Notes on Number Theory and Discrete Mathematics
Vol. 18, 2012, No. 3, 45–47

A note on sumsets and difference sets in $\mathbb{Z}/n\mathbb{Z}$

Christopher J. Richardson[1] **and Craig V. Spencer**[2]

[1] Department of Math, Physics, and Computer Science, Baker University
P.O. Box 65, Baldwin City, KS 66006, United States
e-mail: ChristopherJRichardson@stu.bakeru.edu

[2] Department of Mathematics, Kansas State University
138 Cardwell Hall, Manhattan, KS 66506, United States
e-mail: cvs@math.ksu.edu

Abstract: In this brief note, we investigate the quantity $k(n)$, which is the smallest natural number r such that for all subsets $A \subseteq \mathbb{Z}/n\mathbb{Z}$ satisfying $A - A = \mathbb{Z}/n\mathbb{Z}$, we have $rA = \mathbb{Z}/n\mathbb{Z}$.
Keywords: Sumsets, Difference sets.
AMS Classification: 11B30, 11B13, 05B10.

1 Introduction

For a group G and subsets $A, B \subseteq G$, we define the sumset $A + B = \{x + y : x \in A, y \in B\}$ and the difference set $A - B = \{x - y : x \in A, y \in B\}$, and for $m \in \mathbb{N}$, we write

$$mA = \underbrace{A + A + \cdots + A}_{m \text{ times}}.$$

In the problem session at the Conference in Number Theory [1], Todd Cochrane posed the following question.

Question 1.1. *Does there exist an absolute positive integer k such that if p is prime, $A \subseteq \mathbb{Z}/p\mathbb{Z}$, and $A - A = \mathbb{Z}/p\mathbb{Z}$, then $kA = \mathbb{Z}/p\mathbb{Z}$?*

The question can also be considered with the role of cyclic groups of prime order replaced by cyclic groups, finite Abelian groups, or finite groups. In this paper, we restrict ourselves to studying cyclic groups. For $n \in \mathbb{N}$, define

$$k(n) = \min\{r \in \mathbb{N} : \forall A \subseteq \mathbb{Z}/n\mathbb{Z},\ A - A = \mathbb{Z}/n\mathbb{Z} \Rightarrow rA = \mathbb{Z}/n\mathbb{Z}\}.$$

Question 1.1 is equivalent to showing whether or not the set $\{k(p) : p \text{ is prime}\}$ is finite. In Section 2, we obtain the following upper bound on $k(p)$ when p is prime.

Theorem 1.2. *Suppose that p is an odd prime. Then, $k(p) \leq 2\lceil \log_2 \log_2 p \rceil$.*

Note that this theorem is not strong enough to answer Question 1.1, but it does imply that the function of m defined by $\max\{k(p) : p \leq m, p \text{ is prime}\}$ cannot grow to quickly.

In Section 3, we describe computer searches used to find the values of $k(n)$ in Table 1. Based on the data in Table 1, it is conceivable that $k(n) \leq 4$ for all $n \in \mathbb{N}$; however, due to the computational time required to compute $k(n)$ for large values of n, our data is somewhat limited.

Table 1: Values of $k(n)$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$k(n)$	1	1	2	2	2	3	3	3	3	3	3	3	3	3
n	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$k(n)$	3	3	3	3	3	3	3	3	3	4	3	3	3	4
n	29	30	31	32	33	34	35	36	37	41	43	47	53	
$k(n)$	4	4	4	4	4	4	4	4	4	4	4	4	4	

2 Proof of Theorem 1.2

In this section, we obtain an upper bound for $k(p)$ under the assumption that p is prime. We first recall two theorems required for our proof.

Theorem 2.1 (Cauchy-Davenport Theorem)**.** *Let p be prime and $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ be non-empty. Then, $|A + B| \geq \min\{p, |A| + |B| - 1\}$.*

Proof. See [2, page 5]. □

Theorem 2.2 (Ruzsa's Lemma)**.** *Let A, B, C be non-empty subsets of an additive group. Then, $|C||A - B| \leq |A + C||B + C|$.*

Proof. See [2, page 7]. □

We first use Theorem 2.2 to obtain a lower bound on $|rA|$ when p is prime, $A \subseteq \mathbb{Z}/p\mathbb{Z}$, and $A - A = \mathbb{Z}/p\mathbb{Z}$.

