ISSN 2220-5438

Reprint from

Moscow Journal of Combinatorics and Number Theory

URSS

МФТИ

Volume 7 • Issue 2 2017

Moscow Journal of Combinatorics and Number Theory Volume 7 • Issue 2 2017

URSS

Moscow Journal
of Combinatorics
and Number Theory
2017, vol. 7, iss. 2,
pp. 22–58, [pp. 110–146]

An inverse theorem in $\mathbb{Z}/p\mathbb{Z}$ and rainbow-free colorings

Mario Huicochea (Mexico)

Abstract: The purpose of this paper is to improve a result of Conlon about the existence of rainbow solutions of linear equations in n variables with coefficients in $\mathbb{Z}/p\mathbb{Z}$, see [3]. To obtain his result, Conlon proves an inverse theorem, and then he demonstrates the existence of a rainbow solution. In this paper we establish an inverse theorem, and then we proceed to demonstrate a theorem on existence of rainbow solutions under weaker conditions than those in Conlon's work.

Keywords: Inverse theorem, Anti-Ramsey theory

AMS Subject Classification: 11B75,05D10

Received: 31.03.2016; **revised:** 30.01.2017

1. Introduction

Let p be a prime number bigger than 3. We denote by $\mathbb{Z}/p\mathbb{Z}$ the set of congruence classes modulo p, and we write $(\mathbb{Z}/p\mathbb{Z})^* := (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$. For any X and Y subsets of $\mathbb{Z}/p\mathbb{Z}$ and $r \in \mathbb{Z}/p\mathbb{Z}$, set

$$X + Y := \{x + y : \ x \in X, \ y \in Y\} \quad \text{and} \quad rX := \{rx : \ x \in X\}.$$

For any $n \in \mathbb{N}$, an $n-$*coloring* of $\mathbb{Z}/p\mathbb{Z}$ is a partition $\mathbb{Z}/p\mathbb{Z} = \bigcup_{i=1}^{n} X_i$ such that X_i is not empty for each $i \in \{1, \ldots, n\}$; for each $i \in \{1, \ldots, n\}$, X_i is known as a *color class*. We say that a subset Y of $\mathbb{Z}/p\mathbb{Z}$ is *rainbow* with respect to the $n-$coloring $\mathbb{Z}/p\mathbb{Z} = \bigcup_{i=1}^{n} X_i$ if Y intersects each color class; if it is clear which coloring we are talking about, we simply say that Y is rainbow. In the case where $n = 3$, Jungić et al. proved the following statement.

THEOREM 1.1. *Let $a_1, a_2, a_3 \in (\mathbb{Z}/p\mathbb{Z})^*$ be not all equal and $b \in \mathbb{Z}/p\mathbb{Z}$. For any $3-$coloring with the property that each color class has at least 4 elements, there is a rainbow subset $\{z_1, z_2, z_3\}$ of $\mathbb{Z}/p\mathbb{Z}$ such that $a_1z_1 + a_2z_2 + a_3z_3 = b$.*

PROOF. See [8]. □

Later Conlon demonstrated the following theorem.

THEOREM 1.2. *Let $n \in \mathbb{N}_{\geq 4}$ be such that $p \geq 3n^2 - 4n - 3$. Take $a_1, \ldots, a_n \in (\mathbb{Z}/p\mathbb{Z})^*$ not all equal and $b \in \mathbb{Z}/p\mathbb{Z}$. For any $n-$coloring with the property that each color class has at least n elements, there is a rainbow subset $\{z_1, \ldots, z_n\}$ of $\mathbb{Z}/p\mathbb{Z}$ such that $\sum_{i=1}^{n} a_i z_i = b$.*

PROOF. See [3]. □

The proof of the previous theorem is based on an inverse theorem. We need some notation to state it. For all $m \in \mathbb{Z}$, we denote by $\overline{m}$ its projection in $\mathbb{Z}/p\mathbb{Z}$. We write

$$\Gamma = \Gamma(p) := \{m \in \mathbb{Z} : \ 0 \leq m \leq p-1\};$$

thus Γ contains one and only one representative of each class of $\mathbb{Z}/p\mathbb{Z}$. For any $x, y \in \mathbb{Z}/p\mathbb{Z}$, let $k \in \Gamma$ be such that $\overline{k} = y - x$ and set

$$[x, y] := \left\{x + \overline{i} \in \mathbb{Z}/p\mathbb{Z} : \ i \in \Gamma, \ i \leq k\right\}$$

which is called an *interval*. For all $r \in (\mathbb{Z}/p\mathbb{Z})^*$ and $l \in \mathbb{N}$, an *arithmetic progression with difference r and length l* is a subset X of $\mathbb{Z}/p\mathbb{Z}$ such that there are $x, y \in \mathbb{Z}/p\mathbb{Z}$ satisfying that $X = r[x, y]$ and $l = |X|$.

THEOREM 1.3. *Let $n \in \mathbb{N}_{\geq 3}$ be such that $p \geq 3n^2 - 4n - 3$. Take $X_1, \ldots, X_n$ subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $\min_{1 \leq i \leq n} |X_i| \geq n + 1$ and $\sum_{i=1}^{n} |X_i| \leq p - 1$. If*

$$\left| \sum_{i=1}^{n} X_i \right| \leq \sum_{i=1}^{n} |X_i|,$$

then all the X_i are contained in arithmetic progressions with the same common difference and length at most $|X_i| + n - 1$.

PROOF. See [3]. □

In Theorem 1.3 it is allowed that the subsets $X_1, \ldots, X_n$ intersect. However, when we are working with $n-$colorings $\mathbb{Z}/p\mathbb{Z} = \bigcup_{i=1}^{n} X_i$, we have that the subsets $X_1, \ldots, X_n$ are pairwise disjoint. Proceeding in this direction, we state the first main result of this paper which is an inverse theorem and it will be used to improve Theorem 1.1 and Theorem 1.2. We denote by $\mathbb{S}_n$ the set of permutations of $\{1, \ldots, n\}$.

THEOREM 1.4. *Let $n \in \mathbb{N}_{\geq 2}$ and $a_1, \ldots, a_n \in (\mathbb{Z}/p\mathbb{Z})^*$ be not all equal. Take $X_1, \ldots, X_n$ pairwise disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $\min_{1\leq i\leq n} |X_i| \geq 4$.*

i) If $|X_1| + |X_2| \leq p - 6$ and

$$|(a_1X_1 + a_2X_2) \cup (a_2X_1 + a_1X_2)| \leq |X_1| + |X_2|,$$

then $a_1 = -a_2$ and there are $r, x, y, z, w \in \mathbb{Z}/p\mathbb{Z}$ such that

$$\{X_1, X_2\} = \{r[x, y], r[y + z, x - z] \setminus \{w\}\}.$$

ii) If $n \geq 3$ and $\sum_{i=1}^{n} |X_i| \leq p - 2$, then

$$\left| \bigcup_{\sigma\in\mathbb{S}_n} \sum_{i=1}^{n} a_{\sigma(i)}X_i \right| > \sum_{i=1}^{n} |X_i|.$$

The size of the sums of dilations has been study widely in the last few years, see [1]. In particular, there have been interesting results in groups of prime order, see [9], [10]. It was kindly remarked by the referee that Theorem 1.4 gives a (small) contribution to this area when the sets are pairwise disjoint. It would be interesting to know if some of the ideas of this paper can be used in further research about the size of the sums of dilations.

Theorem 1.4 is the main tool of the second main result of this paper which is the following theorem and it improves Theorem 1.1 and Theorem 1.2.

THEOREM 1.5. *Let $n \in \mathbb{N}_{\geq 3}$. Take $a_1, \ldots, a_n \in (\mathbb{Z}/p\mathbb{Z})^*$ not all equal and $b \in \mathbb{Z}/p\mathbb{Z}$. For any $n-$coloring with the property that each color class has at least 4 elements, there is a rainbow subset $\{z_1, \ldots, z_n\}$ of $\mathbb{Z}/p\mathbb{Z}$ such that $\sum_{i=1}^{n} a_i z_i = b$.*

There are two remarks that need to be done about the assumptions of Theorem 1.5. The first one is that if we allow $a_1 = a_2 = \ldots = a_n$, then the conclusion of Theorem 1.5 is not always true, see [7, Thm. 5]. The second point is that the conclusion of Theorem 1.5 is not always true if we allow some color classes to have

exactly one element, see [7, Thm. 6]. However, we think that maybe the conclusion of Theorem 1.5 holds if each color class has at least 2 elements (but much more effort would need to be done).

This paper is organized in the following way. In Section 2 we recall some additive number theory results, and, at the end of this section, we demonstrate an inverse result needed later. In Section 3 we develop some tools about almost arithmetic progressions used in the forthcoming sections. In Section 4 we demonstrate Theorem 1.4 when $n = 2$. Then we show Theorem 1.4 when $n = 3$ in Section 5. The proof of Theorem 1.4 is done by induction; however, to complete the induction, we need to solve some particular cases when $n > 3$ and this is done in Section 6. The proof of Theorem 1.4 is completed in Section 7 and the proof of Theorem 1.5, which is a straightforward consequence of Theorem 1.4, is finished in Section 8.

2. Additive number theory

Before we start stating the inverse theorems used in this paper, we recall the Cauchy-Davenport Theorem.

THEOREM 2.1. *Let X_1 and X_2 be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $X_1+X_2 \neq \mathbb{Z}/p\mathbb{Z}$. Then*

$$|X_1 + X_2| \geq |X_1| + |X_2| - 1.$$

PROOF. See [2, 4, 5]. □

For $r \in (\mathbb{Z}/p\mathbb{Z})^*$, a subset X of $\mathbb{Z}/p\mathbb{Z}$ is an *almost arithmetic progression with difference r* if there are an arithmetic progression Y with difference r and $y \in \mathbb{Z}/p\mathbb{Z}$ such that $X = Y \setminus \{y\}$. We remark some trivial facts about almost arithmetic progressions.

Remark 2.1. *Let X be a subset of $\mathbb{Z}/p\mathbb{Z}$ and $r \in (\mathbb{Z}/p\mathbb{Z})^*$.*

i) X is an almost arithmetic progression with difference r if and only if there are $x, y, z \in \mathbb{Z}/p\mathbb{Z}$ such that $X = r[x, y] \setminus \{z\}$.

ii) X is an almost arithmetic progression with difference r if and only if X is an almost arithmetic progression with difference $-r$ (since $r[x, y] = (-r)[-y, -x]$ for all $x, y \in \mathbb{Z}/p\mathbb{Z}$).

iii) If $X \neq \mathbb{Z}/p\mathbb{Z}$ and X is an arithmetic progression with difference r, then it is an almost arithmetic progression with difference r.

Let $r \in (\mathbb{Z}/p\mathbb{Z})^*$. The family of arithmetic progressions with difference r will be denoted by $\mathrm{AP}(r)$, and the family of almost arithmetic progressions with difference r will be denoted by $\mathrm{AAP}(r)$. With this notation we restate the well-known theorems of Vosper and Hamidoune-Rødseth.

