ON A GENERALIZATION OF A THEOREM BY VOSPER

Oriol Serra
UPC, Jordi Girona, 1, 08034 Barcelona, Spain
oserra@mat.upc.es

Gilles Zémor
ENST, 46 rue Barrault, 75 634 Paris 13, France
zemor@infres.enst.fr

Received: 4/7/00, Accepted: 8/4/00, Published: 8/4/00

Abstract

Let S, T be subsets of $\mathbb{Z}/p\mathbb{Z}$ with $\min\{|S|, |T|\} > 1$. The Cauchy–Davenport theorem states that $|S+T| \geq \min\{p, |S|+|T|-1\}$. A theorem by Vosper characterizes the critical pair in the above inequality. We prove the following generalization of Vosper's theorem. If $|S+T| \leq \min\{p-2, |S|+|T|+m\}$, $2 \leq |S|, |T|$, and $|S| \leq p - \binom{m+4}{2}$, then S is a union of at most $m+2$ arithmetic progressions with the same difference. The term $\binom{m+4}{2}$ is best possible, i.e. cannot be replaced by a smaller number.

1. Introduction

One of the subjects of additive number theory is the study of *inverse problems*, i.e. the study of the structure of subsets S and T of a group such that the cardinality $|S+T|$ is "small". The oldest result in this vein is the Cauchy-Davenport theorem which states that $|S+T| \geq \min\{p, |S|+|T|-1\}$ for any subsets S, T of a group of prime order p. Vosper's theorem [6] characterizes the sets for which equality holds. It states :

Theorem 1 (Vosper) *Let S and T be subsets of a group of prime order p such that $|S| \geq 2$, $|T| \geq 2$, and $|S+T| < p-1$. Then either $|S+T| \geq |S|+|T|$, or S and T are in arithmetic progression with the same difference.*

Freiman [1] gave the following improvement of Vosper's Theorem in the case when $S = T$.

Theorem 2 (Freiman) *Let S be a subset of a group of prime order p such that $|S| < p/35$. Suppose that $|S+S| \leq 2|S|+m$ with $m \leq \frac{2}{5}|S|-3$. Then S is contained in an arithmetic progression of length at most $|S|+m+1$.*

As far as we know, the first improvement of Vosper's result for different sets S and T is the recent result of Hamidoune and Rødseth [5] who proved :

Theorem 3 (Hamidoune-Rødseth) *Let S and T be subsets of a group of prime order p, such that $|S| \geq 3$, $|T| \geq 3$, $7 \leq |S+T| \leq p-4$. Then either $|S+T| \geq |S|+|T|+1$, or S and T are contained in arithmetic progressions with the same difference and $|S|+1$ and $|T|+1$ elements respectively.*

In another direction, the Cauchy-Davenport theorem was generalized to arbitrary Abelian groups by Mann [2, p. 2] :

Theorem 4 (Mann) *Let S be a subset of an arbitrary Abelian group G. Then one of the following holds:*

- **(i)** *for every subset T such that $S+T \neq G$ we have $|S+T| \geq |S|+|T|-1$.*
- **(ii)** *there exists a proper subgroup H of G such that $|S+H| < |S|+|H|-1$.*

The following theorem of Hamidoune [4] is both a generalization of Mann's theorem and of Vosper's theorem.

Theorem 5 (Hamidoune) *Let G be a (not necessarily Abelian) group generated by a finite subset S containing 0. Suppose that every nonzero element of G has order $\geq |S|$. Then one of the following holds:*

- **(i)** *for every subset T such that $2 \leq |T| < \infty$, we have $|S+T| \geq \min(|G|-1, |S|+|T|)$.*
- **(ii)** *S is an arithmetic progression.*

Notice the similarity between Mann's and Hamidoune's theorems 4 and 5. Together they state, broadly speaking, that subsets S of a group for which $S+T$ is "small" for some T tend either to cluster around subgroups or to be an arithmetic progression.

