Some Properties of $(k, 0)$-sets of Cyclic Groups

W.S. Ng

Institute of Mathematical Sciences
Faculty of Science
University of Malaya
50603 Kuala Lumpur
Malaysia
E-mail: *ng_wei_shean@hotmail.com*

Abstract

Let S be a nonempty subset of the cyclic group $\mathbb{Z}_p$, where p is an odd prime. Denote the n-fold sum of S as $n \cdot \cdot S$. That is, $n \cdot \cdot S = \{s_1 + \cdots + s_n \mid s_1, \ldots, s_n \in S\}$. We say that S is an $(n, 0)$-set if $0 \notin n \cdot \cdot S$. Let k, s be integers with $k \geq 2$ such that $p - 1 = ks$. In this paper we determine the number of $(k, 0)$-sets of $\mathbb{Z}_p$ which are in arithmetic progression and show explicitly the forms taken by those $(k, 0)$-sets which achieve the maximum cardinality.

ARS COMBINATORIA 64(2002), pp. 163-168

1 Introduction

Let A be a finite abelian group written additively and S a nonempty subset of A. For any positive integer n, let $n \cdot \cdot S$ denote the n-fold sum of S, that is,

$$n \cdot \cdot S = \{s_1 + s_2 + \cdots + s_n \mid s_i \in S, i = 1, \ldots, n\}.$$

In particular, $1 \cdot \cdot S = S$. Let k, l be positive integers. In [1], S is said to be a (k,l)-set if $k \cdot \cdot S \cap l \cdot \cdot S = \emptyset$. We say here that S is a $(k,0)$-set if $0 \notin k \cdot \cdot S$. In this paper we consider the case A is the cyclic group $\mathbb{Z}_p$ where p is an odd prime. We write $p - 1 = ks$ for some integers k, s where $k \geq 2$ and determine the number of $(k,0)$-sets of $\mathbb{Z}_p$ which are in arithmetic progression. We also show explicitly the forms taken by those $(k,0)$-sets which achieve the maximum cardinality.

2 Number and maximum cardinality of $(k,0)$-sets

It is easy to see that the largest possible cardinality of a $(1,0)$-set in $\mathbb{Z}_p$ is $p - 1$ and that there is only one such set, that is, $\{1, \ldots, p-1\}$. We thus only need to consider $(k,0)$-sets for $k \geq 2$. We first determine the maximum cardinality of a $(k, 0)$-set as follows:

Theorem 2.1 *Let p be an odd prime and let k, s be integers with $k \geq 2$ such that $p - 1 = ks$. Then the largest possible cardinality of a $(k,0)$-set in $\mathbb{Z}_p$ is s.*

Proof: Let S be a $(k,0)$-set in $\mathbb{Z}_p$. Since $k \geq 2$, so $2 \cdot \cdot S \neq \mathbb{Z}_p$ and it follows by the Cauchy-Davenport Theorem (see [2, Corollary 1.2.3] or [3, Theorem 2.2]) that $|2 \cdot \cdot S| \geq 2|S| - 1$. Since $k \cdot \cdot S \subseteq \{1, \ldots, p-1\} \neq \mathbb{Z}_p$, we have by induction that

$$ks = p - 1 \geq |k \cdot \cdot S| \geq k|S| - (k-1).$$

Thus $|S| \leq s + \frac{k-1}{k}$. Since $0 < \dfrac{k-1}{k} < 1$, it follows that $|S| \leq s$.

We now show that there does exist a $(k,0)$-set of size s in $\mathbb{Z}_p$. Let $S = \{1, \ldots, s\} \subseteq \mathbb{Z}_p$. Since $k(s-1) < p$, the elements $k, k+1, \ldots, k + k(s-1)$ are all distinct (modulo p) and hence,

$$k \cdot \cdot S = \{k, k+1, \ldots, ks\}.$$

Obviously, $k \cdot \cdot S \cap \{0, 1, \ldots, k-1\} = \emptyset$. In particular, $0 \notin k \cdot \cdot S$ which implies that S is a $(k, 0)$-set of size s. □

We now determine the number of $(k, 0)$-sets of $\mathbb{Z}_p$ of size t $(1 \leq t \leq s)$ which are in arithmetic progression.

