BULL. AUSTRAL. MATH. SOC. 11P70, 20D60, 05B10, 11B25
VOL. 65 (2002) [137-144]

MAXIMAL (k,l)-FREE SETS IN $\mathbb{Z}/p\mathbb{Z}$ ARE ARITHMETIC PROGRESSIONS

ALAIN PLAGNE

Given two different positive integers k and l, a (k,l)-free set of some group $(G,+)$ is defined as a set $S \subset G$ such that $kS \cap lS = \emptyset$. This paper is devoted to the complete determination of the structure of (k,l)-free sets of $\mathbb{Z}/p\mathbb{Z}$ (p an odd prime) with maximal cardinality. Except in the case where $k = 2$ and $l = 1$ (the so-called sum-free sets), these maximal sets are shown to be arithmetic progressions. This answers affirmatively a conjecture by Bier and Chin which appeared in a recent issue of this Bulletin.

1. INTRODUCTION

Given two different positive integers k and l and an additively written group G, we say that a subset $\mathcal{S}$ of G is a (k,l)-free set (Bier and Chin call them rather (k,l)-sets in [**1**]) if

$$k\mathcal{S} \cap l\mathcal{S} = \emptyset.$$

As usual, the j-fold sum $j\mathcal{S}$ is defined as

$$j\mathcal{S} = \{s_1 + \cdots + s_j | s_1, \ldots, s_j \in \mathcal{S}\}.$$

Note that $(2,1)$-free sets are known under the name of sum-free sets. They already have been widely studied (see [**10**, Chapter 2] or the last paper by Yap on the subject [**11**]).

In this paper we consider the case of cyclic groups with odd prime order $\mathbb{Z}/p\mathbb{Z}$ (p prime) and investigate their maximal (k,l)-free subsets (in the sense of $|\cdot|$). Clearly, the existence of a (non-void) (k,l)-free set implies that

$$k \neq l \bmod p. \tag{1}$$

In [**1**], Bier and Chin study the maximal cardinality of a (k,l)-free set. They prove the following result.

Received 28th June, 2001
The author was supported by the DGA-Recherche (France).

THEOREM 1.1. *Given p an odd prime, k and l two integers subject to* (1), *then the maximal cardinality of a (k,l)-free set in $\mathbb{Z}/p\mathbb{Z}$ is*

$$\left\lceil \frac{p-1}{k+l} \right\rceil . \tag{2}$$

Furthermore, these authors investigate the structure of maximal (k,l)-free sets in $\mathbb{Z}/p\mathbb{Z}$. In this paper, a (k,l)-free set $\mathcal{S}$ is said to be maximal if it has maximal cardinality, that is if, for any (k,l)-free set $\mathcal{T}$, one has $|\mathcal{S}| \geqslant |\mathcal{T}|$. Bier and Chin prove that if

$$p - 1 - (k+l)\left(\left\lceil \frac{p-1}{k+l} \right\rceil - 1\right) < k + l - 1, \tag{3}$$

then any maximal (k,l)-free set is an arithmetic progression. This is a significant restriction because if $p = 0 \bmod (k+l)$ (respectively $p = 1 \bmod (k+l)$) then the left-hand side of (3) is $k+l-1$ (respectively $k+l$). The case $p = 0 \bmod (k+l)$ is easy to deal with since the primality of p implies clearly $p = k+l$. Then by (2), maximal (k,l)-free sets have then cardinality 1 and are consequently (trivial) arithmetic progressions. The case $p = 1 \bmod (k+l)$ is more serious. In particular, it is known [**10**] that if $p = 1 \bmod 3$, then there are maximal sum-free sets which are not arithmetic progressions, as shown by the following example

$$\{q, q+2, q+3, \ldots, 2q-1, 2q+1\},$$

where $q = (p-1)/3$.

Nonetheless, Bier and Chin conjecture the remarkable fact that, except for sum-free sets (that is, as soon as $\max(k,l) \geqslant 3$), any maximal (k,l)-free set of any cyclic group of prime order is an arithmetic progression.

The purpose of this note is to prove this conjecture. Section 3 of the paper gives a complete proof of the following theorem.