THEOREM 2.2. *Let X_1 and X_2 be subsets of $\mathbb{Z}/p\mathbb{Z}$ such that* $\min\{|X_1|, |X_2|\} \geq 2$ *and*

$$|X_1 + X_2| = |X_1| + |X_2| - 1 \leq p - 2.$$

Then there is $r \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $X_1, X_2 \in \mathrm{AP}(r)$.

PROOF. See [11]. □

THEOREM 2.3. *Let X_1 and X_2 be subsets of $\mathbb{Z}/p\mathbb{Z}$ such that* $\min\{|X_1|, |X_2|\} \geq 3$ *and*

$$7 \leq |X_1 + X_2| = |X_1| + |X_2| \leq p - 4.$$

Then there is $r \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $X_1, X_2 \in \mathrm{AAP}(r)$.

PROOF. See [6]. □

Another inverse result needed in Section 5 is the following statement.

LEMMA 2.1. *Let X and Y be subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|X| \geq 4$ and $X+Y \neq \mathbb{Z}/p\mathbb{Z}$. Assume that $X \in \mathrm{AP}(r)$ for some $r \in (\mathbb{Z}/p\mathbb{Z})^*$. If*

$$|X + Y| \leq |X| + |Y| + 1,$$

then there are $z, w, u, v \in \mathbb{Z}/p\mathbb{Z}$ such that $Y = r[z, w] \setminus \{u, v\}$.

PROOF. We assume that $r = 1$ (otherwise we consider $r^{-1}X$ and $r^{-1}Y$ instead of X and Y respectively). Furthermore, translating X if necessary, we assume that $X = [0, x]$ for some $x \in \mathbb{Z}/p\mathbb{Z}$. Write $Y = \bigcup_{i=1}^{n} [z_i, w_i]$ such that

- For all $i, j \in \{1, \ldots, n\}$, $[z_i - 1, w_i + 1] \cap [z_j, w_j] = \varnothing$ if $i \neq j$.
- For all $i \in \{1, \ldots, n-1\}$, $[w_i+1, z_{i+1}-1] \cap Y = \varnothing$ and $[w_n+1, z_1-1] \cap Y = \varnothing$.

In particular, $\mathbb{Z}/p\mathbb{Z} \setminus Y = [w_n + 1, z_1 - 1] \cup \bigcup_{i=1}^{n-1} [w_i + 1, z_{i+1} - 1]$. If $[z_n, w_n + x] \cap$ $\cap [z_1, w_1] \neq \varnothing$ and $[z_i, w_i + x] \cap [z_{i+1}, w_{i+1}] \neq \varnothing$ for each $i \in \{1, \ldots, n - 1\}$, then $[z_n, w_n + x] \supseteq [w_n + 1, z_1 - 1]$ and $[z_i, w_i + x] \supseteq [w_i + 1, z_{i+1} - 1]$ for each

$i \in \{1, \dots, n-1\}$. Thus, in this case,

$$X + Y = \bigcup_{i=1}^{n} [z_i, w_i + n] \supseteq [w_n + 1, z_1 - 1] \cup \bigcup_{i=1}^{n-1} [w_i + 1, z_{i+1} - 1] = \mathbb{Z}/p\mathbb{Z} \setminus Y.$$

However, this is impossible since $Y \subseteq X+Y$ and $X+Y \neq \mathbb{Z}/p\mathbb{Z}$. Hence we assume without loss of generality that $[z_n, w_n + x] \cap [z_1, w_1] = \varnothing$ and therefore

$$[w_n + 1, w_n + x] \subseteq (X + Y) \setminus [z_1, w_n]. \tag{1}$$

For all $i \in \{1, \dots, n-1\}$, define $Z_i := [w_i+1, w_i+3]$ if $|[w_i+1, z_{i+1}-1]| > 3$ and $Z_i := [w_i + 1, z_{i+1} - 1]$ otherwise. Note that $|Z_i| \geq 1$ for each $i \in \{1, \dots, n-1\}$. Since $|X| \geq 4$, we have that $[0, 3] \subseteq X$ and therefore

$$\bigcup_{i=1}^{n-1} Z_i \subseteq (X + Y) \cap [z_1, w_n].$$

By the construction of the subsets Z_i and (1), we have that

$$Z := Y \cup \bigcup_{i=1}^{n-1} Z_i \cup [w_n + 1, w_n + x]$$

is a disjoint union. Furthermore, since $Y = 0 + Y \subseteq X + Y$, we have that Z is a subset of $X + Y$, and then

$$\begin{aligned} \sum_{i=1}^{n} |Z_i| &= |Z| - |[w_n + 1, w_n + x]| - |Y| \\ &= |Z| - (|X| - 1) - |Y| \\ &\leq |X + Y| - (|X| - 1) - |Y| \\ &\leq 2. \end{aligned} \tag{2}$$

From (2) we have that $n \leq 2$, and thereby $Z_i = [w_i + 1, z_{i+1} - 1]$ for all $i \in \{1, \dots, n-1\}$. Taking $z = z_1$ and $w = w_n$, by (2), we have the existence of $u, v \in \mathbb{Z}/p\mathbb{Z}$ such that $Y = [z, w] \setminus \{u, v\}$ as desired. □

3. Almost arithmetic progressions

In the previous section we defined the almost arithmetic progressions. In this section we continue studying their properties.

LEMMA 3.1. *Let X and Y be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ and $d \in \mathbb{Z}/p\mathbb{Z}$. If $X \subseteq Y$ and $|Y \setminus X| \leq 1$, then*

$$\big||(Y+d) \setminus Y| - |(X+d) \setminus X|\big| \leq 1.$$

PROOF. For any subset Z of $\mathbb{Z}/p\mathbb{Z}$,

$$|(Z+d) \setminus Z| = |Z| - |(Z+d) \cap Z|. \tag{3}$$

If $|Y \setminus X| = 0$, the statement is trivial. Therefore, from now on, we assume that $Y \setminus X \neq \varnothing$. Let $x \in Y \setminus X$, so that $Y = X \cup \{x\}$. Note that

$$\begin{aligned}
|(Y+d) \setminus Y| =& |((X \cup \{x\}) + d) \setminus (X \cup \{x\})| \\
=& |(X+d) \setminus (X \cup \{x\})| \\
&+ |\{x+d\} \setminus (X \cup \{x\})| && \Big(\text{since } x \notin X\Big) \\
=& |X+d| - |(X+d) \cap (X \cup \{x\})| \\
&+ |\{x+d\}| - |\{x+d\} \cap (X \cup \{x\})| && \Big(\text{by (3)}\Big) \\
=& |X+d| - |(X+d) \cap X| - |(X+d) \cap \{x\}| \\
&+ 1 - |\{x+d\} \cap (X \cup \{x\})| && \Big(\text{since } x \notin X\Big) \\
=& |(X+d) \setminus X| - |(X+d) \cap \{x\}| + 1 \\
&- |\{x+d\} \cap (X \cup \{x\})|. && \Big(\text{by (3)}\Big) \quad (4)
\end{aligned}$$

Since

$$\Big|1 - |(X+d) \cap \{x\}| - |\{x+d\} \cap (X \cup \{x\})|\Big| \leq 1,$$

the claim is a consequence of (4). □

Recall that

$$\Gamma := \{m \in \mathbb{Z} : \ 0 \leq m \leq p-1\},$$

and also recall that $\overline{m}$ is the projection of $m \in \mathbb{Z}$ into $\mathbb{Z}/p\mathbb{Z}$.

LEMMA 3.2. *Let $d \in \mathbb{Z}/p\mathbb{Z}$ and $X \in \mathrm{AP}(1)$. If $m \in \Gamma$ is such that $\overline{m} = d$, then*

$$|(X+d) \setminus X| = \min\{m, p-m, |X|, p-|X|\}.$$

PROOF. If $|X| \le p - |X|$, then

$$|(X+d) \setminus X| = \begin{cases} m & \text{if } d \in \{0, \dots, \overline{|X|}\}; \\ |X| & \text{if } d \in \{\overline{|X|}, \dots, \overline{p-|X|}\}; \\ p-m & \text{if } d \in \{\overline{p-|X|}, \dots, p-1\}. \end{cases}$$

If $|X| \ge p - |X|$, then

$$|(X+d) \setminus X| = \begin{cases} m & \text{if } d \in \{0, \dots, \overline{p-|X|}\}; \\ p-|X| & \text{if } d \in \{\overline{p-|X|}, \dots, \overline{|X|}\}; \\ p-m & \text{if } d \in \{\overline{|X|}, \dots, p-1\}. \end{cases}$$

In any case our claim is true. □

LEMMA 3.3. *Let $d \in \mathbb{Z}/p\mathbb{Z}$ and $X \in \mathrm{AAP}(1)$. If $m \in \Gamma$ is such that $\overline{m} = d$, then*

$$|(X+d) \setminus X| \ge \min\{m, p-m, |X|, p-|X|\} - 2.$$

Furthermore, if

$$\min\{m, p-m, |X|, p-|X|\} \ne p-|X|,$$

then

$$|(X+d) \setminus X| \ge \min\{m, p-m, |X|, p-|X|\} - 1.$$

PROOF. Let $Y \in \mathrm{AP}(1)$ and $y \in \mathbb{Z}/p\mathbb{Z}$ be such that $X = Y \setminus \{y\}$. Note that $X \subseteq Y$ and $|Y \setminus X| \le 1$; then Lemma 3.1 yields

$$\big|\,|(Y+d) \setminus Y| - |(X+d) \setminus X|\,\big| \le 1. \tag{5}$$

On the one hand,

$$\min\{m, p-m, |Y|, p-|Y|\} \ge \min\{m, p-m, |X|, p-|X|\} - 1, \tag{6}$$

and the first claim follows from Lemma 3.2, (5) and (6).

On the other hand, if

$$\min\{m, p-m, |X|, p-|X|\} \neq p-|X|,$$

then

$$\min\{m, p-m, |Y|, p-|Y|\} \geq \min\{m, p-m, |X|, p-|X|\}. \tag{7}$$

Thus the second claim follows from Lemma 3.2, (5) and (7). □

In several parts of the proof of Theorem 1.4, the following two lemmas will be used.

