A NOTE ON THE MINIMAL NUMBER OF REPRESENTATIONS IN $A + A$

Mirosława Radziejewska[1]
Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Poznań, Poland
mjanczak@amu.edu.pl

Received: 2/9/11, Accepted: 2/13/12, Published: 3/1/12

Abstract

Let $f_K(p)$ be the largest n such that for every set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with at most n elements there exists at least one element in $A+A$ with less than K representations. We show a new lower bound for $f_K(p)$:

$$f_K(p) \geq \frac{K \log p}{2\left(\log K + 2\log\log p\right)\left(4 + \log\log K + \log\log\log p\right)} - 1.$$

1. Introduction

Let $f_K(p)$ be the largest n such that for every set $A \subseteq \mathbb{Z}_p$ (where $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$) with at most n elements there exists at least one element in $A+A$ with less than K representations. Straus [8] proved that $f_2(p) \geq \frac{1}{2}\log_2(p-1)+1$ for all primes p. Browkin, Divis and Schinzel [1] showed that $f_2(p) \geq \log_2 p$.

For $x \in \mathbb{Z}_p$ let $\nu(x)$ be the number of representation of x in $\mathbb{Z}_p$ in the form $x = a_1 + a_2$, where $a_1, a_2 \in A$. Straus [8] constructed a set $S \subseteq \mathbb{Z}_p$ such that $\nu(x) \geq 2$ for all $x \in S+S$ and $|S| = \gamma_p \log_2 p$, where $\gamma_p \leq 2$ is uniformly bounded and tends to $2/\log_2 3$ as $p \to \infty$. So for all primes p we have $f_2(p) < \frac{(2+o(1))}{\log 3}\log p$.

For $K \geq 2$, the lower bound $f_K(p) \geq \sqrt{K}\left\lfloor \frac{\log p}{2\log 12} \right\rfloor - 1$, was established in [5], and was improved by Croot and Schoen [3], who showed that

$$f_K(p) \geq \frac{cK\log p}{\left(\log K + \log\log p\right)^2}. \tag{1}$$

On the other hand, Łuczak and Schoen proved in [6] that $f_{2^Q}(p) \leq \left(\gamma_p \log_2 p\right)^Q$, where $\gamma_p = (2+o(1))/\log_2 3$ is the constant from the Straus construction and $Q \in \mathbb{Z}$, $0 < Q < \ln p/(2\ln(\gamma_p \log_2 p))$.

The aim of this note is to give a new lower bound for $f_K(p)$.

[1]The author is supported by Grant N N201 391837 of the Polish Research Committee.

Theorem 1. *For $K \geq 2$ we have*

$$f_K(p) \geq \frac{K \log p}{2(\log K + 2\log\log p)(4 + \log\log K + \log\log\log p)} - 1.$$

This implies that:

$$f_K(p) \quad \geq \quad \begin{cases} \frac{cK \log p}{\log\log p \log\log\log p}, & \text{if } K \leq \log p, \\ \frac{cK \log p}{\log K \log\log K}, & \text{if } \ \log p < K. \end{cases}$$

In particular, if $K = c_1 \log p$ (which is the most important case; see [6] for applications) we have

$$f_K(p) \geq \frac{c_2(\log p)^2}{(\log\log p)(\log\log\log p)},$$

which is a slight improvement over (1).

Throughout the note, by $\log x$ we always mean $\log_2 x$ and p denotes a prime number greater than or equal to 5. For a real number x let $\|x\|$ be the distance from x to the nearest integer number: $\|x\| = \min\{x - \lfloor x \rfloor, \lfloor x \rfloor + 1 - x\}$. Capital letters A, B, etc., will generally refer to group subsets, usually sets of residues modulo p. Define $A + B = \{a + b : \ a \in A, \ b \in B\}$ and $A - B = \{a - b : \ a \in A, \ b \in B\}$.

2. The Proof of Theorem 1

Our approach closely follows the method introduced in [5]. However, instead of applying Ruzsa's covering lemma [7] we use the following result of Chang [2].

Lemma 2. (Chang) *Let A and B be subsets of an abelian group G. If $|A + A| \leq M|A|$ and $|B + A| \leq N|B|$ then there exist sets $S_1, S_2, \ldots, S_k$ with $|S_i| \leq 2M$ for $i = 1, 2, \ldots, k$, $k \leq \log(MN) + 1$, and $A \subseteq B - B + \big(S_1 - S_1\big) + \big(S_2 - S_2\big) + \cdots + \big(S_k - S_k\big)$.*

The next lemma is the well-known Dirichlet approximation theorem.