THEOREM 1.2. *Let p be an odd prime and let k, l be positive integers which are different modulo p and which satisfy $\max(k,l) \geqslant 3$. Then any maximal (k,l)-free set in $\mathbb{Z}/p\mathbb{Z}$ is an arithmetic progression.*

As will clearly follow from the proof, for our method Bier and Chin's exceptional cases are run-of-the-mill cases.

2. Tools

Let us recall first that an arithmetic progression is a set of the type

$$\{a + jd \mid j = 0, 1, \ldots, s\}$$

for some integers a, s and d and that an almost-progression is an arithmetic progression from which one element has been removed. In particular an arithmetic progression is an almost-progression.

The useful tools for this study are the addition theorems. We refer to one of the two books [**6, 7**] for a general account on this topic. The first result of this type is almost two hundred years old. It was first proved by Cauchy ([**2**]) and rediscovered more than one century later by Davenport ([**3, 4**]). It is now known as the Cauchy–Davenport Theorem.

THEOREM 2.1. *Let $\mathcal{A}$ and $\mathcal{B}$ be non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ (p prime) then*

$$|\mathcal{A}+\mathcal{B}| \geqslant \min(p, |\mathcal{A}|+|\mathcal{B}|-1).$$

Vosper [**8, 9**] studied the equality case. He obtained the following characterisation.

THEOREM 2.2. *Let $\mathcal{A}$ and $\mathcal{B}$ be non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ (p prime) such that*

$$|\mathcal{A}+\mathcal{B}| = |\mathcal{A}|+|\mathcal{B}|-1$$

then one of the following possibilities occurs.

(i) $\mathcal{A}+\mathcal{B}=\mathbb{Z}/p\mathbb{Z}$,
(ii) *$\mathcal{A}$ or $\mathcal{B}$ has cardinality one,*
(iii) *$\mathcal{A}$ coincides with the complementary set of $c-\mathcal{B}$ for some $c \in \mathbb{Z}/p\mathbb{Z}$,*
(iv) *$\mathcal{A}$ and $\mathcal{B}$ are arithmetic progressions with the same common difference.*

A step beyond Vosper's result was done by Hamidoune and Rødseth ([**5**]) who proved the following crucial result for our work.

THEOREM 2.3. *Suppose that $\mathcal{A}$ and $\mathcal{B}$ are subsets of $\mathbb{Z}/p\mathbb{Z}$ with $|\mathcal{A}|, |\mathcal{B}| \geqslant 3$ and that*

$$7 \leqslant |\mathcal{A}+\mathcal{B}| = |\mathcal{A}|+|\mathcal{B}| \leqslant p-4,$$

then $\mathcal{A}$ and $\mathcal{B}$ are almost-progressions with the same difference.

From these results, we deduce the following key-corollary.

COROLLARY 2.4. *Suppose that $\mathcal{A}$ and $\mathcal{B}$ are subsets of $\mathbb{Z}/p\mathbb{Z}$ with $|\mathcal{A}|, |\mathcal{B}| \geqslant 3$, that $7 \leqslant |\mathcal{A}+\mathcal{B}| \leqslant p-4$ and that $\mathcal{A}$ is not an almost-progression. Then*

$$|\mathcal{A}+\mathcal{B}| \geqslant |\mathcal{A}|+|\mathcal{B}|+1.$$

3. Proof of the structural result

In this section we prove our Theorem 1.2 stated in the Introduction. In the sequel, we suppose without loss of generality that $k > l$ and recall that excluding the case of sum-free sets leads to

$$k+l \geqslant 4. \tag{4}$$

We proceed by contradiction and suppose that we have a maximal (k, l)-free set $\mathcal{S} \subset \mathbb{Z}/p\mathbb{Z}$ which is not an arithmetic progression. Write

$$s = |\mathcal{S}| = \left\lceil \frac{p-1}{k+l} \right\rceil \tag{5}$$

https://doi.org/10.1017/S0004972700020153 Published online by Cambridge University Press

as given by Bier and Chin's Theorem 1.1. Since any set with at most two elements is an arithmetic progression, we may freely assume that $s \geqslant 3$. This with assumption (4) shows that

$$p \geqslant 11.$$

Since $\mathcal{S}$ is a (k,l)-free set, we have $k\mathcal{S} \cap l\mathcal{S} = \emptyset$ thus $0 \notin k\mathcal{S} - l\mathcal{S}$ and

$$|k\mathcal{S} - l\mathcal{S}| \leqslant p - 1. \tag{6}$$

We may apply the Cauchy-Davenport Theorem, that yields

$$|k\mathcal{S} - l\mathcal{S}| \geqslant |(k-1)\mathcal{S} - l\mathcal{S}| + |\mathcal{S}| - 1. \tag{7}$$