LEMMA 3.4. *Let X be a subset of $\mathbb{Z}/p\mathbb{Z}$ such that $2 \leq |X| \leq p-2$ and $r, t \in (\mathbb{Z}/p\mathbb{Z})^*$. If $X, tX \in \mathrm{AP}(r)$, then $t \in \{\pm 1\}$.*

PROOF. Assume, without loss of generality, that $r = 1$ (otherwise we take $r^{-1}X$ instead of X). Since $X \in \mathrm{AP}(1)$, there are $x, y \in \mathbb{Z}/p\mathbb{Z}$ such that $X = [x, y]$ and therefore

$$|(X+1) \setminus X| = |[x+1, y+1] \setminus [x, y]| = 1. \tag{8}$$

Let $m \in \Gamma$ be such that $\overline{m} = t$. From Lemma 3.2

$$\begin{aligned} \min\{m, p-m, |X|, p-|X|\} &= \min\{m, p-m, |tX|, p-|tX|\} \\ &= |(tX+t) \setminus tX| \\ &= |(X+1) \setminus X|. \end{aligned} \tag{9}$$

From (8) and (9),

$$\min\{m, p-m, |X|, p-|X|\} = 1;$$

however, the inequality $2 \leq |X| \leq p-2$ implies that

$$\min\{m, p-m\} = 1$$

so $m \in \{1, p-1\}$ and finally $t \in \{\pm 1\}$. □

LEMMA 3.5. *Let X be a subset of $\mathbb{Z}/p\mathbb{Z}$ such that $4 \leq |X| \leq p-5$ and $r, t \in (\mathbb{Z}/p\mathbb{Z})^*$. If $X, tX \in \mathrm{AAP}(r)$, then $t \in \{\pm 1\}$.*

PROOF. Assume without loss of generality that $r = 1$ (otherwise we take $r^{-1}X$ instead of X). Since $X \in \mathrm{AAP}(1)$, there are $x, y, z \in \mathbb{Z}/p\mathbb{Z}$ such that $X = [x, y] \setminus \{z\}$ and therefore

$$|(X+1) \setminus X| = \big|\big([x+1, y+1] \setminus \{z+1\}\big) \setminus \big([x, y] \setminus \{z\}\big)\big| \leq 2. \tag{10}$$

Let $m \in \Gamma$ be such that $\overline{m} = t$. Now we show that $\min\{m, p-m, |X|, p-|X|\} \neq$ $\neq p - |X|$ by contradiction. Assume that $\min\{m, p-m, |X|, p-|X|\} = p - |X|$. Since $tX \in \mathrm{AAP}(1)$, the first claim of Lemma 3.3 yields

$$\begin{aligned} p - |X| - 2 &= \min\{m, p-m, |X|, p-|X|\} - 2 \\ &= \min\{m, p-m, |tX|, p-|tX|\} - 2 \\ &\leq |(tX+t) \setminus tX| \\ &= |(X+1) \setminus X|. \end{aligned} \tag{11}$$

Hence (10) and (11) lead to

$$p - 4 \leq |X|$$

and this contradicts the inequality $|X| \leq p-5$. Thus $\min\{m, p-m, |X|, p-|X|\} \neq$ $\neq p - |X|$. The second claim of Lemma 3.3 yields

$$\begin{aligned} \min\{m, p-m, |X|, p-|X|\} - 1 &= \min\{m, p-m, |tX|, p-|tX|\} - 1 \\ &\leq |(tX+t) \setminus tX| \\ &= |(X+1) \setminus X|. \end{aligned} \tag{12}$$

From (10) and (12),

$$\min\{m, p-m, |X|, p-|X|\} \leq 3,$$

and thereby the inequalities $4 \leq |X| \leq p-5$ let us conclude that

$$\min\{m, p-m\} = \min\{m, p-m, |X|, p-|X|\} \leq 3. \tag{13}$$

We show that $m \neq 2$ by contradiction. If $m = 2$, then $t = 2$, and therefore $2X = 2([x, y] \setminus \{z\}) \in \mathrm{AAP}(1)$; however, this will mean that $|[x, y]| \leq 2$ or $|[x, y]| \geq p-3$ which is impossible due to the inequality $4 \leq |X| \leq p-5$. In

the same way it is proven that $m \notin \{3, p-2, p-3\}$. From (13) we conclude that $m \in \{1, p-1\}$ and consequently $t \in \{\pm 1\}$. □

With similar ideas to the ones used in the previous lemmas, we demonstrate the following claim used in Section 4.

LEMMA 3.6. *Let X and Y be subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $6 \leq |X| \leq p-6$, $X \subseteq Y$ and $|Y \setminus X| \leq 1$. Take $r, s \in (\mathbb{Z}/p\mathbb{Z})^*$. If $X \in \mathrm{AAP}(r)$ and $Y \in \mathrm{AAP}(s)$, then $r \in \{\pm s\}$.*

PROOF. Assume without loss of generality that $s = 1$ (otherwise we take $s^{-1}X$ and $s^{-1}Y$ instead of X and Y respectively). Since $Y \in \mathrm{AAP}(1)$, there are $x, y, z \in \mathbb{Z}/p\mathbb{Z}$ such that $Y = [x, y] \setminus \{z\}$, and therefore

$$|(Y+1) \setminus Y| = \big|\big([x+1, y+1] \setminus \{z+1\}\big) \setminus \big([x, y] \setminus \{z\}\big)\big| \leq 2. \tag{14}$$

Furthermore, Lemma 3.1 yields

$$|(X+1) \setminus X| \leq |(Y+1) \setminus Y| + 1,$$

and then (14) leads to

$$|(X+1) \setminus X| \leq 3. \tag{15}$$

Let $m \in \Gamma$ be such that $\overline{m} = r^{-1}$. Since $X \in \mathrm{AAP}(r)$, we have that $r^{-1}X \in \mathrm{AAP}(1)$ and the first claim of Lemma 3.3 yields

$$\begin{aligned} \min\{m, p-m, |X|, p-|X|\} - 2 &= \min\{m, p-m, |r^{-1}X|, p-|r^{-1}X|\} - 2 \\ &\leq |(r^{-1}X + r^{-1}) \setminus r^{-1}X| \\ &= |(X+1) \setminus X|. \end{aligned} \tag{16}$$

From (15) and (16)

$$\min\{m, p-m, |X|, p-|X|\} \leq 5,$$

and then, from the inequalities $6 \leq |X| \leq p-6$, we conclude that

$$\min\{m, p-m\} \leq 5. \tag{17}$$

We show that $m \neq 2$ by contradiction. If $m = 2$, then $r = 2^{-1}$. With this value of r, if X is contained in an almost arithmetic progression Z with difference 1 such that

$|Z \setminus X| \leq 1$, then $|Z| \geq p-3$ or $|Z| \leq 3$. This would mean that $X \nsubseteq Y$ which is impossible. In the same way it is proven that $m \notin \{3, 4, 5, p-2, p-3, p-4, p-5\}$; then $m \in \{1, p-1\}$ by (17), and finally $r \in \{\pm 1\}$. □

For all $x \in \mathbb{R}$, we denote by $[x]$ its integral part. The following result is a technical lemma that will be used in the proof of Lemma 3.8 which is very important in the proof of Theorem 1.4.

LEMMA 3.7. *Let $w, z \in \mathbb{Z}/p\mathbb{Z}$ and $t \in (\mathbb{Z}/p\mathbb{Z})^*$. Take $m \in \Gamma$ such that $\overline{m} = t^{-1}$. If $i, j \in \Gamma$ are such that $0 \leq i, j \leq m-1$ and $(w+\bar{i})t, (w+\bar{j})t \in \left[z, z+\left[\overline{\frac{p}{m}}\right]-1\right]$, then $i = j$.*

PROOF. If $(w+\bar{i})t, (w+\bar{j})t \in \left[z, z+\left[\overline{\frac{p}{m}}\right]-1\right]$, then $(w-t^{-1}z+\bar{i})t, (w-t^{-1}z+\bar{j})t \in \in \left[0, \left[\overline{\frac{p}{m}}\right]-1\right]$, and consequently either $\{0, (\bar{i}-\bar{j})t\} \subseteq \left[0, \left[\overline{\frac{p}{m}}\right]-1\right]$ or $\{0, (\bar{j}-\bar{i})t\} \subseteq \subseteq \left[0, \left[\overline{\frac{p}{m}}\right]-1\right]$; we assume, without loss of generality, that $\{0, (\bar{i}-\bar{j})t\} \subseteq \left[0, \left[\overline{\frac{p}{m}}\right]-1\right]$. Thus there exist $l, n, a, q, b \in \Gamma$ such that $b \leq \left[\frac{p}{m}\right]-1$ and

$$\begin{aligned} \overline{n} &= t, \\ \bar{l} &= \bar{i} - \bar{j}, \\ \bar{b} &= t(\bar{i} - \bar{j}), \\ mn &= qp + 1, \\ ln &= ap + b. \end{aligned}$$

Since $0 \leq i, j \leq m-1$, we get that $0 \leq l < m$ and then

$$a < q. \tag{18}$$

Now see that

$$\begin{aligned} lqp + l &= l(qp+1) \\ &= lmn \\ &= mln \\ &= m(ap+b) \\ &= amp + mb, \end{aligned}$$

and, since $l, mb \in \Gamma$, we arrive to the equalities

$$l = mb \quad \text{and} \quad lq = am. \tag{19}$$

Now (19) leads to

$$am = mbq$$

and therefore

$$a = bq. \tag{20}$$

By (18) and (20), we conclude that $a = b = 0$ and thereby $i = j$. □

The following lemma is very important in the proof of Theorem 1.4. For arbitrary $r, s \in (\mathbb{Z}/p\mathbb{Z})^*$, it bounds the cardinality of an arithmetic progression with difference s which contains an arithmetic progression with difference r.

LEMMA 3.8. *Let $x, y, z, w \in \mathbb{Z}/p\mathbb{Z}$, $r, s \in (\mathbb{Z}/p\mathbb{Z})^*$ and Y be a subset of $[z, w]$. Take $m \in \Gamma$ such that $\overline{m} = r^{-1}s$. If $r[x, y] = s([z, w] \setminus Y)$, then*

$$|Y| + 1 \geq \min\left\{p - m, m, |[x, y]|, p - |[x, y]|\right\}.$$

Furthermore, if $|[x, y]| \geq \min\{m, p - m\}$, then

$$|[z, w]| \geq \left[\frac{|[x, y]|}{\min\{m, p - m\}}\right] + (\min\{m, p - m\} - 1)\left[\frac{p}{\min\{m, p - m\}}\right].$$

PROOF. We start by proving the first claim. Write $[z, w] \setminus Y = \bigcup_{i=1}^{n} [z_i, w_i]$ where $[z_i - 1, w_i + 1] \cap [z_j, w_j] = \varnothing$ if $i \neq j$. Note that $n \leq |Y|$, and therefore

$$\begin{aligned} \Big|\big(s([z, w] \setminus Y) + s\big) \setminus s([z, w] \setminus Y)\Big| &= \Big|\big(([z, w] \setminus Y) + 1\big) \setminus ([z, w] \setminus Y)\Big| \\ &\leq n + 1 \\ &\leq |Y| + 1. \end{aligned} \tag{21}$$

On the other hand, Lemma 3.2 implies

$$\begin{aligned} \Big|\big(r[x, y] + s\big) \setminus r[x, y]\Big| &= \Big|\big([x, y] + r^{-1}s\big) \setminus [x, y]\Big| \\ &= \min\left\{p - m, m, |[x, y]|, p - |[x, y]|\right\}. \end{aligned} \tag{22}$$

The first claim follows from (21) and (22) since $r[x, y] = s([z, w] \setminus Y)$.

We start the proof of the second statement. We divide it into two cases.