A very interesting feature of Hamidoune's proof of his result is that it unites Theorems 1 and 4 under a short, elegant, and insightful explanation. This involves defining k–isoperimetric numbers and k-atoms associated to S. It turns out that the 1–atoms lead naturally to the subgroup H in Theorem 4 and that the 2–atoms lead to the difference of the arithmetic progression in Theorem 5.

In this paper, we study the 2–atoms of an arbitrary subset S of a group of prime order and give a sufficient condition on $|S|$ for them to be of cardinality two. We shall see that this condition is necessary in very many situations. This leads to a further generalization of Vosper's theorem in the prime order case. Our main result is :

Theorem 6 *Let m be a non-negative integer and let S be a subset of a group of prime order p such that $2 \le |S| < p - \binom{m+4}{2}$. Then either*

$$|S+T| > |S| + |T| + m,$$

for any subset T such that $2 \le |T|$ and $|S+T| \le p-2$, or S is the union of at most $m+2$ arithmetic progressions with the same difference.

Our proof leads to the condition $|S| < p - \binom{m+4}{2}$ in a natural way, and we shall see that this bound is best possible. More precisely, there exist subsets S of $\mathbb{Z}/p\mathbb{Z}$ with cardinality $p - \binom{m+4}{2}$ that are not the union of at most $m+2$ arithmetic progressions and for which $|S+T| \le |S| + |T| + m \le p-2$ for some subset $|T| \ge 2$. Note that this situation is unlike that of $\mathbb{Z}$, but these sets S have to be "large", i.e. $|S| \ge p - \binom{m+4}{2}$.

2. Atoms

Let S be a fixed subset of $\mathbb{Z}/p\mathbb{Z}$ with $0 \in S$. For a subset $X \subset G$ we write

$$N_S(X) = (X+S) \setminus X.$$

We omit the subscript S when the reference to it is clear from the context. If $0 \in X$, we write $X^* = X \setminus \{0\}$.

Following the terminology of Hamidoune [4], we say that S is k–*separable* if there is $X \subset \mathbb{Z}/p\mathbb{Z}$ such that $|X| \ge k$ and $|X+S| \le p-k$. If S is k–separable, the k–*isoperimetric connectivity* of S is

$$\kappa_k(S) = \min\{|N(X)|,\ X \subset \mathbb{Z}/p\mathbb{Z}, k \le |X| \text{ and } |X+S| \le p-k\},$$

and the k–*isoperimetric number* of S is

$$d_k(S) = \min\{|N(X)|,\ X \subset \mathbb{Z}/p\mathbb{Z}, |X| = k\}.$$

We say that a subset $F \subset G$ is a k–*fragment* of S if $|N(F)| = \kappa_k(S)$, $|F| \ge k$ and $|F+S| \le p-k$. A k–fragment of minimum cardinality is said to be a k–*atom* of S. We denote by $\alpha_k(S)$ the cardinality of a k–atom of S. Note that $\alpha_k(S) > k$ if and only if $\kappa_k(S) < d_k(S)$. Note also that, when $|S| = 2$ and S is k-separable, then $\alpha_k(S) = k$ and $\kappa_k(S) = 1$. To avoid trivial cases we always assume that $|S| > 2$.

The following basic property of k–atoms is proved in [4].

Theorem 7 *Let A be a k–atom and let F be a k–fragment of a subset $S \subset \mathbb{Z}/p\mathbb{Z}$ with $0 \in S$. Then, either $A \subset F$ or $|A \cap F| \le k-1$.*

This theorem has a number of consequences. We use it here to derive some intermediate results that we shall need. For the rest of this section it is always assumed that S is a 2–separable subset of $\mathbb{Z}/p\mathbb{Z}$, $0 \in S$, and $|S| \ge 3$.