3.1. Proving that $\mathcal{S}$ is an almost-progression. We now prove that $\mathcal{S}$ is an almost-progression. Indeed suppose the contrary and assume first $s \geqslant 4$. In this case, the Cauchy-Davenport Theorem shows that

$$|\mathcal{S} - \mathcal{S}| \geqslant \min\big(p, 2|\mathcal{S}| - 1\big) \geqslant 7$$

and thus for any $1 \leqslant i \leqslant k, 1 \leqslant j \leqslant l$,

$$|i\mathcal{S} - j\mathcal{S}| \geqslant |\mathcal{S} - \mathcal{S}| \geqslant 7.$$

Moreover, by (6) and (7), we get for $0 \leqslant i \leqslant k-1, 0 \leqslant j \leqslant l$, that

$$|i\mathcal{S} - j\mathcal{S}| \leqslant \big|(k-1)\mathcal{S} - l\mathcal{S}\big| \leqslant p - |\mathcal{S}| \leqslant p - 4.$$

We are thus in a position to apply Corollary 2.4 to any of the $i\mathcal{S} - l\mathcal{S}$ $(2 \leqslant i \leqslant k-1)$ and to infer

$$|i\mathcal{S} - l\mathcal{S}| \geqslant \big|(i-1)\mathcal{S} - l\mathcal{S}\big| + |\mathcal{S}| + 1, \tag{8}$$

and to any of the $\mathcal{S} - j\mathcal{S}$ $(1 \leqslant j \leqslant l)$ to get

$$|\mathcal{S} - j\mathcal{S}| \geqslant \big|\mathcal{S} - (j-1)\mathcal{S}\big| + |\mathcal{S}| + 1. \tag{9}$$

Summing these inequalities for $2 \leqslant i \leqslant k-1$ and $1 \leqslant j \leqslant l$, we obtain

$$\big|(k-1)\mathcal{S} - l\mathcal{S}\big| \geqslant (k+l-2)\big(|\mathcal{S}| + 1\big) + |\mathcal{S}|.$$

Comparing this with (6) and (7) gives

$$p - 1 \geqslant |k\mathcal{S} - l\mathcal{S}| \geqslant (k+l)|\mathcal{S}| + k + l - 3 > (k+l)|\mathcal{S}|,$$

by (4), contrary to (5).

In the case $s = 3$, we have to be more careful because of the restrictions on the application of the Hamidoune-Rødseth Theorem. Note that we still have

$$|\mathcal{S} - \mathcal{S}| \geqslant 7 = 2|\mathcal{S}| + 1. \tag{10}$$

This follows from the following fact that $|\mathcal{S} - \mathcal{S}|$ is unchanged by a translation or by the multiplication of all the elements of $\mathcal{S}$ by a fixed non-zero element of $\mathbb{Z}/p\mathbb{Z}$, thus we may suppose that $\mathcal{S}$ is of the form $\{0, 1, x\}$ with $2 \leqslant x \leqslant p - 1$. In this case $\mathcal{S} - \mathcal{S} = \{-x, 1 - x, -1, 0, 1, x - 1, x\}$. If two of these elements are equal, we have either $x = p-1$, $x = (p+1)/2$ or $x = 2$, corresponding to arithmetic progressions with respective differences $1, (p+1)/2$ and 1, that is to cases excluded by assumption. This proves (10).