- First we assume that

$$m = \min\{m, p-m\}. \tag{23}$$

For all $u \in \mathbb{Z}/p\mathbb{Z}$, define

$$L(u) := rs^{-1}[x,y] \cap \left[u, u + \overline{\left[\frac{p}{m}\right]} - 1\right];$$

$$M(u) := rs^{-1}[x,y] \cap \left[u + \overline{(m-1)\left[\frac{p}{m}\right]}, u - 1\right].$$

Now see that $\mathbb{Z}/p\mathbb{Z}$ is equal to the disjoint union

$$\left(\bigcup_{i=0}^{m-2}\left[u + \overline{i\left[\frac{p}{m}\right]}, u + \overline{(i+1)\left[\frac{p}{m}\right]} - 1\right]\right) \cup \left[u + \overline{(m-1)\left[\frac{p}{m}\right]}, u - 1\right]$$

and therefore, intersecting with $rs^{-1}[x,y]$, we obtain that

$$rs^{-1}[x,y] = \left(\bigcup_{i=0}^{m-2} L\left(u + \overline{i\left[\frac{p}{m}\right]}\right)\right) \cup M(u) \tag{24}$$

where the left-hand side union is also disjoint. For all $j \in \Gamma$ such that $0 \le j \le m-2$, Lemma 3.7 implies that if $v \in \mathbb{Z}/p\mathbb{Z}$ is such that $rs^{-1}v \in L\left(u + \overline{j\left[\frac{p}{m}\right]}\right)$, then, for all $i \in \Gamma$ such that $1 \le i \le m-1$, we have that $rs^{-1}(v+\bar{i}) \notin L\left(u + \overline{j\left[\frac{p}{m}\right]}\right)$. Thus, by the Pigeonhole Principle and (24), for all $v \in \mathbb{Z}/p\mathbb{Z}$ such that $\left[v, v+\overline{m-1}\right] \subseteq [x,y]$, we have that $M(u)$ has an element of $rs^{-1}\left[v, v+\overline{m-1}\right]$; consequently

$$|M(u)| \ge \frac{|[x,y]|}{m}. \tag{25}$$

Since $r[x,y] \subseteq s[z,w]$, we have that $s[w+1, z-1] \subseteq \mathbb{Z}/p\mathbb{Z} \setminus r[x,y]$ and then

$$[w+1, z-1] \subseteq \mathbb{Z}/p\mathbb{Z} \setminus rs^{-1}[x,y]. \tag{26}$$

By the Pigeonhole Principle, there is no interval Z with $|Z| < (m-1)\left[\frac{p}{m}\right]$ containing all the points $rs^{-1}x, rs^{-1}(x+1), \ldots, rs^{-1}(x+\overline{m-2})$ (otherwise we contradict Lemma 3.7). Thus, since $|[x,y]| \ge \min\{m, p-m\} = m$, the previous assertion yields $rs^{-1}[x,y]$ is not contained in an interval Z when

$|Z| < (m-1)\left[\frac{p}{m}\right]$, and consequently

$$|[w+1, z-1]| \leq p - (m-1)\left[\frac{p}{m}\right].$$

Thus there is $u_0 \in \mathbb{Z}/p\mathbb{Z}$ such that

$$[w+1, z-1] \subseteq \left[u_0 + \overline{(m-1)\left[\frac{p}{m}\right]}, u_0 - 1\right].$$

Note that $[w+1, z-1]$ and $M(u_0)$ are disjoint by (26). Hence

$$\begin{aligned} |[w+1, z-1]| &\leq \left|\left[u_0 + \overline{(m-1)\left[\frac{p}{m}\right]}, u_0 - 1\right]\right| - |M(u_0)| \\ &= p - (m-1)\left[\frac{p}{m}\right] - |M(u_0)| \\ &\leq p - (m-1)\left[\frac{p}{m}\right] - \frac{|[x,y]|}{m}. \qquad \Big(\text{by (25)}\Big) \end{aligned} \tag{27}$$

Finally,

$$\begin{aligned} |[z,w]| =& p - |[w+1, z-1]| \\ \geq& p - \left(p - (m-1)\left[\frac{p}{m}\right] - \frac{|[x,y]|}{m}\right) \qquad \Big(\text{by (27)}\Big) \\ \geq& \left[\frac{|[x,y]|}{m}\right] + (m-1)\left[\frac{p}{m}\right] \\ =& \left[\frac{|[x,y]|}{\min\{m, p-m\}}\right] \\ &+ (\min\{m, p-m\} - 1)\left[\frac{p}{\min\{m, p-m\}}\right]. \end{aligned}$$

- Now we assume that (23) is false (in other words, $\min\{m, p-m\} \neq m$). Note that

$$(-r)[-y, -x] = r[x,y] = s([z,w] \setminus Y),$$

and $p-m$ is the element of Γ with the property that $\overline{p-m} = (-r)^{-1}s$. Moreover, since (23) is false, we have that

$$p - m = \min\{m, p-m\} = \min\{p-(p-m), p-m\}.$$

Thus we may apply the previous case to find a lower bound of $|[z,w]|$ taking $[-y,-x]$ (resp. $(-r)^{-1}s$, $p-m$) instead of $[x,y]$ (resp. $r^{-1}s$, m), and we get that

$$\begin{aligned} |[z,w]| &\geq \left[\frac{|[-y,-x]|}{(p-m)}\right] + ((p-m)-1)\left[\frac{p}{p-m}\right] \\ &= \left[\frac{|[x,y]|}{\min\{m,p-m\}}\right] + (\min\{m,p-m\}-1)\left[\frac{p}{\min\{m,p-m\}}\right]. \end{aligned}$$

□

4. Case $n = 2$

In this section we show Theorem 1.4 when $n = 2$. First we prove the following statement.

LEMMA 4.1. *Let $a_1, a_2 \in (\mathbb{Z}/p\mathbb{Z})^*$ be such that $a_1 \notin \{\pm a_2\}$. Take X_1 and X_2 disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $\min\{|X_1|, |X_2|\} \geq 4$ and $|X_1| + |X_2| \leq p-6$. Then*

$$|(a_1X_1 + a_2X_2) \cup (a_2X_1 + a_1X_2)| > |X_1| + |X_2|.$$

PROOF. Write

$$X := (a_1X_1 + a_2X_2) \cup (a_2X_1 + a_1X_2) \text{ and } Y := (a_1X_1 + a_2X_2) \cap (a_2X_1 + a_1X_2).$$

We assume that the claim is false and we will get a contradiction. Thus assume that

$$|X| \leq |X_1| + |X_2|. \tag{28}$$

Theorem 2.1, applied to the sumsets $|a_1X_1 + a_2X_2|$ and $|a_2X_1 + a_1X_2|$, yields

$$\min\{|a_1X_1 + a_2X_2|, |a_2X_1 + a_1X_2|\} \geq |X_1| + |X_2| - 1,$$

and then (28) leads to

$$|a_1X_1 + a_2X_2|, |a_2X_1 + a_1X_2|, |X| \in \{|X_1| + |X_2| - 1, |X_1| + |X_2|\}. \tag{29}$$

We have two cases.

- Assume that

$$|a_1X_1 + a_2X_2| = |a_2X_1 + a_1X_2| = |X_1| + |X_2| - 1. \tag{30}$$

The equality $|a_1X_1 + a_2X_2| = |X_1| + |X_2| - 1$ implies, by Theorem 2.2, the existence of $r \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a_1X_1, a_2X_2 \in \mathrm{AP}(r)$. In the same way the equality $|a_2X_1 + a_1X_2| = |X_1| + |X_2| - 1$ yields the existence of $s \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a_2X_1, a_1X_2 \in \mathrm{AP}(s)$. Thus $a_1X_1, (rs^{-1}a_2a_1^{-1})a_1X_1 \in \mathrm{AP}(r)$. Then, from Lemma 3.4, we conclude that $rs^{-1}a_2a_1^{-1} \in \{\pm 1\}$ and then

$$ra_2 \in \{\pm sa_1\}. \tag{31}$$

Also $a_2X_2, (rs^{-1}a_1a_2^{-1})a_2X_2 \in \mathrm{AP}(r)$. Hence, from Lemma 3.4, we deduce that $rs^{-1}a_1a_2^{-1} \in \{\pm 1\}$ and therefore

$$ra_1 \in \{\pm sa_2\}. \tag{32}$$

Since $a_1 \notin \{\pm a_2\}$, we get from (31) and (32) that

$$r^2 = -s^2. \tag{33}$$

We have that

$$|X| + |Y| = |a_1X_1 + a_2X_2| + |a_2X_1 + a_1X_2|;$$

this equality, (29) and (30) imply that $|Y| \geq |X_1| + |X_2| - 2$. In particular, since $Y \subseteq a_2X_1 + a_1X_2$ and $a_2X_1 + a_1X_2 \in \mathrm{AP}(s)$, we have that $Y \in \mathrm{AAP}(s)$. In the same way we deduce that $Y \in \mathrm{AAP}(r)$. We conclude that $Y, rs^{-1}Y \in \mathrm{AAP}(r)$, and then Lemma 3.5 implies $rs^{-1} \in \{\pm 1\}$ contradicting (33).

- Assume that (30) is false. Suppose, without loss of generality, that

$$|a_1X_1 + a_2X_2| = |X_1| + |X_2|. \tag{34}$$

The equality $|a_1X_1 + a_2X_2| = |X_1| + |X_2|$ implies, by Theorem 2.3, the existence of $r \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a_1X_1, a_2X_2 \in \mathrm{AAP}(r)$. If $|a_2X_1 + a_1X_2| = |X_1| + |X_2| - 1$, Theorem 2.2 yields the existence of $s \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a_2X_1, a_1X_2 \in \mathrm{AP}(s)$. If $|a_2X_1 + a_1X_2| = |X_1| + |X_2|$, Theorem 2.3 yields the existence of $s \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a_2X_1, a_1X_2 \in \mathrm{AAP}(s)$. In any case there is $s \in (\mathbb{Z}/p\mathbb{Z})^*$ such that

$a_2X_1, a_1X_2 \in \mathrm{AAP}(s)$. Now see that $a_1X_1, (rs^{-1}a_2a_1^{-1})a_1X_1 \in \mathrm{AAP}(r)$. Then, from Lemma 3.5, we conclude that $rs^{-1}a_2a_1^{-1} \in \{\pm 1\}$, and hence

$$ra_2 \in \{\pm sa_1\}. \tag{35}$$

Also $a_2X_2, (rs^{-1}a_1a_2^{-1})a_2X_2 \in \mathrm{AAP}(r)$. From Lemma 3.5 we see that $rs^{-1}a_1a_2^{-1} \in \{\pm 1\}$ and therefore

$$ra_1 \in \{\pm sa_2\}. \tag{36}$$

Since $a_1 \notin \{\pm a_2\}$, we obtain from (35) and (36) that

$$r^2 = -s^2. \tag{37}$$

If

$$|a_2X_1 + a_1X_2| = |X_1| + |X_2|,$$

then (29) leads to

$$a_2X_1 + a_1X_2 = a_1X_1 + a_2X_2.$$

This means that $a_1X_1 + a_2X_2 \in \mathrm{AAP}(r)$ and $a_1X_1 + a_2X_2 \in \mathrm{AAP}(s)$. In other words, $a_1X_1 + a_2X_2, rs^{-1}(a_1X_1 + a_2X_2) \in \mathrm{AAP}(r)$ and Lemma 3.5 let us conclude $rs^{-1} \in \{\pm 1\}$ contradicting (37). If

$$|a_2X_1 + a_1X_2| \neq |X_1| + |X_2|,$$

then (29) implies that

$$|a_2X_1 + a_1X_2| = |X_1| + |X_2| - 1.$$

From (29) and (34), we have that

$$a_2X_1 + a_1X_2 \subseteq a_1X_1 + a_2X_2.$$

Recall that $a_1X_1 + a_2X_2 \in \mathrm{AAP}(r)$ and $a_1X_1 + a_2X_2 \in \mathrm{AAP}(s)$, so Lemma 3.6 applied to these almost arithmetic progressions yields $r \in \{\pm s\}$ contradicting (37). □

Now we proof Theorem 1.1 when $n = 2$.