Proposition 8 *Let A be a 2–atom of S. Then, $|A|(|A|-1) \le 2\kappa_2(S)$.*

Proof. We may assume $|A| > 2$. Let $S = \{0 = s_0, s_1, \ldots, s_r\}$, $r \ge 2$. We have

$$\kappa_2(S) = |A+S| - |A| = \left|\bigcup_{i=1}^{r}[(A+s_i) \setminus \cup_{0\le j<i}(A+s_j)]\right|. \tag{1}$$

If A is a 2–atom then so is $A+z$ for any z. Therefore equation (1) and Theorem 7 imply

$$\kappa_2(S) \ge (|A|-1) + (|A|-2) + \max\{|A|-3, 0\} + \ldots + \max\{|A|-r, 0\}.$$

If $|A| > |S|$ then $|A+S| - |A| \ge (|A|-1) + (|A|-2) \ge 2|A| - 3 \ge 2|S| - 1 \ge d_2(S)$, which implies $\alpha_2(S) = 2$. Hence $|A| \le |S|$. Therefore,

$$\kappa_2(S) \ge (|A|-1) + \ldots + 2 + 1 = |A|(|A|-1)/2,$$

as claimed. ∎

Recall that $X \subset G$ is a Sidon set if $|2X| = \binom{|X|+1}{2}$, that is, there are no two unordered pairs of (possibly equal) elements in X with the same sum. The following is an easy consequence of Theorem 7.

Proposition 9 *Let A be a 2–atom of S. If $|A| > 2$ then A is a Sidon set.*

Proof. Suppose that $x + y = x' + y'$ for x, y, x', y' in A. Then $\{x, y'\} \in (A + x - x') \cap A$. Since $A + z$ is a 2–atom for each $z \in \mathbb{Z}/p\mathbb{Z}$, Theorem 7 implies either $x = y'$ or $x = x'$. Hence, all twofold sums of elements of A are different and A is a Sidon set. ∎

Proposition 10 *Suppose S is a Sidon set in $\mathbb{Z}/p\mathbb{Z}$. Then, $\alpha_2(S) = 2$.*

Proof.

For each $x \in \mathbb{Z}/p\mathbb{Z}$, $x \ne 0$, we have $|S \cap (S+x)| \le 1$. For $k \le |S|$ let $X = \{x_1, \ldots, x_k\} \subset \mathbb{Z}/p\mathbb{Z}$. Then,

$$\begin{aligned} |N(X)| &= |S+X| - |X| = \left|\bigcup_{i=1}^{k}[(S+x_i) \setminus \bigcup_{j<i}(S+x_j)]\right| - |X| \\ &\ge [|S| + (|S|-1) + (|S|-2) + \cdots + (|S| - |X| + 1)] - |X| = \frac{1}{2}|X|(2|S| - |X| - 1). \end{aligned}$$

In particular,

$$d_k(S) \ge \frac{1}{2}k(2|S| - k - 1). \tag{2}$$

Let A be a 2–atom of S and suppose that $|A| > 2$, so that $|N(A)| < d_2(S)$. We have, for any $s \in S^*$, $|S + \{0, s\}| = 2|S| - 1$ so that $|N(\{0, s\})| = 2|S| - 3$: we conclude therefore that $|N(A)| < 2|S| - 3$. But according to the lower bound (2), which is a quadratic function of k with negative leading term and zeros at $k = 0$ and $k = 2|S| - 1$, this implies $|A| > 2|S| - 3$. By Proposition 8 we then have $(2|S| - 3)(2|S| - 4) < 2(2|S| - 4)$, which implies $|S| < 3$ against our assumption. Hence, $\alpha_2(S) = 2$. ∎

Finally we have :

Proposition 11 *Let A be a 2–atom of S. Then, $\alpha_2(A) = 2$. Moreover, $|A| \leq m + 3$, where $m = \kappa_2(S) - |S|$.*

Proof. If $\alpha_2(S) = |A| = 2$ there is nothing to prove. Suppose that $|A| > 2$. We may assume that $0 \in A$. By Proposition 9, A is a Sidon set. By Proposition 10 we have $\alpha_2(A) = 2$.

