BULL. AUSTRAL. MATH. SOC. 20K01, 11P99, 20D60
VOL. 63 (2001) [115–121]

ON (k, l)-SETS IN CYCLIC GROUPS OF ODD PRIME ORDER

T. BIER AND A.Y.M. CHIN

Let A be a finite Abelian group written additively. For two positive integers k, l with $k \neq l$, we say that a subset $S \subset A$ is of *type* (k,l) or is a (k,l)*-set* if the equation $x_1 + x_2 + \cdots + x_k - x_{k+1} - \cdots - x_{k+l} = 0$ has no solution in the set S. In this paper we determine the largest possible cardinality of a (k, l)-set of the cyclic group $\mathbb{Z}_p$ where p is an odd prime. We also determine the number of (k, l)-sets of $\mathbb{Z}_p$ which are in arithmetic progression and have maximum cardinality.

1. INTRODUCTION

Let A be a finite Abelian group written additively. For two positive integers k, l with $k \neq l$, we say that a subset $S \subset A$ is of *type* (k,l) or is a (k,l)*-set* if the equation

$$x_1 + x_2 + \cdots + x_k - x_{k+1} - \cdots - x_{k+l} = 0$$

has no solution in the set S. For convenience, we shall write the k-fold sum

$$S + \cdots + S = \{x_1 + \cdots + x_k \mid x_1, \ldots, x_k \in S\}$$

as kS. The condition that S is a (k, l)-set is then clearly equivalent to the condition

$$kS \cap lS = \emptyset. \tag{1.1}$$

It is obvious from (1.1) that the condition $k > l$ does not give rise to any loss of generality. We also note that a set S of type (k,l) has the property that for $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant l$,

$$iS - jS \neq A.$$

This can be proved by assuming the contrary and using the observation that $A \pm S = A$ to get a contradiction.

We note that (k, l)-sets as defined above are in fact a generalisation of sum-free sets. Recall that a subset $S \subset A$ is called *sum-free* if S does not contain $x + y$ for any $x, y \in S$ (see [3] for example). Thus S is a $(2, 1)$-set if and only if it is sum-free in the usual sense.

Received 10th April, 2000

Let s be a positive integer and a, d be integers. An *arithmetic progression* of *length* s with *difference* d and *initial term* a is a set of the form

$$\{a, a+d, a+2d, \ldots, a+(s-1)d\}.$$

For an odd prime p, we write

$$p-1 = (k+l)(s-1)+b$$

where k, l, b, s are positive integers with $0 < l < k$ and $0 < b \leqslant k+l$. In this paper we show that the largest possible cardinality of a (k, l)-set of the cyclic group $\mathbb{Z}_p$ is given by s. We also show that the number of (k, l)-sets of cardinality s which are in arithmetic progression in $\mathbb{Z}_p$ is $b(p-1)/2$. As for (k, l)-sets of $\mathbb{Z}_p$ which are not in arithmetic progression, we show that there do not exist such sets of cardinality s if $0 < b < k+l-1$ and conjecture that such sets also do not exist if $b = k+l > 3$ or $b = k+l-1$. In what follows we shall always assume that $k > l > 0$.

2. Some preliminaries

We mention in this section two results from additive number theory which have been used in the proofs of the results here. The first is a well-known result of Cauchy and Davenport (see [1, Corollary 1.2.3] or [2, Theorem 2.2]):

Theorem 2.1. (Cauchy-Davenport) *Let p be a prime. For nonempty subsets $S, T \subseteq \mathbb{Z}_p$ with $S+T \neq \mathbb{Z}_p$,*

$$|S+T| \geqslant |S| + |T| - 1. \tag{2.1}$$

Clearly, the theorem of Cauchy-Davenport implies by induction over k that if $kS \neq \mathbb{Z}_p$, then

$$|kS| \geqslant k|S| - k + 1 = k\big(|S|-1\big) + 1. \tag{2.2}$$

We also have a characterisation of the case of equality, due to Vosper (see [1, Theorem 1.3] or [2, Theorem 2.7] or [4]) which may be formulated as follows:

Theorem 2.2. (Vosper's Theorem) *Let p be a prime and let S, T be nonempty subsets of $\mathbb{Z}_p$ with $S+T \neq \mathbb{Z}_p$. Then either $|S+T| \geqslant |S|+|T|$ or $|S+T| = |S|+|T|-1$. The latter occurs if and only if at least one of the following conditions holds:*

(i) $|S+T| = p-1$ *and* $\overline{T} = c - S$ *where* $c \in \mathbb{Z}_p \setminus (S+T)$;

(ii) S *and* T *are in arithmetic progression with the same difference;*

(iii) $|S| = 1$ *or* $|T| = 1$.

https://doi.org/10.1017/S0004972700019171 Published online by Cambridge University Press

3. The maximum cardinality of (k, l)-sets of $\mathbb{Z}_p$

We obtain the maximum cardinality of (k, l)-sets of $\mathbb{Z}_p$ as follows:

Theorem 3.1. *Let p be an odd prime and assume that the integer $p-1$ can be written in the form $p-1=(k+l)(s-1)+b$ where $s \geqslant 1$ and $0 < b \leqslant k+l$. Then the maximum cardinality of (k,l)-sets of $\mathbb{Z}_p$ is given by s.*

Proof: We first show the upper bound. Let S be a (k,l)-set of $\mathbb{Z}_p$ so that

$$X = kS - lS \subseteq \mathbb{Z}_p \setminus \{0\}.$$

Then from the inequalities (2.1) and (2.2) we find that

$$p-1 \geqslant |X| \geqslant (k+l)\big(|S|-1\big)+1.$$

From the assumption in the theorem this may be written as

$$(k+l)(s-1)+b \geqslant (k+l)\big(|S|-1\big)+1,$$

or equivalently as

$$k+l > b-1 \geqslant (k+l)\big(|S|-s\big),$$

which clearly implies that $|S| \leqslant s$.

Now we show that (k,l)-sets with cardinality s do indeed exist. From $p-1 = l(s-1)+b+k(s-1)$ with $0 < b \leqslant (k+l)$, it follows that $0 < l(s-1)+1 < p$, so that in particular $l(s-1)+1 \not\equiv 0 \pmod p$. Also clearly $k-l \not\equiv 0 \pmod p$. We then have that the residue class mod p given by

$$a = \frac{l(s-1)+1}{k-l} \tag{3.1}$$

is not zero, and the associated integer a with $0 < a < p$ has the following properties: There exists an integer m such that

(i) $(k-l)a - l(s-1) = 1 + mp$;
(ii) $(k-l)a + k(s-1) = p - b + mp$.

For the arithmetic progression

$$S = \{a, a+1, \ldots, a+(s-1)\} \tag{3.2}$$

of length s, the set $X = kS - lS$ is also an arithmetic progression with difference 1, with first term given in (i) and with last term given in (ii). Then (i) and (ii) show that for $b > 0$ the set X cannot contain 0. This shows that S defined in (3.2) is a (k,l)-set. □

Remark. We note that in the case $p = 3s+1$, by taking $k=2$, $l=1$ and $b=3$ in Theorem 3.1, we have that the largest possible cardinality of a sum-free set of $\mathbb{Z}_p$ is given by s. This agrees with [5, Theorem 6].

https://doi.org/10.1017/S0004972700019171 Published online by Cambridge University Press

4. (k, l)-SETS IN ARITHMETIC PROGRESSION WITH MAXIMUM CARDINALITY

We first consider (k, l)-sets of $\mathbb{Z}_p$ with cardinality 1. Clearly, for any $a \in \mathbb{Z}_p \setminus \{0\}$, the set $\{a\}$ is a (k, l)-set $(0 < l < k < p)$. Therefore there are altogether $p-1$ (k, l)-sets of cardinality 1 in $\mathbb{Z}_p$. For (k, l)-sets in arithmetic progression with maximum cardinality $\geqslant 2$, we have the following:

THEOREM 4.1. *Assume that for a given odd prime number p, $p-1$ can be written in the form $p-1 = (k+l)(s-1)+b$ where $s \geqslant 2$ and $0 < b \leqslant k+l$. Then the number of (k, l)-sets of maximum cardinality s which are in arithmetic progression in $\mathbb{Z}_p$ is $b(p-1)/2$.*