Lemma 3. *Let $A \subseteq \mathbb{Z}_p$. There exists an integer $0 < d < p$ such that for every $a \in A$ we have $\|da/p\| \leq p^{-1/|A|}$.*

Proof of Theorem 1. Let $A \subseteq \mathbb{Z}_p$ be the smallest set such that for every element $x \in A + A$ we have $\nu(x) \geq K \geq 2$. By definition $|A| = f_K(p) + 1$ and

$$K|A + A| \leq \sum_{t \in A+A} \nu(t) = |A|^2,$$

and hence $|A + A| \leq \frac{|A|^2}{K}$. Clearly we may apply Lemma 2 for A, $B = \{0\}$, $N = |A|$ and $M = \frac{|A|}{K}$. So there exist sets $S_1, S_2, \ldots, S_k$ such that

$$A \subseteq \big(S_1 - S_1\big) + \big(S_2 - S_2\big) + \cdots + \big(S_k - S_k\big),$$

and $|S_i| \le 2\frac{|A|}{K}$ for every $1 \le i \le k$ and some $k \le \log(\frac{|A|^2}{K}) + 1$. By Dirichlet's theorem applied to the set $\bigcup_{i=1}^{k} S_i$ there is an integer $0 < d < p$ such that for every element $x \in \bigcup_{i=1}^{k} S_i$ we have

$$\left\| \frac{dx}{p} \right\| \le p^{-\frac{1}{|\bigcup_{i=1}^{k} S_i|}}. \tag{2}$$

Now we show that

$$p^{-\frac{1}{|\bigcup_{i=1}^{k} S_i|}} \ge \frac{1}{8k}.$$

Indeed, suppose that the above inequality does not hold. We have $d \cdot \bigcup_{i=1}^{k} S_i \subseteq \big(-\frac{p}{8k}, \frac{p}{8k}\big)$ by (2). Since $A \subseteq kS - kS$, then $d \cdot A \subseteq \big(-\frac{p}{4}, \frac{p}{4}\big)$. Let $M = d \cdot m$ be the largest element in $d \cdot A$. Then $M + M$ has exactly one representation in $d \cdot A + d \cdot A$, a contradiction. Therefore, by (2) we have

$$p^{-\frac{K}{2k|A|}} \ge \frac{1}{8k}. \tag{3}$$

We also have $k \le \log(\frac{|A|^2}{K}) + 1$, so (3) implies

$$\frac{|A|}{\sqrt{K}} \log \frac{|A|}{\sqrt{K}} \log \big(16 \log \frac{|A|}{\sqrt{K}}\big) \ge \frac{\sqrt{K} \log p}{4}.$$

It is easy to see that $\log \frac{|A|}{\sqrt{K}} \log \big(16 \log \frac{|A|}{\sqrt{K}}\big) \ge 1$. Hence

$$\begin{aligned} |A| &\ge \frac{K \log p}{4 \log(\sqrt{K} \log p) \log \big(16 \log(\sqrt{K} \log p)\big)} \\ &\ge \frac{K \log p}{2\,(\log K + 2 \log\log p)\,(4 + \log\log K + \log\log\log p)}, \end{aligned}$$

which completes the proof. $\square$

References

[1] J. Browkin, B. Divis, A. Schinzel, *Addition of sequences in general fields,* Monatshefte für Mathematik **82** (1976), 261–268.

[2] M. Chang, *A polynomial bound in Freiman's theorem,* Duke Math. J. **113** (2002) (3), 399–419.

[3] E. Croot, T. Schoen, *On sumsets and spectral gaps,* Acta Arithmetica **136** (2009), 47–55.

[4] D. L. Hilliker, E. G. Straus, *Uniqueness of linear combinations (mod p),* Journal of Number Theory **24** (1986), 1–6.

[5] M. Jańczak, *A note on a problem of Hilliker and Straus,* The Electronic Journal of Combinatorics **14** (2007), 1–8.

[6] T. Łuczak, T. Schoen, *On the problem of Konyagin,* Acta Arithmetica **134** (2008), 101–109.

[7] I. Z. Ruzsa, *An analog of Frieman's theorem in groups,* Asterisque **258** (1999), 323–326.

[8] E. G. Straus, *Differences of residues* (mod p), Journal of Number Theory **8** (1976), 40–42.