On the other hand, we have $|S + A| - |A| = |S| + m$, which implies

$$|A| + m = |S + A| - |S| \geq \kappa_2(A) = d_2(A) = 2|A| - 3.$$

Hence $|A| \leq m + 3$. ∎

3. Surjective pairs of subsets

To prove that a set S is the union of sufficiently few arithmetic progressions, say of difference a, our basic strategy is to show that $\{0, a\}$ is a 2-atom of S. This is why, in this section, we study 2–atoms A of sets S such that $|A| > 2$. We shall prove that these 2–atoms have very special structure, namely that they define, together with S, *surjective pairs*. Before defining this concept we need some notation.

Let Y be a fixed subset of $\mathbb{Z}/p\mathbb{Z}$. For each subset $X \subset \mathbb{Z}/p\mathbb{Z}$ and each integer $i \geq 2$ we denote

$$N_i(X) = N_Y(X + (i-1)Y),$$

where $iY = \underbrace{Y + \ldots + Y}_{i}$. We write $N_0(X) = X$ and $N_1(X) = N_Y(X)$. Note that

$$N_{i+1}(X) = (N_i(X) + Y) \setminus \bigcup_{0 \leq j \leq i} N_i(X).$$

For a subset U of Y and $i \geq 1$, we denote by $N_i^U(X)$ the set of elements $z \in N_i(X)$ such that $z - U \subset N_{i-1}(X)$ and U is a maximal subset of Y with this property. We also write

$$N_i^{\leq U}(X) = \bigcup_{V \subset U} N_i^V(X).$$

Lemma 12 *For each $U \subset Y$ and $i \geq 1$, if $N_{i+1}^U(X) \neq \emptyset$ then*

$$N_{i+1}^U(X) - U \subset N_i^{\leq U}(X).$$

Proof. Let $z \in N_{i+1}^U(x)$, $u \in U$ and $z' = z - u \in N_i(X)$. Then $z' \in N_i^V(X)$ for some subset V of Y. But, for any $v \in V$, we have $z - v = z' - v + u \in N_j(X)$ for some $j < i + 1$. Since $z \in N_{i+1}(X)$ we must have $j = i$: this implies $V \subset U$. In particular, if $N_{i+1}^U(X) \neq \emptyset$, then $N_{i+1}^U(X) - U \subset \cup_{V \subset U} N_i^V(X) = N_i^{\leq U}(X)$. ∎

Definition A pair (X, Y) of subsets of $\mathbb{Z}/p\mathbb{Z}$ is said to be *h-surjective* if $X, Y \neq \mathbb{Z}/p\mathbb{Z}$ and

$$|(z - Y) \cap X| \geq h \text{ for each } z \in N_Y(X). \tag{3}$$

The following two lemmas are the key steps in our proof of Theorem 6.

Lemma 13 *Let S be a 2-separable subset of $\mathbb{Z}/p\mathbb{Z}$ and let A be a 2–atom of S such that $|A^*| \geq 2$. Then*

- **(i)** *(S, A) is a 2-surjective pair, and*
- **(ii)** *$(S + A, A)$ is a $|A^*|$-surjective pair.*

Proof. We may assume that $0 \in A$. Let $z \in N_A(S)$ and suppose that there is only a single element $z' \in A$ such that $z - z' \in S$. Let $A' = A \setminus \{z'\}$. Then $|A + S| = |(A' + S) \cup \{z\}| = |A' + S| + 1$. Therefore, $|N_S(A)| = |N_S(A')|$ and $|A'| \geq 2$, contradicting the minimality of A. Hence, (S, A) is 2-surjective.

Let U be a subset of A^* with at most $|A| - 2$ elements.