PROOF: Let S be a (k, l)-set in $\mathbb{Z}_p$ with $|S| = s$. Suppose that S is in arithmetic progression. We may then write

$$S = \{x, x+d, x+2d, \ldots, x+(s-1)d\}$$

for some $x \in \mathbb{Z}_p \setminus \{0\}$ and $d \in \{1, \ldots, (p-1)/2\}$. This gives us

$$kS - lS = \{(k-l)x - l(s-1)d, (k-l)x - l(s-1)d + d, \ldots, (k-l)x + k(s-1)d\}.$$

That is, $kS - lS$ is itself an arithmetic progression with difference d, initial term $a = (k-l)x - l(s-1)d$ and cardinality $|kS - lS| = (k+l)(s-1) + 1 = p - b$. Now since S is a (k, l)-set in $\mathbb{Z}_p$ we have that

$$0 \notin kS - lS \subseteq \{1, 2, \ldots, p-1\}.$$

Hence the element 0 must be one of the elements $a-d$, $a-2d$, $\ldots$, $a-bd$. It follows that for a given d, there are precisely b choices for the initial term a, and thus also precisely b choices for the element x, so that by considering the $(p-1)/2$ possibilities for d, we arrive at the number $b\big((p-1)/2\big)$ of (k,l)-sets S. □

5. (k, l)-SETS NOT IN ARITHMETIC PROGRESSION WITH MAXIMUM CARDINALITY

We first give a result on the nonexistence of (k, l)-sets as follows:

PROPOSITION 5.1. *Assume that for a given odd prime number p, $p-1$ can be written in the form $p-1 = (k+l)(s-1)+b$ where $s > 2$ and $0 < b < k+l-1$. Then there does not exist any (k, l)-set of $\mathbb{Z}_p$ with cardinality s which is not in arithmetic progression.*

PROOF: Suppose to the contrary that there exists a (k, l)-set S of $\mathbb{Z}_p$ with cardinality s which is not in arithmetic progression. Since $0 \notin kS - lS$, we have that $|kS - lS| \leqslant p-1$. Suppose that $|kS - lS| < p-1$. Then since S is not in arithmetic

https://doi.org/10.1017/S0004972700019171 Published online by Cambridge University Press

progression and $|S| \neq 1$, it follows by using Vosper's Theorem repeatedly that

$$\begin{aligned} |kS - lS| &\geqslant |S| + |(k-1)S - lS| \\ &\geqslant 2|S| + |(k-2)S - lS| \\ &\geqslant \quad \cdots \\ &\geqslant k|S| + |S + (l-1)S| \\ &\geqslant (k+1)|S| + |(l-1)S| \\ &\geqslant \quad \cdots \\ &\geqslant (k+l)|S| = (k+l)s. \end{aligned}$$

We thus have that

$$(k+l)(s-1) + b = p - 1 > |kS - lS| \geqslant (k+l)s$$

from which it follows that $b > k + l$. But this contradicts the assumption that $b < k + l - 1$. Hence $|kS - lS| = p - 1$ and by Vosper's Theorem (refer to condition (i) in Theorem 2.2), we then have that

$$|kS| + |lS| = p = (k+l)(s-1) + b + 1 < (k+l)s. \tag{5.1}$$

Since S is not in arithmetic progression, $|S| > 1$ and $|kS|, |lS| < p - 1$, we also have by Vosper's Theorem and induction that $|kS| \geqslant k|S| = ks$ and $|lS| \geqslant l|S| = ls$. But then $|kS| + |lS| \geqslant (k+l)s$ which contradicts (5.1). Therefore there does not exist any (k, l)-set of $\mathbb{Z}_p$ with cardinality s which is not in arithmetic progression. □

We next obtain a characterisation of (k, l)-sets of $\mathbb{Z}_p$ for the remaining cases where $b = k + l - 1$ or $b = k + l$.

