Sum and Difference Sets in $\mathbb{Z}/p\mathbb{Z}$

CJ Richardson
Advisor Dr. C. Spencer

July 27, 2011
Sum and Difference Sets in $\mathbb{Z}/p\mathbb{Z}$

Introduction and Terms

Definitions

**Definition**

*The sum set $A + B$ is defined as*

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

**Definition**

*The difference set $A - B$ is defined as*

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

Definition

The sum set $A + B$ is defined as

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

Definition

The difference set $A - B$ is defined as

$$A - B = \{a - b : a \in A, b \in B\}.$$
Sum and Difference Sets in $\mathbb{Z}/p\mathbb{Z}$

Introduction and Terms

Terms

Definitions cont.

**Definition**

$kA$ is defined as $A + .. + A$ with $k \in \mathbb{N}$ number of A’s.
(i.e. $3A = A + A + A$)

**Definition**

For this paper $p$ will be used to denote any prime.
### Definitions cont.

**Definition**

$kA$ is defined as $A + \ldots + A$ with $k \in \mathbb{N}$ number of $A$'s.  
(i.e. $3A = A + A + A$)

**Definition**

For this paper $p$ will be used to denote any prime.
Additive Combinatorics

- Arithmetic combinatorics arose out of the interplay between number theory, combinatorics, ergodic theory and harmonic analysis.

- This summer I focused on the number theory and combinatorics parts of this field.

- It is about combinatorial estimates associated with arithmetic operations (addition, subtraction, multiplication, and division).

- Additive combinatorics refers to the special case when only the operations of addition and subtraction are involved.
Sum and Difference Sets in $\mathbb{Z}/p\mathbb{Z}$

Introduction and Terms

Introduction

The Problem

If $A - A = \mathbb{Z}/p\mathbb{Z}$ then $kA = \mathbb{Z}/p\mathbb{Z}$ for some $k \in \mathbb{Z}$.

- But what do we know about how big $k$ has to be?
- How small can $A$ and still satisfy $A - A = \mathbb{Z}/p\mathbb{Z}$?
- How do $A - A$ and $A + A$ relate in these specific cases?

This summer we worked to find answers to these questions.
The Problem

If $A - A = \mathbb{Z}/p\mathbb{Z}$ then $kA = \mathbb{Z}/p\mathbb{Z}$ for some $k \in \mathbb{Z}$.

- But what do we know about how big $k$ has to be?
- How small can $A$ and still satisfy $A - A = \mathbb{Z}/p\mathbb{Z}$?
- How do $A - A$ and $A + A$ relate in these specific cases?

This summer we worked to find answers to these questions.
If $A - A = \mathbb{Z}/p\mathbb{Z}$ then $kA = \mathbb{Z}/p\mathbb{Z}$ for some $k \in \mathbb{Z}$.

- But what do we know about how big $k$ has to be?
- How small can $A$ and still satisfy $A - A = \mathbb{Z}/p\mathbb{Z}$?
- How do $A - A$ and $A + A$ relate in these specific cases?

This summer we worked to find answers to these questions.
Theorem (Cauchy-Davenport Theorem)

Let $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ be non-empty. Then

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

Proof.

See [1, page 5].
Theorem (Ruzsa’s Lemma)

Let $A, B, C$ be non-empty subsets of an abelian group. Then

$$|C||A - B| \leq |A + C||B + C|.$$ 

Proof.

See [1, page 7].
Proof of Results

Theorem

Suppose \( A \subseteq \mathbb{Z}/p\mathbb{Z} \) with \( A - A = \mathbb{Z}/p\mathbb{Z} \). Then for \( k \geq 2 \)

\[
|kA| > p^{1 - (\frac{1}{2})^k}.
\]

Proof.

We will proceed by induction on \( k \).
Proof of Results

Theorem

Suppose \( A \subseteq \mathbb{Z}/p\mathbb{Z} \) with \( A - A = \mathbb{Z}/p\mathbb{Z} \). Then for \( k \geq 2 \)

\[
|kA| > p^{1 - \left(\frac{1}{2}\right)^k}.
\]

Proof.

We will proceed by induction on \( k \).
Step 1.