THEOREM 4.1. *Let $a_1, a_2 \in (\mathbb{Z}/p\mathbb{Z})^*$ be such that $a_1 \neq a_2$. Take X_1 and X_2 disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$ such that* $\min\{|X_1|, |X_2|\} \geq 4$ *and* $|X_1| + |X_2| \leq p - 6$. *If*

$$|(a_1X_1 + a_2X_2) \cup (a_2X_1 + a_1X_2)| \leq |X_1| + |X_2|,$$

then $a_1 = -a_2$ and there are $r, x, y, z, w \in \mathbb{Z}/p\mathbb{Z}$ such that

$$\{X_1, X_2\} = \{r[x, y], r[y + z, x - z] \setminus \{w\}\}.$$

PROOF. From Lemma 4.1 we have that $a_1 = -a_2$. Write

$$X := (a_1X_1 + a_2X_2) \cup (a_2X_1 + a_1X_2).$$

Theorem 2.1, applied to the sumsets $|a_1X_1 + a_2X_2|$ and $|a_2X_1 + a_1X_2|$, yields

$$\min\{|a_1X_1 + a_2X_2|, |a_2X_1 + a_1X_2|\} \geq |X_1| + |X_2| - 1,$$

and then, since $|X| \leq |X_1| + |X_2|$, we conclude that

$$|a_1X_1 + a_2X_2|, |a_2X_1 + a_1X_2|, |X| \in \{|X_1| + |X_2| - 1, |X_1| + |X_2|\}.$$

If $|a_1X_1 + a_2X_2| = |X_1| + |X_2| - 1$, Theorem 2.2 yields the existence of $s \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a_1X_1, a_2X_2 \in \mathrm{AP}(s)$. If $|a_1X_1 + a_2X_2| = |X_1| + |X_2|$, Theorem 2.3 yields the existence of $s \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a_1X_1, a_2X_2 \in \mathrm{AAP}(s)$. In any case there is $s \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a_1X_1, a_2X_2 \in \mathrm{AAP}(s)$. Write $r := a_1^{-1}s$. Since $a_1 = -a_2$, there are $x_1, y_1, x_2, y_2, z_1, z_2 \in \mathbb{Z}/p\mathbb{Z}$ such that $X_1 = r[x_1, y_1] \setminus \{z_1\}$ and $X_2 = r[x_2, y_2] \setminus \{z_2\}$. Since $|X| \leq |X_1| + |X_2|$ and $a_1 = -a_2$, we have that

$$x_1 - y_2 \in \{x_2 - y_1 + i : \ i \in \{0, \pm 1\}\};$$

checking these cases we obtain straightforward the existence of $x, y, z, w \in \mathbb{Z}/p\mathbb{Z}$ such that

$$\{X_1, X_2\} = \{r[x, y], r[y + z, x - z] \setminus \{w\}\}. \square$$

5. Case $n = 3$

We demonstrate Theorem 1.4 when $n = 3$ in this section. For all X and Y subsets of $\mathbb{Z}/p\mathbb{Z}$,

$$X - Y := X + (-Y) = \{x - y : \ x \in X, \ y \in Y\}.$$

We need an auxiliary result.

LEMMA 5.1. *Let X and Y be subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $\min\{|X|, |Y|\} \geq 4$ and $X - Y \neq \mathbb{Z}/p\mathbb{Z}$. Assume that there are $r, x, y \in \mathbb{Z}/p\mathbb{Z}$ such that $X = r[x, y]$. If*

$$|(X - Y) \cup (Y - X)| \leq |X| + |Y| + 1,$$

then there are $v, w, z \in \mathbb{Z}/p\mathbb{Z}$ such that $Y = r[y + z, x - z] \setminus \{v, w\}$.

PROOF. We have that

$$|X - Y| \leq |(X - Y) \cup (Y - X)| \leq |X| + |Y| + 1. \tag{38}$$

If we apply Lemma 2.1 to the sets X and $-Y$, we get that there are $z', w', u', v' \in \mathbb{Z}/p\mathbb{Z}$ such that $-Y = r[z', w'] \setminus \{u', v'\}$. Thus, to achieve (38), we need that

$$-(x + z') \in \{y + w' + i : \ i \in \{\pm 2, \pm 1, 0\}\}. \tag{39}$$

Checking the cases that we have by (39), we conclude from (38) that there are $v, w, z \in \mathbb{Z}/p\mathbb{Z}$ such that $Y = r[y + z, x - z] \setminus \{v, w\}$. □

The previous lemma is applied in the following statement.

LEMMA 5.2. *Let $a_1, a_2, a_3 \in (\mathbb{Z}/p\mathbb{Z})^*$ be not all equal and assume that $a_i \in \{\pm a_j\}$ for all $i, j \in \{1, 2, 3\}$. Take X_1, X_2, X_3 pairwise disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $\min_{1 \leq i \leq 3} |X_i| \geq 4$ and $\sum_{i=1}^{3} |X_i| \leq p - 2$. Then*

$$\left| \bigcup_{\sigma \in \mathbb{S}_3} \sum_{i=1}^{3} a_{\sigma(i)} X_i \right| > \sum_{i=1}^{3} |X_i|.$$

PROOF. Assume, without loss of generality, that $a_1 = -a_2$. Set

$$Y := \bigcup_{\sigma \in \mathbb{S}_3} \sum_{i=1}^{3} a_{\sigma(i)} X_i,$$

and for any choice $\{i, j, k\} = \{1, 2, 3\}$, set

$$Y_i := (a_1 X_j + a_2 X_k) \cup (a_1 X_k + a_2 X_j).$$

We assume that the statement is false and we will arrive at a contradiction. Thus

$$|Y| \leq \sum_{i=1}^{3} |X_i|. \tag{40}$$

First we will demonstrate that there are $r \in (\mathbb{Z}/p\mathbb{Z})^*$ and $i \in \{1, 2, 3\}$ such that $X_i \in \mathrm{AP}(r)$. If

$$|Y_1| \leq |X_2| + |X_3|,$$

then Theorem 4.1 yields there are $r, x, y, z, w \in \mathbb{Z}/p\mathbb{Z}$ such that

$$\{X_2, X_3\} = \big\{r[x, y], r[y + z, x - z] \setminus \{w\}\big\}.$$

and our claim is true. Now assume that

$$|Y_1| > |X_2| + |X_3|. \tag{41}$$

Then we have that

$$\begin{aligned}
\sum_{i=1}^{3} |X_i| &\geq |Y| && \Big(\text{by (40)}\Big) \\
&\geq |Y_1 + a_3 X_1| \\
&\geq |Y_1| + |a_3 X_1| - 1 && \Big(\text{by Theorem 2.1}\Big) \\
&\geq \sum_{i=1}^{3} |X_i|. && \Big(\text{by (41)}\Big)
\end{aligned}$$

This yields

$$|Y_1 + a_3 X_1| = |Y_1| + |a_3 X_1| - 1,$$

and Theorem 2.2 implies the existence of $r \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a_3 X_1 \in \mathrm{AP}(a_3 r)$; in other words, $X_1 \in \mathrm{AP}(r)$. In any case our claim is true and we assume, without

loss of generality, that there are $x, y, r \in \mathbb{Z}/p\mathbb{Z}$ such that $X_1 = r[x, y]$. Now we see that

$$\begin{aligned}\sum_{i=1}^{3} |X_i| &\geq |Y| && \Big(\text{by (40)}\Big)\\ &\geq |Y_2 + a_3 X_2| &&\\ &\geq |Y_2| + |X_2| - 1 && \Big(\text{by Theorem 2.1}\Big)\end{aligned}$$

and then

$$|Y_2| \leq |X_1| + |X_3| + 1.$$

This inequality let us apply Lemma 5.1 to the sets a_1X_1 and a_1X_3, and we conclude that there are $z_3, v_3, w_3 \in \mathbb{Z}/p\mathbb{Z}$ such that $a_1X_3 = a_1r[y+z_3, x-z_3]\setminus\{v_3, w_3\}$. In the same way there are $z_2, v_2, w_2 \in \mathbb{Z}/p\mathbb{Z}$ such that $a_1X_2 = a_1r[y+z_2, x-z_2]\setminus\{v_2, w_2\}$. However, since $\min_{1\leq i\leq 3} |X_i| \geq 4$, it is impossible that a_1X_1, a_1X_2 and a_1X_3 are pairwise disjoint. Thus X_1, X_2 and X_3 are not pairwise disjoint and this contradiction concludes the proof. □

Now we show Theorem 1.4 when $n = 3$.

THEOREM 5.1. *Let $a_1, a_2, a_3 \in (\mathbb{Z}/p\mathbb{Z})^*$ be not all equal. Take X_1, X_2, X_3 pairwise disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $\min_{1\leq i\leq 3} |X_i| \geq 4$ and $\sum_{i=1}^{3} |X_i| \leq p-2$. Then*

$$\left|\bigcup_{\sigma\in\mathbb{S}_3} \sum_{i=1}^{3} a_{\sigma(i)}X_i\right| > \sum_{i=1}^{3} |X_i|.$$

PROOF. From Lemma 5.1 we may assume that there are $i, j \in \{1, 2, 3\}$ with the property that $a_i \notin \{\pm a_j\}$; without loss of generality, $a_1 \notin \{\pm a_2\}$. Write

$$Y := \bigcup_{\sigma\in\mathbb{S}_3} \sum_{i=1}^{3} a_{\sigma(i)}X_i,$$

and for any choice $\{i, j, k\} = \{1, 2, 3\}$, set

$$Y_i := (a_1X_j + a_2X_k) \cup (a_1X_k + a_2X_j).$$

We assume that the claim is false and we arrive at a contradiction. Thus we have that

$$|Y| \leq \sum_{i=1}^{3} |X_i|. \tag{42}$$

From Theorem 4.1, since $a_1 \notin \{\pm a_2\}$, we have that

$$|Y_3| > |X_1| + |X_2|. \tag{43}$$

Then we have that

$$\begin{aligned} \sum_{i=1}^{3} |X_i| &\geq |Y| && \Big(\text{by (42)}\Big) \\ &\geq |Y_3 + a_3 X_3| \\ &\geq |Y_3| + |a_3 X_3| - 1 && \Big(\text{by Theorem 2.1}\Big) \\ &\geq \sum_{i=1}^{3} |X_i|. && \Big(\text{by (43)}\Big) \end{aligned} \tag{44}$$

