \cap (ja_0 + (\ell - j)A_1) \neq \emptyset$ for some $i \neq j,\ i,j \in \{0, \ldots, \ell-1\}$, then there are elements $a_1, \ldots, a_{\ell-i}, b_1, \ldots, b_{\ell-j} \in A_1$ such that

$$ia_0 + a_1 + \cdots + a_{\ell-i} = ja_0 + b_1 + \cdots + b_{\ell-j},$$

so that we would have

$$\begin{aligned} \|ja_0 - ia_0\| &= \|a_1 + \cdots + a_{\ell-i} - b_1 - \cdots - b_{\ell-j}\| \\ &\leq \|a_1\| + \cdots + \|a_{\ell-i}\| + \|b_1\| + \cdots + \|b_{\ell-j}\| \\ &\leq \frac{p}{2h}. \end{aligned}$$

Now by (4) and Theorem 4

$$\begin{aligned} |hA| &\geq |\ell A_1| + |a_0 + (\ell-1)A_1| + \cdots + |(\ell-1)a_0 + A_1| \\ &\geq \big(\ell|A_1| - \ell + 1\big) + \big((\ell-1)|A_1| - \ell + 2\big) + \cdots + |A_1| \\ &> \ell^2|A|/4 - \ell^2/2 > |hA|, \end{aligned}$$

a contradiction. Hence A is contained in an arithmetic progression of cardinality $\lfloor p/h \rfloor$ in $\mathbb{Z}_p$ and is F_h-isomorphic to a subset of integers. Applying Theorem 3 we infer that A is contained in an arithmetic progression of size $\max_{1\leq j\leq h-1} \frac{|hA|-P_j(|A|)}{h-j} + 1$, which completes the proof. $\square$

Remark. Using a rectification principle from [1], one can prove that the bound for $L(A)$ similar to that given in Theorem 3 holds also for $A \subseteq \mathbb{Z}_p$, provided we put much more restrictive bounds on the size of A.

References

[1] Y. Bilu, V. F. Lev and I. Z. Ruzsa, *Rectification principles in additive number theory,* Discrete Computational Geometry 19 (1998), 343–353.

[2] G. Freiman, "Foundations of a structural theory of set addition," *Translations of Math. Monographs* **37** (1973), American Math. Soc., Providence.

[3] V. F. Lev, *Structure theorem for multiple addition and the Frobenius problem,* Journal of Number Theory 58 (1996), 79–88.