- **Applying Ruzsa’s Lemma with** $A = C = B$ **implies**
  \[ |A||A - A| \leq |A + A|^2. \]

- **Since** $|A - A| = p$, **we know that** $|A| > p^{\frac{1}{2}}$. **Therefore,**
  \[ p^{\frac{3}{2}} < |A + A|^2. \]

- **Taking the square root of both sides gives**
  \[ |A + A| > p^{\frac{3}{4}} = p^{1 - (\frac{1}{2})^2} \] **so the theorem holds for** $k = 2$.

---

Step 2.

Assume the result holds for some $j \geq 2$. Thus $|jA| \geq p^{1 - (\frac{1}{2})^j}$. 
Step 1.

- Applying Ruzsa’s Lemma with \( A = C = B \) implies
  \[ |A||A - A| \leq |A + A|^2. \]
- Since \(|A - A| = p\), we know that \(|A| > p^{\frac{1}{2}}\). Therefore,
  \[ p^{\frac{3}{2}} < |A + A|^2. \]
- Taking the square root of both sides gives
  \[ |A + A| > p^{\frac{3}{4}} = p^{1 - \left(\frac{1}{2}\right)^2} \] so the theorem holds for \( k = 2 \).

Step 2.

Assume the result holds for some \( j \geq 2 \). Thus \(|jA| \geq p^{1 - \left(\frac{1}{2}\right)^j}|.\)
Step 3.

- We now prove the result for \( k = j + 1 \).
- Applying Ruzsa’s Lemma gives \( |jA||A - A| \leq |(j + 1)A|^2 \).
- Since \( |jA| > p^{1 - \frac{1}{2}j} = \frac{p}{p^{\frac{1}{2}j}} \) and \( |A - A| = p \), it follows that
  \[
  |(j + 1)A|^2 > \frac{p^2}{p^{\frac{1}{2}j}}.
  \]
- Taking the square root of both sides gives that
  \[
  |(j + a)A| > p^{1 - \frac{1}{2}(j + 1)}.
  \]

Therefore by induction \( |kA| > p^{1 - \frac{1}{2}k} \forall k \geq 2 \).
Theorem

Suppose that $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $A - A = \mathbb{Z}/p\mathbb{Z}$, then for $k \geq \lceil -\log_2 \log_p 2 \rceil$, $2kA = \mathbb{Z}/p\mathbb{Z}$. (1)

This is the best bound we found this summer.
Proof.

- By the Cauchy-Davenport, if $|kA| > \frac{p}{2}$ then $|2kA| = p$.
- Thus by the previous theorem we find that $|2kA| = \mathbb{Z}/p\mathbb{Z}$ when $p^{1-(\frac{1}{2})^k} > \frac{p}{2}$.
- By taking the base-$p$ logarithm of both sides, we get $\log_p p^{1-(\frac{1}{2})^k} > \log_p p - \log_p 2$.
- Simplifying gives $-(\frac{1}{2})^k > -\log_p 2$ implying that $(\frac{1}{2})^k < \log_p 2$.
- Taking the base-2 logarithm of both sides, we find that $k > -\log_2 \log_p 2$.

Hence, for any $k$ that satisfies (1), $2kA = \mathbb{Z}/p\mathbb{Z}$.
Table: Largest $k$ necessary so that $A - A = \mathbb{Z}/p\mathbb{Z}$ implies that $kA = \mathbb{Z}/p\mathbb{Z}$

<table>
<thead>
<tr>
<th>prime</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k$</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>
Table: Number of $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $A - A = \mathbb{Z}/p\mathbb{Z}$

<table>
<thead>
<tr>
<th>prime</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets with</td>
<td>4</td>
<td>16</td>
<td>78</td>
<td>1541</td>
<td>6605</td>
</tr>
<tr>
<td>Total subsets</td>
<td>8</td>
<td>32</td>
<td>128</td>
<td>2048</td>
<td>8192</td>
</tr>
<tr>
<td>prime</td>
<td>17</td>
<td>19</td>
<td>23</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>Sets with</td>
<td>116230</td>
<td>479409</td>
<td>7987579</td>
<td>526724333</td>
<td></td>
</tr>
<tr>
<td>Total subsets</td>
<td>131072</td>
<td>524288</td>
<td>8388608</td>
<td>536870912</td>
<td></td>
</tr>
</tbody>
</table>
Conjecture

For $A \subseteq \mathbb{Z}/p\mathbb{Z}$ if $A - A = \mathbb{Z}/p\mathbb{Z}$ then $4A = \mathbb{Z}/p\mathbb{Z}$.