Theorem 2.2 *Let p be an odd prime and let k, s be integers with $k \geq 2$ such that $p - 1 = ks$. Then the number of $(k, 0)$-sets of size t which are in arithmetic progression in $\mathbb{Z}_p$ is*

(i) $p - 1$ if $t = 1$;

(ii) $\dfrac{(p-1-k(t-1))(p-1)}{2}$ if $1 < t \leq s$.

In particular, the number of $(k, 0)$-sets of maximum cardinality s which are in arithmetic progression in $\mathbb{Z}_p$ is $\dfrac{k(p-1)}{2}$.

Proof: It is clear that $ka \not\equiv 0 \pmod{p}$ for any nonzero element $a \in \mathbb{Z}_p$; hence (i) follows easily. In order to show (ii), let S be a $(k, 0)$-set of size t $(1 < t \leq s)$ which is in arithmetic progression in $\mathbb{Z}_p$. We may write

$$S = \{a, a + d, \ldots, a + (t-1)d\}$$

for some $a \in \mathbb{Z}_p \setminus \{0\}$ and $d \in \{1, \ldots, \frac{p-1}{2}\}$. Now consider the elements

$$ka, ka + d, \ldots, ka + k(t-1)d$$

in $\mathbb{Z}_p$. Since $k(t-1) \leq ks - k = p - 1 - k < p$, so the elements ka, $ka + d, \ldots, ka + k(t-1)d$ are distinct (modulo p) and by induction we have that

$$k \cdot \cdot S = \{ka, ka + d, \ldots, ka + k(t-1)d\}.$$

Since S is a $(k, 0)$-set, it follows that $0 \notin k \cdot \cdot S$ and hence, $0 = ka - id$ for some $i \in \{1, \ldots, k(s-t+1)\}$. Thus for a given d, there are $k(s-t+1)$ possible choices for a. Since there are $\frac{p-1}{2}$ possible choices for d, there are altogether $\dfrac{k(s-t+1)(p-1)}{2} = \dfrac{(p-1-k(t-1))(p-1)}{2}$ possible choices for S. □

In the case of $(2, 0)$-sets with maximum cardinality, we obtain the total number of such sets as follows:

Proposition 2.3 *Let p be an odd prime. Then there are exactly $2^{\frac{p-1}{2}}$ sets of type $(2, 0)$ with maximum cardinality in $\mathbb{Z}_p$.*

Proof: Let S be a $(2,0)$-set of $\mathbb{Z}_p$. Obviously, $0 \notin S$. We also note that $a \in S$ if and only if $-a \equiv p - a \notin S$. By Theorem 2.1, the maximum cardinality of a $(2,0)$-set in $\mathbb{Z}_p$ is $\frac{p-1}{2}$.

To find nonzero elements $a_1, \ldots, a_{\frac{p-1}{2}}$ of $\mathbb{Z}_p$ such that $a_i + a_j \not\equiv 0 \pmod{p}$ for any $i, j = 1, \ldots, \frac{p-1}{2}$, we start by choosing a_1 to be any nonzero element of $\mathbb{Z}_p$. There are clearly $p-1$ possibilities for a_1. Since $a_2 \not\equiv p - a_1 \pmod{p}$, there are $p-3$ possible choices for a_2. Then since $a_3 \not\equiv p-a_1, p-a_2 \pmod{p}$, we are left with $p-5$ possible choices for a_3. Continuing in this way, we are finally left with 2 possible choices for $a_{\frac{p-1}{2}}$. Since ordering of elements is irrelevant in a set, we therefore have that the number of $(2,0)$-sets of cardinality $\frac{p-1}{2}$ in $\mathbb{Z}_p$ is