PROPOSITION 5.2. *Assume that for a given odd prime number p, $p - 1$ can be written in the form $p - 1 = (k+l)(s-1) + b$ where $s > 2$ and $b = k + l - 1$ or $b = k + l$. If S is a (k, l)-set of $\mathbb{Z}_p$ which is not in arithmetic progression with $|S| = s$, then*

(i) $|kS| = ks$, $|lS| = ls$ *for* $b = k + l - 1$;
(ii) $|kS| = ks + 1$, $|lS| = ls$ *or* $|kS| = ks$, $|lS| = ls + 1$ *for* $b = k + l$.

PROOF: Let S be a (k, l)-set of $\mathbb{Z}_p$ with cardinality s which is not in arithmetic progression. It may be shown using arguments similar to those in the proof of Proposition 5.1 that $|kS - lS| = p - 1$. Hence by Vosper's Theorem,

$$|kS| + |lS| = p = (k+l)(s-1) + b + 1.$$

https://doi.org/10.1017/S0004972700019171 Published online by Cambridge University Press

In particular,

$$|kS| + |lS| = (k+l)s \tag{5.2}$$

if $b = k + l - 1$ and

$$|kS| + |lS| = (k+l)s + 1 \tag{5.3}$$

if $b = k + l$. Since S is not in arithmetic progression, $|S| > 1$ and $|kS|, |lS| < p - 1$, it may also be shown via Vosper's Theorem and induction that $|kS| \geqslant k|S| = ks$ and $|lS| \geqslant l|S| = ls$. Thus by (5.2) we see that $|kS| = ks$, $|lS| = ls$ if $b = k + l - 1$, and by (5.3), either $|kS| = ks + 1$, $|lS| = ls$ or $|kS| = ks$, $|lS| = ls + 1$ if $b = k + l$. □

For the case $b = k + l = 3$ (that is, $k = 2$, $l = 1$), we note in the next proposition that there do exist (k, l)-sets satisfying the first condition in part (ii) of Proposition 5.2. It is necessary to mention here that the result in Proposition 5.3 is known and can be found for example in [3].

PROPOSITION 5.3. *Let p be a prime number which can be written in the form $p = 3s + 1$ where $s > 2$. Then there exist $(2, 1)$-sets of $\mathbb{Z}_p$ which are not in arithmetic progression and which achieve the maximum cardinality s.*

PROOF: Consider the subset

$$S = \{s, s+2, s+3, \ldots, 2s-1, 2s+1\}$$

of $\mathbb{Z}_p$. Note that

$$2S = \{2s, 2s+2, 2s+3, \ldots, 3s, 0, 1, \ldots, s-1, s+1\}$$

and $2S \cap S = \emptyset$. Hence, S is a $(2, 1)$-set with cardinality s. □

The existence of other pairs (k, l) with (k, l)-sets of $\mathbb{Z}_p$ of cardinality s which are not in arithmetic progression remains in doubt. Indeed, we make the following conjecture:

CONJECTURE. *Assume that for a given odd prime number p, $p-1$ can be written in the form $p - 1 = (k + l)(s - 1) + b$ where $s > 2$ and $b = k + l - 1$ or $b = k + l > 3$. Then there are no (k, l)-sets of $\mathbb{Z}_p$ with cardinality s which are not in arithmetic progression.*

REFERENCES

[1] H.B. Mann, *Addition theorems: The addition theorems of group theory and number theory*, Interscience Tracts in Pure and Applied Mathematics **18** (John Wiley, New York, London, Sydney, 1965).

[2] M.B. Nathanson, *Additive number theory: Inverse problems and the geometry of sumsets*, Springer Graduate Texts in Mathematics **165** (Springer-Verlag, Berlin, Heidelberg, New York, 1996).

[3] A.P. Street, 'Sum free sets', in *Springer Lecture Notes in Mathematics* **292** (Springer-Verlag, Berlin, Heidelberg, New York, 1972), pp. 123–272.

[4] A.G. Vosper, 'The critical pairs of subsets of a group of prime order', *J. London Math. Soc.* **31** (1956), 200–205.

[5] H.P. Yap, 'Maximal sum-free sets of group elements', *J. London Math. Soc.* **44** (1969), 131–136.

Institute of Mathematical Sciences
Faculty of Science
University of Malaya
50603 Kuala Lumpur
Malaysia
e-mail: bier@mnt.math.um.edu.my
acym@mnt.math.um.edu.my