Unfortunately, with (6) and (7) we only get

$$\left|(k-1)\mathcal{S} - l\mathcal{S}\right| \leqslant p - 3$$

which is not sufficient to apply Corollary 2.4 to $\left|(k-1)\mathcal{S} - l\mathcal{S}\right|$. Instead, we can use Vosper's Theorem and obtain

$$\left|(k-1)\mathcal{S} - l\mathcal{S}\right| \geqslant \left|(k-2)\mathcal{S} - l\mathcal{S}\right| + |\mathcal{S}|.$$

Still, equations (8) for $2 \leqslant i \leqslant k-2$ and (9) for $1 \leqslant j \leqslant l$ remain valid. By adding all these inequalities and comparing to (6), what we get is only

$$p - 1 \geqslant |k\mathcal{S} - l\mathcal{S}| \geqslant (k+l)|\mathcal{S}| + k + l - 4.$$

If $k + l > 4$, the contradiction with (5) is immediate. The case $k + l = 4$ (or equivalently $k = 3$ and $l = 1$) is not so direct. Thanks to (5), we already know that $p = 13$ (recall that $s = 3$). Therefore, we are looking for a $(3,1)$-free set of cardinality 3 in $\mathbb{Z}/13\mathbb{Z}$. By multiplying by a non-zero residue modulo p, one can restrict the search to sets $\mathcal{S}$ of the form $\{1, x, y\}$ with $2 \leqslant x < y \leqslant 12$. Now, an exhaustive search by hand (no computer at all is needed!) can be done easily by writing that

$$3\mathcal{S} = \{3, 2+x, 2+y, 1+2x, 1+x+y, 1+2y, 3x, 2x+y, 2y+x, 3y\}$$

and $3\mathcal{S} \cap \mathcal{S} = \emptyset$. We find that, up to multiplication by a non-zero residue modulo p, the only possible subsets $\mathcal{S}$ are $\{1, 2, 8\}$ and $\{1, 4, 11\}$ (this corresponds to 6 solutions for $\mathcal{S}$ in the form required, $\{1, x, y\}$ with $2 \leqslant x < y \leqslant 12$). Since these solutions are arithmetic progressions (with respective differences 7 and 10), we come to a contradiction.

This closes the proof that $\mathcal{S}$ is an almost-progression.

3.2. End of the proof. Since $\mathcal{S}$ is an almost-progression, we can write it, for some a and d in $\mathbb{Z}/p\mathbb{Z}$ ($d \neq 0$), in the form

$$\mathcal{S} = \{a + jd, j \in \mathcal{E}\}$$

with $\mathcal{E} = \{-t, \dots, -1, 1, \dots, u\}$ where $t, u > 0$ (this follows from the fact that $\mathcal{S}$ is not an arithmetic progression) and $t + u = |\mathcal{E}| = s$. Up to changing d into $-d$, we may assume $u \geqslant t$. Also, multiplying $\mathcal{S}$ by a non-zero residue modulo p preserves the (k,l)-freeness (and the fact that $\mathcal{S}$ is an almost-progression). We may thus assume $d = 1$.

Suppose first that $t = 1$. This implies $u \geqslant 2$. Then, by induction it is readily seen that (for any $k, l \geqslant 1$)

$$k\mathcal{S} = \{ka\} + \{-k, -k+2, \dots, ku\}$$

and

$$l\mathcal{S} = \{la\} + \{-l, -l+2, \dots, lu\}.$$

We now show that

$$ka - k + 1, la - l + 1 \notin k\mathcal{S} \cup l\mathcal{S}. \tag{11}$$

Since the two proofs are identical, we only show that $ka - k + 1 \notin k\mathcal{S} \cup l\mathcal{S}$. That $ka-k+1 \notin k\mathcal{S}$ is an immediate consequence of $k\mathcal{S} \neq \mathbb{Z}/p\mathbb{Z}$. Now suppose that $ka-k+1 \in l\mathcal{S}$. If $ka - k + 1 = la - l$, then $ka - k + 3 = la - l + 2 \in k\mathcal{S} \cap l\mathcal{S}$ (remember that $|\mathcal{E}| \geqslant 3$), a contradiction to the (k,l)-freeness. If $ka - k + 1 = la - l + 2$, then $ka - k + 2 = la - l + 3 \in k\mathcal{S} \cap l\mathcal{S}$, another contradiction. Finally if $ka - k + 1 = la - l + w$ with $3 \leqslant w \leqslant l(u+1)$, then $ka - k = la - l + (w-1) \in k\mathcal{S} \cap l\mathcal{S}$, a contradiction again. This proves (11).