By Lemma 12 and the Cauchy-Davenport theorem, if $N_i^U(S) \neq \emptyset$ for some $i \geq 2$, then we have

$$|N_{i-1}^{\leq U}(S)| \geq |N_i^U(S) - U| \geq |N_i^U(S)| + |U| - 1. \tag{4}$$

If $|U| \leq |N_1^{\leq U}(S)|$, then

$$|S + (A \setminus U)| - |A \setminus U| \geq |S + A| - |N_1^{\leq U}(S)| + |U| - |A| \leq |S + A| - |A|,$$

thus contradicting the hypothesis that A is a 2-atom. Hence,

$$|N_1^{\leq U}(S)| \leq |U| - 1, \;\; U \subset A^*, |U| \leq |A| - 2.$$

Therefore, if $N_2^U(S) \neq \emptyset$, then (4) implies

$$|N_2^U(S)| \leq |N_1^{\leq U}(S)| - (|U| - 1) \leq 0,$$

a contradiction. Hence $N_2^U(S) = \emptyset$ for each proper subset of A^* and therefore $(S + A, A)$ is an $|A^*|$-surjective pair. ∎

Lemma 14 *Let (X, Y) be an h-surjective pair in $\mathbb{Z}/p\mathbb{Z}$ and $i \geq 1$. If $X + iY \neq \mathbb{Z}/p\mathbb{Z}$ then $(X + iY, Y)$ is also an h-surjective pair. In particular, if $|N_i^{\leq U}(X)| < h$ for some $U \subset Y$ and $i \geq 1$ then $N_{i+1}^U(X) = \emptyset$.*

Proof. Assume that $(X+(i-1)Y, Y)$ is h-surjective for some $i \geq 1$. We have $N_1(X+(i-1)Y) = N_i(X)$. For each subset U of Y with strictly less than h elements, we have $N_i^{\leq U}(X) = \emptyset$. If $N_{i+1}^U(X) \neq \emptyset$, $i \geq 1$ then Lemma 12 implies $N_{i+1}^U(X) - U \subset N_i^{\leq U}(X) = \emptyset$, a contradiction. Therefore, $(X + iY, Y)$ is also h-surjective. The first part of the result follows by induction.

Suppose now that $|N_i^{\leq U}(X)| < h$ for some $U \subset Y$. Then, if $N_{i+1}^U(X) \neq \emptyset$, Lemma 12 implies $h > |N_i^{\leq U}(X)| \geq |N_{i+1}^U(X) - U| \geq |U|$, this contradicts the h-surjectivity of $(X + iY, Y)$. ∎

Theorem 15 *Let $S \subset \mathbb{Z}/p\mathbb{Z}$ be a 2-separable subset. If $\alpha_2(S) > 2$ then*

$$|S| \geq p - \binom{m+4}{2},$$

where $m = \kappa_2(S) - |S|$.

Proof. We may assume $|S| > 2$. Let A be a 2–atom of S containing 0 and suppose that $|A| > 2$.

We use the above notation with $Y = S$, namely, $N_i(S) = N_A(S + (i-1)A)$. By definition of $\kappa_2(S)$ and m we have $|S + A| = |A| + |S| + m$, so that $|N_1(S)| = |A| + m$.

1. Suppose first $|A| = 3$, so that $N_1(S) = |A| + 3$.

   By Lemma 13 and Lemma 14, if $S + iA \neq \mathbb{Z}/p\mathbb{Z}$, $i \geq 1$, then $(S + iA, A)$ is a 2-surjective pair. Therefore $N_i(S) = N_i^{A^*}(S)$ for $i \geq 2$. If $N_i(S) \neq \emptyset$, then Lemma 12 implies $N_i(S) - A^* \subset N_{i-1}(S)$. By the Cauchy-Davenport theorem this implies, for all $i \geq 2$ such that $N_i(S) \neq \emptyset$,
   $$|N_i(S)| \leq |N_{i-1}(S)| - 1.$$
   Therefore, $|N_i(S)| \leq (m+3) - (i-1) = m + 4 - i$ and $N_i(S) = \emptyset$ for $i \geq m + 4$. Hence, $\mathbb{Z}/p\mathbb{Z} = \cup_{i=0}^{m+3} N_i(X)$ which implies
   $$|S| \geq p - \sum_{i=1}^{m+3} |N_i(S)| \geq p - \frac{(m+3)(m+4)}{2},$$
   as claimed.