$$\begin{aligned}
\frac{(p-1)(p-3)\ldots(2)}{\left(\frac{p-1}{2}\right)!} &= \frac{2\left(\frac{p-1}{2}\right)2\left(\frac{p-3}{2}\right)\ldots 2(1)}{\left(\frac{p-1}{2}\right)!} \\
&= \frac{2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}-1\right)\ldots\left(\frac{p-1}{2}-\frac{p-3}{2}\right)}{\left(\frac{p-1}{2}\right)!} \\
&= \frac{2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!}{\left(\frac{p-1}{2}\right)!} \\
&= 2^{\frac{p-1}{2}}.
\end{aligned}$$

□

3 The $(k,0)$-sets with maximum cardinality

Let p be an odd prime and let k, s be integers with $k \geq 2$ such that $p-1 = ks$. In the previous section we have shown that the exact number of $(k,0)$-sets of $\mathbb{Z}_p$ with maximum cardinality s which are in arithmetic progression is $k\left(\frac{p-1}{2}\right)$. In this section we proceed to find out how all these $(k,0)$-sets look like. Recall from the proof of Theorem 2.1 that the set $S = \{1, \ldots, s\} \subseteq \mathbb{Z}_p$ is a $(k,0)$-set.

Lemma 3.1 *Let p be an odd prime and let k, s be integers with $k \geq 2$ such that $p-1 = ks$. Let $S_m = \{(m-1)s+1, (m-1)s+2, \ldots, ms\}$ where $m \in \{1, \ldots, k\}$. Then S_m is a $(k,0)$-set.*

Proof: Consider the elements

$$k(m-1)s + k, k(m-1)s + k + 1, \ldots, kms$$

in $\mathbb{Z}_p$. Since $k(s-1) = p-(k+1) < p$, so these elements are all distinct (modulo p) and we thus have by induction that

$$k \cdot \cdot S_m = \{k(m-1)s+k, k(m-1)s+k+1, \ldots, kms\}.$$

Note that $0 \notin k \cdot \cdot S_m$. For otherwise,

$$k(m-1)s+k+i \equiv 0 \pmod{p}$$

for some $i \in \{0, 1, \ldots, ks-k\}$. That is,

$$(p-1)(m-1)+k+i \equiv 0 \pmod{p}$$

for some $i \in \{0, 1, \ldots, ks-k\}$. But then

$$m \equiv k+1+i \pmod{p}$$

for some $i \in \{0, 1, \ldots, ks-k\}$. Since $m \in \{1, \ldots, k\}$, this is impossible. Therefore $0 \notin k \cdot \cdot S_m$ and it follows that S_m is a $(k, 0)$-set. □

For a subset $S = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_p$ and integer $r \in \mathbb{Z}_p \setminus \{0\}$, we use the notation rS to denote the set $\{ra_1, \ldots, ra_s\}$. It is clear that $k \cdot \cdot(rS) = r(k \cdot \cdot S)$ for any positive integer k.

Lemma 3.2 *Let $S = \{a_1, \ldots, a_s\} \subseteq \mathbb{Z}_p$ where p is a prime number. If S is a $(k, 0)$-set, so is $rS = \{ra_1, \ldots, ra_s\}$ where $r \in \mathbb{Z}_p \setminus \{0\}$.*

Proof: We show that $0 \notin k \cdot \cdot(rS)$. If $0 \in k \cdot \cdot(rS)$, then $ra_{i_1} + \cdots + ra_{i_k} \equiv 0 \pmod{p}$ for some $i_1, \ldots, i_k \in \{1, \ldots, s\}$. That is, $r(a_{i_1} + \cdots + a_{i_k}) \equiv 0 \pmod{p}$. Since $r \not\equiv 0 \pmod{p}$, it follows that $a_{i_1} + \cdots + a_{i_k} \equiv 0 \pmod{p}$. But this implies that $0 \in k \cdot \cdot S$ which contradicts the fact that S is a $(k, 0)$-set. Hence $0 \notin k \cdot \cdot(rS)$. □

