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

Miroslawa Radziejewska

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 $f_K(p)$:

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

1. Introduction
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. 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 $f_2(p) < \frac{(2 + o(1))}{\log_2 3} \log p$.

For $K \geq 2$, the lower bound $f_K(p) \geq \sqrt{K} \left\lfloor \log_p^{\frac{1}{\log_2 12}} \right\rfloor - 1$, was established in [5], and was improved by Croot and Schoen [3], who showed that

$$f_K(p) \geq \frac{cK \log p}{(\log K + \log \log p)^2},$$

where $c = (2 + o(1))/\log_2 3$ is the constant from the Straus construction and $Q \in \mathbb{Z}$, $0 < Q < \ln p/(2\ln(\gamma_p \log_2 p))$.

On the other hand, Luczak and Schoen proved in [6] that $f_{2Q}(p) \leq (\gamma_p \log_2 p)^Q$, 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:
\[ f_K(p) \geq \begin{cases} \frac{cK \log p}{\log \log p \log \log \log p}, & \text{if } K \leq \log p, \\ \frac{cK \log p}{\log K \log \log \log K}, & \text{if } \log p < K. \end{cases} \]

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 $A \subseteq B - B + (S_1 - S_1) + (S_2 - S_2) + \cdots + (S_k - S_k)$.

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 $|A + A| \leq |A|^2/K$. Clearly we may apply Lemma 2 for $A, B = \{ 0 \}, N = |A|$ and $M = |A|/K$. So there exist sets $S_1, S_2, \ldots, S_k$ such that
\[ A \subseteq (S_1 - S_1) + (S_2 - S_2) + \cdots + (S_k - S_k), \]
and $|S_i| \leq 2\frac{|A|}{K}$ for every $1 \leq i \leq k$ and some $k \leq \log\left(\frac{|A|^2}{K}\right) + 1$. 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

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

(2)

Now we show that

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

Indeed, suppose that the above inequality does not hold. We have $d \cdot \bigcup_{i=1}^{k} S_i \subseteq \left( -\frac{p}{8k} , \frac{p}{8k} \right)$ by (2). Since $A \subseteq kS - kS$, then $d \cdot A \subseteq \left( -\frac{p}{4} , \frac{p}{4} \right)$. 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

$$p^{-\frac{K}{2\log K}} \geq \frac{1}{8k}.$$  

(3)

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

$$\frac{|A|}{\sqrt{K}} \log\left(\frac{|A|}{\sqrt{K}}\right) \log\left(16 \log\left(\frac{|A|}{\sqrt{K}}\right)\right) \geq \frac{\sqrt{K} \log p}{4}.$$  

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

$$|A| \geq \frac{K \log p}{4 \log(\sqrt{K} \log p) \log(16 \log(\sqrt{K} \log p))} \geq \frac{K \log p}{2 (\log K + 2 \log \log p) (4 + \log \log K + \log \log \log p)},$$

which completes the proof. $\square$

References