2. Suppose now that $h + 1 = |A| > 3$. Let us write $\mathbb{Z}/p\mathbb{Z} = \cup_{i=0}^{k} N_i(X)$, so that we have
   $$|S| = p - \sum_{i=1}^{k} |N_i(S)|.$$

By Lemma 13 and Lemma 14, if $S + iA \neq \mathbb{Z}/p\mathbb{Z}$, $i \geq 1$, then $(S + iA, A)$ is an h-surjective pair. Therefore $N_i(S) = N_i^{A^*}(S)$ for $i \geq 2$. If $N_i(S) \neq \emptyset$, then Lemma 12 implies $N_i(S) - A^* \subset N_{i-1}(S)$. Since A^* is a Sidon set with more than 2 elements, it is not an arithmetic progression. By Vosper's theorem this implies, for all $i \geq 2$ such that $|N_i(S)| > 1$,

$$|N_i(S)| \leq |N_{i-1}(S)| - h.$$

Therefore, $|N_2(S)| \leq m + |A| - h = m + 1$, and if $k \geq 3$,

(i) $|N_i(S)| \leq (m+1) - (i-2)h$ for all i such that $3 \leq i \leq k-1$, and

(ii) either $|N_k(S)| = 1$ and $|N_{k-1}(S)| = h$ or $|N_k(S)| \leq (m+1) - (k-2)h$.

In every case we get $k \leq 2 + (m+1)/h$.

By Proposition 11, $|N_1(S)| = m + |A| \leq 2m + 3$; therefore, if $k = 2$ we get

$$|N_1(S)| + |N_2(S)| \leq 3m + 4$$

and it is routinely checked that this is always smaller than $\binom{m+4}{2}$.

If $k \geq 3$ we get

$$\sum_{i=1}^{k} |N_i(S)| \leq (2m+3) + (m+1)(k-1) - h\frac{(k-2)(k-1)}{2} + 1$$

which gives, since we have supposed $h \geq 2$,

$$\sum_{i=1}^{k} |N_i(S)| \leq (2m+4) + (k-1)[(m+1) - (k-2)] \leq (2m+4) + (k-1)m,$$

and, since $k - 1 \leq 1 + (m+1)/h$, we get

$$\sum_{i=1}^{k} |N_i(S)| \leq (3m+4) + m(m+1)/2$$

which is less than $\binom{m+4}{2}$.

This concludes the proof. ∎

4. A Proof of Theorem 6: Discussion

Suppose S is a subset of $\mathbb{Z}/p\mathbb{Z}$ satisfying the conditions of Theorem 6 and suppose there exists $T \subset \mathbb{Z}/p\mathbb{Z}$ such that $2 \leq |T|$, $|S+T| \leq p-2$, and $|S+T| \leq |S| + |T| + m$. Then, without loss of generality we may suppose $0 \in S$, and S is a 2-separable set for which $\kappa_2(S) \leq |S| + m$. Let A be a 2-atom of S containing 0. By Theorem 15 we have $|A| = 2$ and therefore

$$|S + A| \leq |S| + |A| + m = |S| + m + 2.$$

Let $A = \{0, a\}$. Let $S = S_1 \cup \ldots \cup S_h$ be a partition of S into arithmetic progressions of difference a such that $(S_i + a) \cap S_j = \emptyset$ for each pair of different subscripts i, j. Then,

$$|S + A| = \sum_{i=1}^{h} |S_i + \{0, a\}| = |S| + h,$$

which implies $h \leq m + 2$ and Theorem 6 is proved.