From (44) we deduce that

$$|Y_3 + a_3 X_3| = |Y_3| + |a_3 X_3| - 1,$$

and Theorem 2.2 implies that there is $r_3 \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $Y_3, a_3 X_3 \in \mathrm{AP}(r_3)$. Moreover, since $Y = Y_3 + a_3 X_3$ by (44), we deduce that $Y \in \mathrm{AP}(r_3)$. In the same way we find $r_1, r_2 \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $Y_1, a_3 X_1, Y \in \mathrm{AP}(r_1)$ and $Y_2, a_3 X_2, Y \in \mathrm{AP}(r_2)$. Since $Y \in \mathrm{AP}(r_i)$ for all $i \in \{1, 2, 3\}$, we have that $Y, r_i r_j^{-1} Y \in \mathrm{AP}(r_i)$ for all $i, j \in \{1, 2, 3\}$; this fact implies that $r_i \in \{\pm r_j\}$ for all $i, j \in \{1, 2, 3\}$ from Lemma 3.4. Thus we assume, from now on, that $r_1 = r_2 = r_3$ and we write $r := r_1$. From (44) we obtain that

$$|a_1 X_1 + a_2 X_2| \leq |Y_3| \leq |X_1| + |X_2| + 1. \tag{45}$$

We know that $a_1 X_1 \in \mathrm{AP}(a_3^{-1} a_1 r)$. Then, by (45), we can apply Lemma 2.1 to the sets $a_1 X_1$ and $a_2 X_2$; hence there are $z, w, u, v \in \mathbb{Z}/p\mathbb{Z}$ such that $a_2 X_2 = a_3^{-1} a_1 r[z, w] \setminus \{u, v\}$. In particular $a_2 X_2$ is an arithmetic progression with

difference $a_3^{-1}a_1r$ without at most two elements. Since a_1X_1 is an arithmetic progression with difference $a_3^{-1}a_1r$ and it has at least 4 elements, we get that its sum with a_2X_2 is an arithmetic progression with difference $a_3^{-1}a_1r$; in other words, $a_1X_1 + a_2X_2 \in \mathrm{AP}(a_3^{-1}a_1r)$. In the same way (switching a_1 and a_2 in the previous procedure), we conclude that $a_1X_1 + a_2X_2 \in \mathrm{AP}(a_3^{-1}a_2r)$. Thus $a_1X_1 + a_2X_2, a_1a_2^{-1}(a_1X_1 + a_2X_2) \in \mathrm{AP}(a_3^{-1}a_1r)$; then Lemma 3.4 leads to the inclusion $a_1a_2^{-1} \in \{\pm 1\}$, however this is impossible since $a_1 \notin \{\pm a_2\}$. □

6. Special cases when $n > 3$

In this section we show some special cases of Theorem 1.4 when $n > 3$. Before we start with the proof of one of the main statements of this section, we need an auxiliary lemma.

LEMMA 6.1. *Let $n \in \mathbb{N}_{\geq 4}$ and $a \in \mathbb{Z}/p\mathbb{Z} \setminus \{0, \pm 1\}$. Take $x_1, \dots, x_n, y_1, \dots, y_n \in \mathbb{Z}/p\mathbb{Z}$ such that $\min_{1\leq i\leq n} |[x_i, y_i]| \geq 4$ and $\sum_{i=1}^{n} |[x_i, y_i]| \leq p - 1$. Set*

$$X := \left\{ az_i + \sum_{j=1, j\neq i}^{n} x_i : \ i \in \{1, \dots, n\}, \ z_i \in [x_i, y_i] \right\}.$$

If $x, y \in \mathbb{Z}/p\mathbb{Z}$ are such that $X \subseteq [x, y]$, then

$$|[x, y]| > \max_{1\leq i\leq n} |[x_i, y_i]| + n - 1.$$

PROOF. We assume that the claim is false and we will arrive at a contradiction. Set $W := [x, y]$ and $l := \max_{1\leq i\leq n} |[x_i, y_i]|$. Thus

$$|W| \leq l + n - 1. \tag{46}$$

First we will show that $l \leq n - 1$. We assume that $l > n - 1$ and we will arrive at a contradiction. Suppose, without loss of generality, that $l = |[x_1, y_1]|$. Note that

$$a[x_1, y_1] \subseteq X - \sum_{j=2}^{n} x_j \subseteq W - \sum_{j=2}^{n} x_j. \tag{47}$$

Let $m \in \Gamma$ (where $\Gamma = \{i \in \mathbb{Z} : \ 0 \leq i \leq p-1\}$) be such that $\overline{m} = a^{-1}$, and set $k := \min\{m, p-m\}$. If $Y := \left(W - \sum_{j=2}^{n} x_j\right) \setminus a[x_1, y_1]$, then, applying the first claim of Lemma 3.8, we get that

$$|Y| + 1 \geq \min\{m, p-m, l, p-l\}. \tag{48}$$

Hence

$$\begin{aligned} n - 1 &\geq |W| - l && \Big(\text{by (46)}\Big) \\ &= |Y| && \Big(\text{by (47)}\Big) \\ &\geq \min\{m, p-m, l, p-l\} - 1. && \Big(\text{by (48)}\Big) \end{aligned} \tag{49}$$

The assumptions $\min\limits_{1 \leq i \leq n} |[x_i, y_i]| \geq 4$ and $\sum\limits_{i=1}^{n} |[x_i, y_i]| \leq p-1$ yield

$$l + 4(n-1) \leq p - 1. \tag{50}$$

Since $l > n-1$, we conclude that $k = \min\{m, p-m, l, p-l\}$ by (49) and (50). Thus $l \geq k$ and we may apply the second claim of Lemma 3.8. Then

$$\begin{aligned} l + n - 1 &\geq \left| W - \sum_{j=2}^{n} x_j \right| && \Big(\text{by (46)}\Big) \\ &= \left[\frac{l}{k}\right] + (k-1)\left[\frac{p}{k}\right] && \Big(\text{by Lemma 3.8}\Big) \\ &> \frac{l-k}{k} + (k-1)\left(\frac{p-k}{k}\right), \end{aligned}$$

and therefore

$$l + n\left(\frac{k}{k-1}\right) + k > p. \tag{51}$$

Since $a \notin \{0, \pm 1\}$, $k \geq 2$. Hence

$$\begin{aligned} l + 3n &\geq l + 2n + k && \Big(\text{by (49)}\Big) \\ &\geq l + n\left(\frac{k}{k-1}\right) + k && \Big(\text{since } k \geq 2\Big) \end{aligned}$$

$$\begin{aligned} &> p && \Big(\text{by (51)}\Big) \\ &> l + 4(n-1) && \Big(\text{by (50)}\Big) \end{aligned}$$

and this contradicts $n \geq 4$. This shows $l \leq n-1$.

Define

$$Z := \left\{ ax_i + (a-1)\delta + \sum_{j=1, j\neq i}^{n} x_j : \ i \in \{1, \ldots, n\}, \ \delta \in \{0,1\} \right\}.$$

Let $\delta_i, \delta_k \in \{0,1\}$ be such that

$$ax_i + (a-1)\delta_i + \sum_{j=1, j\neq i}^{n} x_j = ax_k + (a-1)\delta_k + \sum_{j=1, j\neq k}^{n} x_j.$$

Then

$$(a-1)(x_i - x_k + \delta_i - \delta_k) = 0$$

and consequently

$$x_i + \delta_i - \delta_k = x_k. \tag{52}$$

Since as the intervals $[x_1, y_1], \ldots, [x_n, y_n]$ are pairwise disjoint and each has at least 4 elements, we conclude from (52) that $x_i = x_k$ and then $|Z| = 2n$. Since W is an interval and $ax_i + a\delta + \sum_{j=1, j\neq i}^{n} x_j \in W$ for all $i \in \{1, \ldots, n\}$ and $\delta \in \{0,1\}$, we have that $ax_i + (a-1)\delta + \sum_{j=1, j\neq i}^{n} x_j \in W$ for all $i \in \{1, \ldots, n\}$ and $\delta \in \{0,1\}$ except at most for one element. In other words,

$$|Z \cap W| \geq 2n - 1. \tag{53}$$

Thus

$$\begin{aligned} 2n - 1 &\leq |Z \cap W| && \Big(\text{by (53)}\Big) \\ &\leq |W| \\ &\leq l + n - 1 && \Big(\text{by (46)}\Big) \end{aligned}$$

$$\leq 2n-2, \qquad \Big(\text{since } l \leq n-1\Big)$$

and this contradiction concludes the proof. □

We show the first important result of this section.

THEOREM 6.1. *Let $n \in \mathbb{N}_{\geq 3}$ and $a_1, \ldots, a_n \in (\mathbb{Z}/p\mathbb{Z})^*$ be not all equal. Take $X_1, \ldots, X_n$ pairwise disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $\min\limits_{1\leq i\leq n} |X_i| \geq 4$ and $\sum\limits_{i=1}^{n} |X_i| \leq$ $\leq p-2$. Assume that there is $l \in \{1, \ldots, n\}$ such that*

$$a_1 = a_2 = \ldots = a_{l-1} = a_{l+1} = \ldots = a_{n-1} = a_n.$$

Then

$$\left| \bigcup_{\sigma\in\mathbb{S}_n} \sum_{j=1}^{n} a_{\sigma(j)} X_j \right| > \sum_{j=1}^{n} |X_j|.$$

PROOF. We demonstrate this claim by induction on n. If $n = 3$, the claim is a particular case of Theorem 5.1. From now on, we assume that $n \geq 4$ and that the claim is true for all $3 \leq m \leq n-1$. Without loss of generality, we assume that $l = 1$ (in other words, $a_2 = \ldots = a_n$), and we write $a := a_1 a_2^{-1}$. Define $Y_i := a_2 X_i$ for all $i \in \{1, \ldots, n\}$. Set

$$Z := \bigcup_{i=1}^{n} \left(aY_i + \sum_{j=1, j\neq i}^{n} Y_j \right) = \bigcup_{\sigma\in\mathbb{S}_n} \sum_{i=1}^{n} a_{\sigma(i)} X_i,$$

and for all $k \in \{1, \ldots, n\}$

$$Z_k := \bigcup_{i=1, i\neq k}^{n} \left(aY_i + \sum_{j=1, j\notin\{i,k\}}^{n} Y_j \right).$$

We complete the proof by induction assuming that the claim is false for n and arriving at a contradiction. Thus

$$\sum_{i=1}^{n} |X_i| \geq |Z|. \tag{54}$$

We have that for all $k \in \{1, \dots, n\}$

$$\begin{aligned}\sum_{i=1}^{n} |Y_i| &= \sum_{i=1}^{n} |X_i| \\ &\geq |Z| && \Big(\text{by (54)}\Big) \\ &\geq |Z_k + Y_k| \\ &\geq |Z_k| + |Y_k| - 1 && \Big(\text{by Theorem 2.1}\Big) \\ &\geq \sum_{i=1}^{n} |Y_i|. && \Big(\text{by induction}\Big) \end{aligned} \tag{55}$$