Now the two elements on the left-hand side of (11) are different. Indeed if it was not so, we would have $a = 1$ (because $l - k$ is non-zero modulo p) and thus $0 \in \mathcal{S}$, which contradicts the (k,l)-freeness. What we obtain is therefore

$$|k\mathcal{S}| + |l\mathcal{S}| \leqslant p - 2.$$

But $|k\mathcal{S}| = k(u+1)$ and $|l\mathcal{S}| = l(u+1)$ and we get

$$(k+l)(u+1) \leqslant p - 2$$

which implies that

$$|\mathcal{S}| = (u+1) \leqslant \frac{p-2}{k+l},$$

in contradiction with the value of s given by (5).

We now consider the case where $t \geqslant 2$; thus $u \geqslant 2$ also. We examine two different cases.

Suppose first that k and l are greater than or equal to 2. We get

$$k\mathcal{S} = \{ka\} + \{-kt, -kt+1, \dots, ku-1, ku\}$$

and

$$l\mathcal{S} = \{la\} + \{-lt, -lt+1, \dots, lu-1, lu\}.$$

https://doi.org/10.1017/S0004972700020153 Published online by Cambridge University Press

Now the (k,l)-freeness is equivalent to $0 \notin k\mathcal{S} - l\mathcal{S}$ which is equivalent to

$$(l-k)a \notin k\mathcal{E} - l\mathcal{E} = \{-kt - lu, -kt - lu + 1, \dots, ku + lt - 1, ku + lt\} = \mathcal{F}.$$

Since by assumption $(l-k)$ is non-zero modulo p, the existence of such an element a is guaranteed if and only if $|\mathcal{F}| < p$. As

$$|\mathcal{F}| = (ku + lt) + (kt + lu) + 1 = (k+l)(t+u) + 1 = (k+l)|\mathcal{S}| + 1,$$

we obtain

$$(k+l)|\mathcal{S}| + 1 < p,$$

in contradiction with (5).

The final case to consider is $k \geqslant 3$ and $l = 1$. In this case,

$$k\mathcal{S} = \{ka\} + \{-kt, -kt+1, \dots, ku-1, ku\}$$

and

$$l\mathcal{S} = \mathcal{S} = \{a\} + \{-t, \dots, -1, 1, \dots, u\}.$$

We now observe that

$$a \notin k\mathcal{S} \cup \mathcal{S}; \tag{12}$$

Again $a \notin \mathcal{S}$ is immediate while $a \notin k\mathcal{S}$ follows from the fact that, should a belong to $k\mathcal{S}$ then either $a-1$ or $a+1$ would also belong to $k\mathcal{S}$ (the elements of $k\mathcal{S}$ are consecutive); but both $a-1$ and $a+1$ belong to $\mathcal{S}$ and we would get $k\mathcal{S} \cap \mathcal{S} \neq \emptyset$ contrarily to the (k,l)-freeness. Thus (12) holds, which contradicts (5), as above.

The conclusion is that our hypothesis on $\mathcal{S}$ was false or, in other words, that $\mathcal{S}$ is an arithmetic progression. This finishes the proof of our Theorem.

References

[1] T. Bier and A.Y.M. Chin, 'On (k,l)-sets in cyclic groups of odd prime order', *Bull. Austral. Math. Soc.* **63** (2001), 115–121.

[2] A.L. Cauchy, 'Recherches sur les nombres', *J. École Polytech.* **9** (1813), 99–123.

[3] H. Davenport, 'On the addition of residue classes', *J. London Math. Soc.* **10** (1935), 30–32.

[4] H. Davenport, 'A historical note', *J. London Math. Soc.* **22** (1947), 100–101.

[5] Y.O. Hamidoune and Ø.J. Rødseth, 'An inverse theorem mod p', *Acta Arith.* **92** (2000), 251–262.

[6] 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).

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

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

[9] A.G. Vosper, 'Addendum to: "The critical pairs of subsets of a group of prime order"', *J. London Math. Soc.* **31** (1956), 280–282.

[10] W.D. Wallis, A.P. Street and J.S. Wallis, *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, Lecture Notes in Mathematics **292** (Springer-Verlag, Berlin, Heidelberg, New York, 1972).

[11] H.P. Yap, 'Maximal sum-free sets in finite abelian groups. V', *Bull. Austral. Math. Soc.* **13** (1975), 337–342.

LIX
École polytechnique
91128 Palaiseau Cedex
France
e-mail: plagne@lix.polytechnique.fr