Lemma 2.3. *Suppose that p is prime, $A \subseteq \mathbb{Z}/p\mathbb{Z}$, and $A - A = \mathbb{Z}/p\mathbb{Z}$. Then, for $r \in \mathbb{N}$, $|rA| > p^{1-2^{-r}}$.*

Proof. We proceed by induction on r. Since $p = |A - A| \leq |A|^2$, it follows that $|A| \geq \lceil p^{1/2} \rceil > p^{1-2^{-1}}$. Thus, the statement holds when $r = 1$. Suppose that the statement of the lemma holds when $r = m$ for some $m \in \mathbb{N}$. Then, by applying Theorem 2.2,

$$p^{2-2^{-m}} = p^{1-2^{-m}} p < |mA||A - A| \leqslant |(m + 1)A|^2.$$

Upon taking the square root of both sides, we obtain that $p^{1-2^{-(m+1)}} < |(m + 1)A|$. The lemma now follows. □

We are now in a position to prove Theorem 1.2.

Proof. (of Theorem 1.2) Suppose that p is an odd prime and that $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $A - A = \mathbb{Z}/p\mathbb{Z}$. Let $r = \lceil \log_2 \log_2 p \rceil$. Then, $2^{-r} \leq (\log_2 p)^{-1}$. By Lemma 2.3,

$$|rA| > p^{1-2^{-r}} \geq p^{1-(\log_2 p)^{-1}} = \frac{p}{2}.$$

Hence, by Theorem 2.1,

$$|(2r)A| \geq \min\{p, 2|rA| - 1\} \geq \min\left\{p, 2\left\lceil \frac{p}{2} \right\rceil - 1\right\} = p.$$

This completes the proof of the theorem. □

3 Data

By performing computations on a computer, we have established the values of $k(n)$ in Table 1. For any subset $A \subseteq \mathbb{Z}/n\mathbb{Z}$, we have $|A - A| \leq |A|^2 - |A| + 1$. For composite values of $n \leq 36$ and prime values of $n \leq 23$, an exhaustive search over all subsets $A \subseteq \mathbb{Z}/n\mathbb{Z}$ satisfying $n \leq |A|^2 - |A| + 1$ was performed to calculate $k(n)$.

For a prime p, if $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $A - A = \mathbb{Z}/p\mathbb{Z}$ and $|A| \geq \frac{(p+1)^2}{4p}$, by Theorem 2.2,

$$\frac{(p+1)^2}{4} \leq |A||A - A| \leq |A + A|^2,$$

and by Theorem 2.1,

$$|4A| \geq \min\{p, 2|A + A| - 1\} \geq \min\left\{p, 2\left(\frac{p+1}{2}\right) - 1\right\} = p.$$

Hence, for primes p with $29 \leq p \leq 53$, we established that $k(p) = 4$ by finding one set $B \subseteq \mathbb{Z}/p\mathbb{Z}$ with $B - B = \mathbb{Z}/p\mathbb{Z}$ but $3B \neq \mathbb{Z}/p\mathbb{Z}$ and then doing an exhaustive search over all subsets $A \subseteq \mathbb{Z}/p\mathbb{Z}$ satisfying $p \leq |A|^2 - |A| + 1$ and $|A| < \frac{(p+1)^2}{4p}$.

Acknowledgements

The authors are grateful to Todd Cochrane and Chris Pinner for valuable discussions during the completion of this work.

C. J. Richardson and C. V. Spencer were supported in part by NSF Grant DMS-1004336 (Summer Undergraduate Mathematics Research at K-State), and C. V. Spencer was also supported in part by NSA Young Investigators Grant H98230-10-1-0155.

References

[1] Problem Session of the Conference in Number Theory, Carleton University, June 28, 2011, `http://www.fields.utoronto.ca/programs/scientific/10-11/numtheoryconf/conferenceproblems.pdf`.

[2] Granville, A. An introduction to additive combinatorics, Additive Combinatorics (Providence, RI, USA), *CRM Proceedings and Lecture Notes, American Math. Soc.,* Vol. 43, 2007, 1–27.