From (55) we have that $|Z_k + Y_k| = |Z_k| + |Y_k| - 1$. Then, by Theorem 2.2, there is $r_k \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $Y_k, Z_k \in \mathrm{AP}(r_k)$. Moreover, since $Z_k + Y_k \subseteq Z$, we have from (55) that $Z = Y_k + Z_k$; in particular, $Z \in \mathrm{AP}(r_k)$ for all $k \in \{1, \dots, n\}$. This means that $Z, r_k r_1^{-1} Z \in \mathrm{AP}(r_k)$ for all $k \in \{1, \dots, n\}$ and, applying Lemma 3.4, we deduce that $r_k r_1^{-1} \in \{\pm 1\}$. Thus, without loss of generality, we assume that $r_k = 1$ for all $k \in \{1, \dots, n\}$. For each $k \in \{1, \dots, n\}$, let $x_k, y_k \in \mathbb{Z}/p\mathbb{Z}$ be such that $Y_k = [x_k, y_k]$. We have to study two cases:

- Assume that $a = -1$. For each $i \in \{1, \dots, n\}$, define $w_i := -y_i + \sum_{k=1, k\neq i}^{n} x_k$ and $W := \{w_i : \ i \in \{1, \dots, n\}\}$. Let $i, j \in \{1, \dots, n\}$ and $\delta \in [-1, 1]$ be such that $w_i = w_j + \delta$. Since $Y_1, \dots, Y_n$ are pairwise disjoint and they have at least 4 elements, for all $k \in \{1, \dots, n\} \setminus \{i, j\}$ and $\delta' \in [-2, 2]$, we have that $w_i \neq w_k + \delta'$. This means that for all $i, j, k \in \{1, \dots, n\}$ pairwise distinct, if $u, v \in \mathbb{Z}/p\mathbb{Z}$ are such that $\{w_i, w_j, w_k\} \subseteq [u, v]$, then $|[u, v]| > 3$. Let $x, y \in \mathbb{Z}/p\mathbb{Z}$ be such that $W \subseteq [x, y]$. The previous argument and the Pigeonhole Principle yield

$$|[x, y]| \geq 4\left[\frac{n}{3}\right] + \left(n - 3\left[\frac{n}{3}\right]\right). \tag{56}$$

  Furthermore, since $n \geq 4$, we conclude from (56) that

$$|[x, y]| > n. \tag{57}$$

Recall that Y_k is an interval for all $k \in \{1, \ldots, n\}$; then, for all $i \in \{1, \ldots, n\}$, we get that

$$\left| -Y_i + \sum_{j=1, j\neq i}^{n} Y_j \right| = \left| \left[-y_i + \sum_{k=1, k\neq i}^{n} x_k, -x_i + \sum_{k=1, k\neq i}^{n} y_k \right] \right|$$
$$= \left(\sum_{j=1}^{n} |Y_j| \right) - (n-1). \tag{58}$$

We have that the set $-Y_i + \sum_{j=1, j\neq i}^{n} Y_j$ is an interval for each $i \in \{1, \ldots, n\}$ and we have bounded its cardinality in (58). On the other hand, from (57), we know how spread are the first elements of these intervals. Then

$$|Z| \geq 1 + \sum_{j=1}^{n} |Y_j|.$$

contradicting (54).

- Assume that $a \neq -1$ so $a \notin \{\pm 1, 0\}$. Set

$$W := \left\{ az + \sum_{k=1, k\neq i}^{n} x_k : \ i \in \{1, \ldots, n\}, \ z \in Y_i \right\}.$$

From Lemma 6.1, since $a \notin \{\pm 1, 0\}$, we know that if $x, y \in \mathbb{Z}/p\mathbb{Z}$ are such that $W \subseteq [x, y]$, then

$$|[x, y]| > \max_{1 \leq i \leq n} |Y_i| + n - 1. \tag{59}$$

For each $i \in \{1, \ldots, n\}$ and $z \in Y_i$, set

$$W_z := az + \sum_{k=1, k\neq i}^{n} Y_k.$$

Since Y_k is an interval for all $k \in \{1, \ldots, n\}$, we have that

$$|W_z| = \left| az + \sum_{k=1, k\neq i}^{n} Y_k \right| = \left(\sum_{k=1, k\neq i}^{n} |Y_k| \right) - (n-2). \tag{60}$$

Assume, without loss of generality, that $|Y_1| = \max_{1\le i\le n} |Y_i|$. We have that the set W_z is an interval for all $z \in Y_1$, and we have bounded its cardinality in (60). On the other hand, from (59), we know how spread are the first elements of these intervals. Then (59) and (60) yield

$$\begin{aligned} |Z| &\ge \left| \bigcup_{z\in Y_1} W_z \right| \\ &= 1 + \sum_{j=1}^{n} |Y_j| \end{aligned}$$

contradicting (54). □

In the proof of Theorem 1.4 we need to deal with some special cases that cannot be solved with the previous results. That is why we need the following lemma.

LEMMA 6.2. *Let $a_1, \dots, a_4 \in (\mathbb{Z}/p\mathbb{Z})^*$ be not all equal, and assume that there are $i, j \in \{1, \dots, 4\}$ such that $a_i = -a_j$. Take $X_1, \dots, X_4$ pairwise disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $\min_{1\le i\le 4} |X_i| \ge 4$ and $\sum_{i=1}^{4} |X_i| \le p - 2$. Then*

$$\left| \bigcup_{\sigma\in\mathbb{S}_4} \sum_{i=1}^{4} a_{\sigma(i)} X_i \right| > \sum_{i=1}^{4} |X_i|.$$

PROOF. Assume, without loss of generality, that $a_1 = -a_2$. Set

$$\begin{aligned} Y &:= \bigcup_{\sigma\in\mathbb{S}_4} \sum_{i=1}^{4} a_{\sigma(i)} X_i, \\ Y_4 &:= \bigcup_{\sigma\in\mathbb{S}_3} \sum_{i=1}^{3} a_{\sigma(i)} X_i, \\ Z &:= \bigcup_{\sigma\in\mathbb{S}_2} \sum_{i=1}^{2} a_{\sigma(i)} X_i. \end{aligned}$$

We assume that the claim is false and we will arrive at a contradiction. Thus

$$|Y| \le \sum_{i=1}^{4} |X_i|. \tag{61}$$

Then

$$\begin{aligned}\sum_{i=1}^{4}|X_i| &\geq |Y| && \Big(\text{by (61)}\Big)\\ &\geq |Y_4 + a_4X_4|\\ &\geq |Y_4| + |a_4X_4| - 1 && \Big(\text{by Theorem 2.1}\Big)\\ &\geq \sum_{i=1}^{4}|X_i|. && \Big(\text{by Theorem 5.1}\Big) \qquad (62)\end{aligned}$$

From (62) we have that

$$|Y_4 + a_4X_4| = |Y_4| + |a_4X_4| - 1,$$

and Theorem 2.2 implies the existence of $r_4 \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $Y_4, a_4X_4 \in \mathrm{AP}(r_4)$. Furthermore, since $Y_4 + a_4X_4 \subseteq Y$, (62) lets us deduce that $Y_4 + a_4X_4 = Y$, and then $Y \in \mathrm{AP}(r_4)$. In the same way, for each $i \in \{1, 2, 3\}$, one may prove the existence of $r_i \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $Y, a_4X_i \in \mathrm{AP}(r_i)$. This means that $Y, r_ir_4^{-1}Y \in \mathrm{AP}(r_i)$ for all $i \in \{1, \ldots, 4\}$ and, applying Lemma 3.4, we deduce that $r_ir_4^{-1} \in \{\pm 1\}$. Thus, without loss of generality, we assume that $r_i = a_4$ for all $i \in \{1, \ldots, 4\}$. Let $x_i, y_i \in \mathbb{Z}/p\mathbb{Z}$ be such that $X_i = [x_i, y_i]$ for each $i \in \{1, \ldots, 4\}$. Observe that

$$\begin{aligned}1 + \sum_{i=1}^{3}|X_i| &= |Y_4| && \Big(\text{by (62)}\Big)\\ &\geq \Big|Z + a_3X_3\Big|\\ &\geq |Z| + |a_3X_3| - 1 && \Big(\text{by Theorem 2.1}\Big)\end{aligned}$$

and we get that

$$|Z| \leq |X_1| + |X_2| + 2. \qquad (63)$$

Since $a_1 = -a_2$, from (63), we obtain that

$$x_1 - y_2 \in \big\{x_2 - y_1 + i : \ i \in \{\pm 3, \pm 2, \pm 1, 0\}\big\}. \qquad (64)$$

From (64) we obtain the existence of $z_2, w_2 \in \mathbb{Z}/p\mathbb{Z}$ such that $z_2 \in [w_2-3, w_2+3]$ and $X_2 = [y_1+z_2, x_1-w_2]$. In the same way, for $i \in \{3,4\}$, there are $z_i, w_i \in \mathbb{Z}/p\mathbb{Z}$ such that $z_i \in [w_i-3, w_i+3]$ and $X_i = [y_1+z_i, x_1-w_i]$. Thus the sets $X_1, \dots, X_4$ are not pairwise disjoint since they have at least 4 elements; this contradiction concludes the proof. □

LEMMA 6.3. *Let $a_1, \dots, a_5 \in (\mathbb{Z}/p\mathbb{Z})^*$ be not all equal, and assume that there are $i, j \in \{1, \dots, 5\}$ such that $a_i = -a_j$. Take $X_1, \dots, X_5$ pairwise disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $\min_{1\le i\le 5} |X_i| \ge 5$ and $\sum_{i=1}^{5} |X_i| \le p-2$. Then*

$$\left| \bigcup_{\sigma\in\mathbb{S}_5} \sum_{i=1}^{5} a_{\sigma(i)} X_i \right| > \sum_{i=1}^{5} |X_i|.$$

PROOF. Assume, without loss of generality, that $a_1 = -a_2$. Set

$$Y := \bigcup_{\sigma\in\mathbb{S}_5} \sum_{i=1}^{5} a_{\sigma(i)} X_i,$$
$$Y_5 := \bigcup_{\sigma\in\mathbb{S}_4} \sum_{i=1}^{4} a_{\sigma(i)} X_i.$$

We assume that the claim is false and we will arrive at a contradiction. Thus

$$|Y| \le \sum_{i=1}^{5} |X_i|. \tag{65}$$

Then

$$\begin{aligned}
\sum_{i=1}^{5} |X_i| &\ge |Y| && \big(\text{by (65)}\big)\\
&\ge |Y_5 + a_5 X_5| &&\\
&\ge |Y_5| + |a_5 X_5| - 1 && \big(\text{by Theorem 2.1}\big)\\
&\ge \sum_{i=1}^{5} |X_i|. && \big(\text{by Lemma 6.2}\big)
\end{aligned}$$

From here on the proof is completed proceeding, *mutatis mutandis*, in the same way as is done in Lemma 6.2 after (62). □

7. Proof of Theorem 1.4

For $n \in \mathbb{N}$, let $\mathbf{a} := (a_1, \ldots, a_n)$ be an element of $\overbrace{(\mathbb{Z}/p\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p\mathbb{Z})^*}^{n-times}$ and $\mathcal{F}$ be a family of n pairwise disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$. We say that $(\mathcal{F}, \mathbf{a}, n)$ is *generic* if the following assertions are true:

i) $n \geq 2$.

ii) Not all the entries of $\mathbf{a}$ are equal.

iii) If $\mathbf{a} = (a_1, a_2)$, then $a_1 \neq -a_2$.