Lemma 3.3 *Let p be an odd prime and let k, s be integers such that $p-1 = ks$. Let $S_m = \{(m-1)s+1, (m-1)s+2, \ldots, ms\}$ where $m \in \{1, \ldots, k\}$. Then $iS_m = (p-i)S_{k+1-m}$ for $i \in \{1, \ldots, \frac{p-1}{2}\}$.*

Proof: Note that

$$S_{k+1-m} = \{(k-m)s+1, (k-m)s+2, \ldots, (k+1-m)s-1, (k+1-m)s\}.$$

Then

$$\begin{aligned}
& (p-i)S_{k+1-m} \\
= \ & (-i)S_{k+1-m} \\
= \ & \{(-i)((k-m)s+1), (-i)((k-m)s+2), \ldots, \\
& \quad (-i)((k+1-m)s-1), \quad (-i)(k+1-m)s\} \\
= \ & \{(-i)(-ms), (-i)(-ms+1), \ldots, (-i)((1-m)s-2), \\
& \quad (-i)((1-m)s-1)\} \\
= \ & \{ims, i(ms-1), \ldots, i((m-1)s+2), i((m-1)s+1)\} \\
= \ & \{i((m-1)s+1), i((m-1)s+2), \ldots, i(ms-1), ims\}.
\end{aligned}$$

Since $S_m = \{(m-1)s+1, (m-1)s+2, \ldots, ms\}$, we therefore have that

$$iS_m = \{i((m-1)s+1), i((m-1)s+2), \ldots, ims\} = (p-i)S_{k+1-m}.$$

□

Theorem 3.4 *Let p be an odd prime and let k, s be integers with $k \geq 2$ such that $p-1 = ks$. Then the $k(\frac{p-1}{2})$ subsets of type $(k,0)$ and size s which are in arithmetic progression in $\mathbb{Z}_p$ are of the form $iS_m = \{i((m-1)s+1), i((m-1)s+2), \ldots, ims\}$ where $i \in \{1, \ldots, \frac{p-1}{2}\}$ and $m \in \{1, \ldots, k\}$.*

Proof: By Lemma 3.1, S_m is a $(k,0)$-set for $m \in \{1, \ldots, k\}$ and by Lemma 3.2 so is iS_m for $i \in \mathbb{Z}_p \setminus \{0\}$. By Lemma 3.3, $iS_m = (p-i)S_{k+1-m}$ for $i \in \{1, \ldots, \frac{p-1}{2}\}$ and $m \in \{1, \ldots, k\}$. Therefore, there are altogether $k(\frac{p-1}{2})$ distinct subsets of the form iS_m. By Theorem 2.2, there are exactly $k(\frac{p-1}{2})$ subsets of type $(k,0)$ and size s which are in arithmetic progression in $\mathbb{Z}_p$. Therefore the sets of the form iS_m where $i \in \{1, \ldots, \frac{p-1}{2}\}$ and $m \in \{1, \ldots, k\}$ are all the sets in $\mathbb{Z}_p$ of type $(k,0)$ and size s which are in arithmetic progression. □

References

[1] T. Bier and A. Y. M. Chin, "On (k,l)-sets in cyclic groups of odd prime order", Bull. Austral. Math. Soc., *to appear.*

[2] H. Mann, "Addition Theorems: The Addition Theorems of Group Theory and Number Theory", Interscience Tracts in Pure and Applied Mathematics, No. 18, John Wiley, New York/London/Sydney, 1965.

[3] M. B. Nathanson, "Additive Number Theory: Inverse Problems and the Geometry of Sumsets", GTM 165, Springer, New York/Berlin/Heidelberg, 1996.