We now show that the term $\binom{m+4}{2}$ in Theorem 6 cannot be reduced. First consider the following example. Let p be a prime number of the form $p = 3b + 1$ for some positive integer b and let $S = [0, b-1] \cup [b+1, 2b-2] \cup [2b+1, 3b-3]$ and $A = \{0, 1, b\}$. Then $|S+A| = |S| + |A|$, i.e. $|N_S(A)| = |S|$. Note that $|S| = p - 6 = \binom{4+0}{2}$. Note also that $|N_S(\{0, x\})| \geq |S| + 1$ for any $x \neq 0$, since otherwise Vosper's theorem would imply that S is an arithmetic progression of difference x, which can be easily checked not to be the case. This shows that 2-atoms of size more than 2 do exist. Furthermore, by Proposition 11, the size of a 2-atom is at most 3 in this example, so that A is actually a 2-atom of S.

This example can be generalized to sets S with $\kappa_2(S) = |S| + m$ for $m > 0$ and for which $\alpha_2(S) = 3$. They are built with a similar pattern. Let b be a positive integer such that $p = (m+3)b + 1$ is a prime number. Let

$$S = [0, b-1] \cup [b+1, 2b-2] \cup [2b+1, 3b-3] \cup \ldots \cup [(m+2)b+1, (m+3)b - (m+3)].$$

Again set $A = \{0, 1, b\}$. We have $|S+A| = |S|+|A|+m$. Note that $|S| = p - \binom{m+4}{2}$, i.e. exactly the bound of Theorem 6. It is not quite clear to us how to formally prove that $d_2(S) > |S|+m$, or, equivalently, that S is not the union of k arithmetic progressions for $k \leq m + 2$, but this can be checked by exhaustive search for many values of m as long as p is not too large. In these cases we actually have $\kappa_2(S) = |S| + m$. This is because the second part of the proof of Theorem 15 shows us that atoms of size > 3 are incompatible with $|S|$ achieving the bound $p - \binom{m+4}{2}$: therefore A actually is a 2–atom.

The above examples are sets S

(i) that satisfy $|S + T| = |S| + |T| + m < p - 2$ for some set T containing more than one element,

(ii) that are the union of $m+3$ arithmetic progressions with the same difference but not less.

Additional examples of sets S of cardinality larger than $p - \binom{m+4}{2}$ can be found

(i) that are the union of $m + k$ arithmetic progressions but not less, for $k > 3$,

(ii) for which we also have $|S + T| = |S| + |T| + m < p - 2$ for some set T containing more than one element.

As a simple example, take $A = \{0, 1, 3, 13, 41\} \subset \mathbb{Z}/91\mathbb{Z}$. Then translates S of $\mathbb{Z}/91\mathbb{Z} \setminus (A + A)$ have $\kappa_2(S) = |S| + 5$, $\alpha_2(S) = 5$, and S is not the union of less than 9 arithmetic progressions.

References

[1] G.A. Freiman, Inverse problems of additive number theory. On the addition of sets of residues with respect to a prime modulus, **2** *Soviet. Math. Doklady*, (1961) 1520–1522.

[2] H. B. Mann, Addition theorems : The addition theorems of group theory and number theory, Interscience, New York, 1965.

[3] M. B. Nathanson, Additive number theory : Inverse problems and the Geometry of sumsets, Springer-Verlag GTM 165 (1996).

[4] Y.O. Hamidoune, An Isoperimetric method in Additive Theory, J. of Algebra **179** (1996), 622-630.

[5] Y.O. Hamidoune and Ø. J. Rødseth, An inverse theorem mod p, Acta Arithmetica, XCII.3, (2000), 251–262.

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