Before we conclude the proof of Theorem 1.4, we prove the following useful lemma.

LEMMA 7.1. *Let $n, m \in \mathbb{N}$ and $a_1, \ldots, a_n \in (\mathbb{Z}/p\mathbb{Z})^*$ be not all equal. Take $X_1, \ldots, X_n$ pairwise disjoint subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $\min_{1 \leq i \leq n} |X_i| \geq 4$ and $\sum_{i=1}^{n} |X_i| \leq$ $\leq p - 2$. Set*

$$\mathbf{a}_1 := (a_1, \ldots, a_m), \qquad \mathcal{F}_1 := \{X_1, \ldots, X_m\},$$
$$\mathbf{a}_2 := (a_{m+1}, \ldots, a_n), \qquad \mathcal{F}_2 := \{X_{m+1}, \ldots, X_n\}.$$

Assume that Theorem 1.4 *is true for all $k \in \mathbb{N}_{\geq 2}$ such that $k < n$. If $(\mathcal{F}_1, \mathbf{a}_1, m)$ and $(\mathcal{F}_2, \mathbf{a}_2, n - m)$ are generic, then*

$$\left| \bigcup_{\sigma \in \mathbb{S}_n} \sum_{i=1}^{n} a_{\sigma(i)} X_i \right| > \sum_{i=1}^{n} |X_i|.$$

PROOF. Set

$$Y_1 := \bigcup_{\sigma \in \mathbb{S}_m} \sum_{i=1}^{m} a_{\sigma(i)} X_i \qquad \text{and} \qquad Y_2 := \bigcup_{\sigma \in \mathbb{S}_{n-m}} \sum_{i=1}^{n-m} a_{m+\sigma(i)} X_{m+i}.$$

The elements $a_1, \ldots, a_m \in (\mathbb{Z}/p\mathbb{Z})^*$ are not all equal and the subsets $X_1, \ldots, X_m$ of $\mathbb{Z}/p\mathbb{Z}$ are pairwise disjoint. We have that $2 \leq m \leq n - 2$; moreover, if we

have $m = 2$, the sum of the entries of $\mathbf{a}_1$ is not zero. Since Theorem 1.4 is true for m, we conclude that

$$|Y_1| > \sum_{i=1}^{m} |X_i|. \tag{66}$$

In the same way we deduce that

$$|Y_2| > \sum_{i=m+1}^{n} |X_i|. \tag{67}$$

We conclude the proof as follows

$$\begin{aligned} \left| \bigcup_{\sigma\in\mathbb{S}_n} \sum_{i=1}^{n} a_{\sigma(i)} X_i \right| &\geq |Y_1 + Y_2| \\ &\geq |Y_1| + |Y_2| - 1 \qquad \Big(\text{by Theorem 2.1}\Big) \\ &> \sum_{i=1}^{n} |X_i|. \qquad \Big(\text{by (66) and (67)}\Big) \end{aligned}$$

□

Now we are ready to complete the proof of Theorem 1.4.

PROOF. (*Theorem* 1.4) The first part of the theorem is already demonstrated in Theorem 4.1. It suffices to show the second claim and this is done by induction over n. The claim is true for $n = 3$ from Theorem 5.1. Thus, from now on, we may assume that $n \geq 4$ and the statement is true for all $2 \leq m \leq n - 1$. Furthermore, since not all the $a_1, \ldots, a_n$ are equal, we assume that $a_1 \neq a_2$ without loss of generality. First we demonstrate the claim when $n = 4$. From Lemma 6.2 we may assume that $a_i \neq -a_j$ for all $i, j \in \{1, \ldots, 4\}$. We deal with two cases.

- Suppose that $a_3 = a_4$. From Theorem 6.1 we may assume that $a_3 \notin \{a_1, a_2\}$. Set

$$\begin{aligned} \mathbf{a}_1 &:= (a_1, a_3), \qquad \mathcal{F}_1 := \{X_1, X_2\}, \\ \mathbf{a}_2 &:= (a_2, a_4), \qquad \mathcal{F}_2 := \{X_3, X_4\}. \end{aligned}$$

  Then $(\mathcal{F}_1, \mathbf{a}_1, 2)$ and $(\mathcal{F}_2, \mathbf{a}_2, 2)$ are generic, and Lemma 7.1 concludes the proof of the claim.

- Suppose that $a_3 \neq a_4$. Set

$$\mathbf{a}_1 := (a_1, a_2), \qquad \mathcal{F}_1 := \{X_1, X_2\},$$
$$\mathbf{a}_2 := (a_3, a_4), \qquad \mathcal{F}_2 := \{X_3, X_4\}.$$

Then $(\mathcal{F}_1, \mathbf{a}_1, 2)$ and $(\mathcal{F}_2, \mathbf{a}_2, 2)$ are generic, and Lemma 7.1 finishes the proof.

Now we demonstrate the claim when $n = 5$. From Lemma 6.3 we may assume that $a_i \neq -a_j$ for all $i, j \in \{1, \ldots, 5\}$. We deal with two cases.

- Suppose that $a_3 = a_4 = a_5$. From Theorem 6.1 we may assume that $a_3 \notin \{a_1, a_2\}$. Set

$$\mathbf{a}_1 := (a_1, a_3), \qquad \mathcal{F}_1 := \{X_1, X_2\},$$
$$\mathbf{a}_2 := (a_2, a_4, a_5), \qquad \mathcal{F}_2 := \{X_3, X_4, X_5\}.$$

Then $(\mathcal{F}_1, \mathbf{a}_1, 2)$ and $(\mathcal{F}_2, \mathbf{a}_2, 3)$ are generic, and Lemma 7.1 concludes the proof of the claim.

- Suppose that a_3, a_4, a_5 are not all equal. Set

$$\mathbf{a}_1 := (a_1, a_2), \qquad \mathcal{F}_1 := \{X_1, X_2\},$$
$$\mathbf{a}_2 := (a_3, a_4, a_5), \qquad \mathcal{F}_2 := \{X_3, X_4, X_5\}.$$

Then $(\mathcal{F}_1, \mathbf{a}_1, 2)$ and $(\mathcal{F}_2, \mathbf{a}_2, 3)$ are generic, and the claim is true by Lemma 7.1.

Finally we show the claim when $n \geq 6$. We have to deal with two cases.

- Suppose that $a_3 = \ldots = a_n$. From Theorem 6.1 we may assume that $a_3 \notin \{a_1, a_2\}$. Set

$$\mathbf{a}_1 := (a_1, a_3, a_4), \qquad \mathcal{F}_1 := \{X_1, X_2, X_3\},$$
$$\mathbf{a}_2 := (a_2, a_5, \ldots, a_n), \qquad \mathcal{F}_2 := \{X_4, \ldots, X_n\}.$$

Then $(\mathcal{F}_1, \mathbf{a}_1, 3)$ and $(\mathcal{F}_2, \mathbf{a}_2, n-3)$ are generic, and Lemma 7.1 lets us conclude the proof of the claim.

- Suppose that $a_3, \ldots, a_n$ are not all equal. Assume, without loss of generality, that $a_4 \neq a_5$. If

$$\mathbf{a}_1 := (a_1, a_2, a_3), \qquad \mathcal{F}_1 := \{X_1, X_2, X_3\},$$

$$\mathbf{a}_2 := (a_4, \dots, a_n), \qquad \mathcal{F}_2 := \{X_4, \dots, X_n\}.$$

Then $(\mathcal{F}_1, \mathbf{a}_1, 3)$ and $(\mathcal{F}_2, \mathbf{a}_2, n-3)$ are generic, and in this case we conclude using Lemma 7.1. □

8. Proof of Theorem 1.5

In this section we conclude the proof of Theorem 1.5.

PROOF. (*Theorem* 1.5) We assume that $n \geq 4$ by [7, Thm. 6]. Set

$$Y := \bigcup_{\sigma \in \mathbb{S}_n} \sum_{i=1}^{n} a_{\sigma(i)} X_i \qquad \text{and} \qquad Y_n := \bigcup_{\sigma \in \mathbb{S}_{n-1}} \sum_{i=1}^{n-1} a_{\sigma(i)} X_i.$$

From Theorem 1.4

$$|Y_n| > \sum_{i=1}^{n-1} |X_i|. \tag{68}$$

We claim that $Y = \mathbb{Z}/p\mathbb{Z}$. If this is not true, we have that $|Y| \leq p-1$ and therefore

$$\begin{aligned} p-1 &\geq |Y| \\ &\geq |Y_n + a_n X_n| \\ &\geq |Y_n| + |a_n X_n| - 1 && \Big(\text{by Theorem 2.1}\Big) \\ &> \left(\sum_{i=1}^{n} |X_i| \right) - 1 && \Big(\text{by (68)}\Big) \\ &= p-1, \end{aligned}$$

and this contradiction yields $Y = \mathbb{Z}/p\mathbb{Z}$. Then we have that $b \in Y$, and therefore there is a rainbow subset $\{z_1, \dots, z_n\}$ of $\mathbb{Z}/p\mathbb{Z} = \bigcup_{i=1}^{n} X_i$ such that $\sum_{i=1}^{n} a_i z_i = b$. □

Acknowledgements

I thank Amanda Montejano, Edgardo Roldán and Adriana Hansberg for their comments and advice about the content of this paper. Also I thank the referee for the useful suggestions to improve this paper.

Bibliography

1. ***B. Bukh***, *Sums of Dilates*, Combin. Probab. Comput. **17** (2008), 627–639.
2. ***A. Cauchy***, *Recherches sur les nombres*, J. Ecole Polytech. **9** (1813), 99–116.
3. ***D. Conlon***, *Rainbow solutions of linear equations over* $\mathbb{Z}_p$, Discrete Math. **306** (2006), 2056–2063.
4. ***H. Davenport***, *On the addition of residue classes*, J. London Math. Soc. **10** (1935), 30–32.
5. ***H. Davenport***, *A historical note*, J. London Math. Soc. **22** (1947), 100–101.
6. ***Y. Hamidoune, Ø. Rødseth***, *An inverse theorem mod p*, Acta Arith. **92** (2000), 251–262.
7. ***M. Huicochea, A. Montejano***, *The structure of rainbow-free colorings for linear equations on three variables in* $\mathbb{Z}_p$, Integers 15A (2015), A8.
8. ***V. Jungić, J. Licht, M. Mahdian, J. Nešetřil, R. Radoičić***, *Rainbow Ramsey Theory and Anti-Ramsey results*, Combin. Probab. Comput. **12** (2005), 599–620.
9. ***A. Plagne***, *Sums of Dilates in Groups of Prime Order*, Combin. Probab. Comput. **20** (2011), 867–873.
10. ***G. Pontiveros***, *Sums of dilates in* $\mathbb{Z}_p$, Combin. Probab. Comput. **22** (2013), 282–293.
11. ***G. Vosper***, *The critical pairs of subsets of a group of prime order*, J. London Math. Soc. **31** (1956), 200–205.

Mario Huicochea

Facultad de Ciencias,
Universidad Nacional
Autonoma de Mexico,
Circuito Exterior,
Cd. Universitaria,
04510 Ciudad de Mexico,
Mexico
dym@cimat.mx