When $A$ is composed of elements having unique differences, and by default unique sums,

- $|A + A| = \frac{|A|^2 + |A|}{2}$.
- $|A + A| > \frac{|A - A|}{2}$.

Therefore by Cauchy - Davenport, in these specific cases, when $A - A = \mathbb{Z}/p\mathbb{Z}$

- $|(A + A) + (A + A)| \geq |A - A|$.
- $4A = \mathbb{Z}/p\mathbb{Z}$. 
Conjecture

For $A \subseteq \mathbb{Z}/p\mathbb{Z}$ if $A - A = \mathbb{Z}/p\mathbb{Z}$ then $4A = \mathbb{Z}/p\mathbb{Z}$.

When $A$ is composed of elements having unique differences, and by default unique sums,

- $|A + A| = \frac{|A|^2 + |A|}{2}$.
- $|A + A| > \frac{|A - A|}{2}$.

Therefore by Cauchy - Davenport, in these specific cases, when $A - A = \mathbb{Z}/p\mathbb{Z}$

- $|(A + A) + (A + A)| \geq |A - A|$.
- $4A = \mathbb{Z}/p\mathbb{Z}$. 
Conjecture

For $A \subseteq \mathbb{Z}/p\mathbb{Z}$ if $A - A = \mathbb{Z}/p\mathbb{Z}$ then $4A = \mathbb{Z}/p\mathbb{Z}$.

When $A$ is composed of elements having unique differences, and by default unique sums,

- $|A + A| = \frac{|A|^2 + |A|}{2}$.
- $|A + A| > \frac{|A - A|}{2}$.

Therefore by Cauchy - Davenport, in these specific cases, when $A - A = \mathbb{Z}/p\mathbb{Z}$

- $|(A + A) + (A + A)| \geq |A - A|$.
- $4A = \mathbb{Z}/p\mathbb{Z}$. 
Based on the data from obtained from computer programs, the sets that require the largest $k$ such that $kA = \mathbb{Z}/p\mathbb{Z}$ are also relatively small sets (which makes sense), but based on the above situation, a small set $A$ with $A - A = \mathbb{Z}/p\mathbb{Z}$ would potentially expand quickly under summation. Based on this, when $A - A = \mathbb{Z}/p\mathbb{Z}$ I believe there is a balance between having no additive structure, thus $A$ expands quickly under summation, and having some additive structure, requiring that $|A|$ is relatively large. In either case, we may only need $A + A + A + A$ to generate all of $\mathbb{Z}/p\mathbb{Z}$.
Based on the data from obtained from computer programs, the sets that require the largest $k$ such that $kA = \mathbb{Z}/p\mathbb{Z}$ are also relatively small sets (which makes sense), but based on the above situation, a small set $A$ with $A - A = \mathbb{Z}/p\mathbb{Z}$ would potentially expand quickly under summation. Based on this, when $A - A = \mathbb{Z}/p\mathbb{Z}$ I believe there is a balance between having no additive structure, thus $A$ expands quickly under summation, and having some additive structure, requiring that $|A|$ is relatively large. In either case, we may only need $A + A + A + A$ to generate all of $\mathbb{Z}/p\mathbb{Z}$.
Conclusions

There is still some work that can be done to solve this problem:

- If someone can prove that $A - A = \mathbb{Z}/p\mathbb{Z}$ implies $|A + A| \geq \frac{|A - A|}{2}$, then it can be shown that $4A = \mathbb{Z}/p\mathbb{Z}$.

- Based on the data obtained from computer programs, we have tested primes up to 37 for the presence of sets with $A - A = \mathbb{Z}/p\mathbb{Z}$, that requires $5A$ to produce all of $\mathbb{Z}/p\mathbb{Z}$, and we have found none that do, but at this point, our data is limited due to computer constraints.

Hence there is some evidence to support the conjecture above.