**Notes on Number Theory and Discrete Mathematics**
**Print ISSN 1310–5132, Online ISSN 2367–8275**
**Vol. 24, 2018, No. 1, 61–75**
**DOI: 10.7546/nntdm.2018.24.1.61-75**

# Almost arithmetic progressions in $\mathbb{Z}/p\mathbb{Z}$

**Mario Huicochea**

Facultad de Ciencias, UNAM-Juriquilla
Querétaro, México
e-mail: dym@cimat.mx

**Received:** 29 June 2016 **Accepted:** 31 October 2017

**Abstract:** For $k \in \mathbb{N} \cup \{0\}$ and $r \in \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$, we say that a subset $X$ of $\mathbb{Z}/p\mathbb{Z}$ is a $k-$almost arithmetic progression with difference $r$ if there is an arithmetic progression $Y$ with difference $r$ containing $X$ such that $|Y \setminus X| \leq k$. Let $X$ be a $k-$almost arithmetic progression with difference $r$ such that $k+2 < |X| < p-4k-9$. The main result of this paper is following: if there is $t \in \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$ such that $X$ is also a $k-$almost arithmetic progression with difference $t$, then $t \in \{\pm r\}$. Moreover, we will show that our result is sharp.
**Keywords:** Arithmetic progressions, Almost arithmetic progressions.
**2010 Mathematics Subject Classification:** Primary 11B13; Secondary 11A07.

## 1 Introduction

In this paper, $p$ is a prime number. We denote by $\mathbb{Z}/p\mathbb{Z}$ the set of congruence classes modulo $p$ with its usual field structure, and we write $(\mathbb{Z}/p\mathbb{Z})^* := \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$. For all $m \in \mathbb{Z}$, we denote by $\overline{m}$ its projection in $\mathbb{Z}/p\mathbb{Z}$. For any $X$ and $Y$ subsets of $\mathbb{Z}/p\mathbb{Z}$ and $r \in (\mathbb{Z}/p\mathbb{Z})^*$, set

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

Given $r \in (\mathbb{Z}/p\mathbb{Z})^*$, we say that $Y$ is an *arithmetic progression with difference* $r$ if there is $y \in \mathbb{Z}/p\mathbb{Z}$ such that $Y = \{y + \bar{i}r:\ 0 \leq i \leq |Y|-1\}$. For $k \in \mathbb{N} \cup \{0\}$, we say that a subset $X$ of $\mathbb{Z}/p\mathbb{Z}$ is a *$k-$almost arithmetic progression with difference* $r$ if there is an arithmetic progression $Y$ with difference $r$ such that $X \subseteq Y$ and $|Y \setminus X| \leq k$. The family of $k-$almost arithmetic progressions with difference $r$ will be denoted by $\mathrm{AAP}(r,k)$.

In additive number theory, it has been shown that the study of $k$-almost arithmetic progressions is very important. For instance, some of the most important inverse theorems in $\mathbb{Z}/p\mathbb{Z}$ can

be stated in terms of $k$-almost arithmetic progressions, see [5],[1],[2]. Also the study of $k-$almost arithmetic progressions has applications in anti-Ramsey theory, see [3]. The purpose of this paper is to continue with the study of $k$-almost arithmetic progressions. Specifically, given a subset $X$ of $\mathbb{Z}/p\mathbb{Z}$, we are interested in determine how many $s \in (\mathbb{Z}/p\mathbb{Z})^*$ can be found such that $X$ is a $k-$almost arithmetic progression with difference $s$. The main result of this paper is the following.

**Theorem 1.1.** *Let $r, t \in (\mathbb{Z}/p\mathbb{Z})^*$ and $k \in \mathbb{N} \cup \{0\}$. Let $X$ be a subset of $\mathbb{Z}/p\mathbb{Z}$ such that $X \in \mathrm{AAP}(r,k) \cap \mathrm{AAP}(t,k)$. If*

$$k + 2 < |X| < p - 4k - 9,$$

*then $t \in \{\pm r\}$.*

This paper is organized as follows. In Section 2 we define the $m-$almost equidistributed subsets and we start studying them. In Section 3 we state and prove a property of the $m-$almost equidistributed subsets that is used in the proof of Theorem 1.1. In Section 4 we give two families of almost equidistributed subsets; these families are the ones used in proof of Theorem 1.1, and the theory developed in the previous sections will be used in these two cases. In Section 5 we complete the proof of Theorem 1.1; furthermore, at the end of this section, we present some examples which show that Theorem 1.1 is sharp.

To avoid confusion, we remark that in this paper the symbols $\ldots, -1, 0, 1, 2, \ldots$ will be elements of $\mathbb{Z}$ while $\ldots, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \ldots$ are their respective projections into $\mathbb{Z}/p\mathbb{Z}$. For all $s \in (\mathbb{Z}/p\mathbb{Z})^*$, $s^{-1}$ is its multiplicative inverse.

# 2 Almost equidistribution

In this section we define the almost equidistributed subsets, and we study some of their properties that will be used in the forthcoming sections. Recall that $\overline{m}$ is the projection of $m \in \mathbb{Z}$ into $\mathbb{Z}/p\mathbb{Z}$. Define $\Gamma := \{m \in \mathbb{Z} : \ 0 \leq m \leq p-1\}$; thus there is one and only one representative of each class of $\mathbb{Z}/p\mathbb{Z}$ in $\Gamma$. For any $x, y \in \mathbb{Z}/p\mathbb{Z}$, let $m \in \Gamma$ be such that $\overline{m} = y - x$ and set

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

which is called an *interval*. Hence, for all $r \in (\mathbb{Z}/p\mathbb{Z})^*$ and $X$ an nonempty subset of $\mathbb{Z}/p\mathbb{Z}$, $X$ is an arithmetic progression with common difference $r$ if and only if there are $x, y \in \mathbb{Z}/p\mathbb{Z}$ such that $r[x, y] = X$. For any $a \in \mathbb{R}$, we denote by $[a]$ the greatest integer less than or equal to $a$.

Let $m \in \Gamma \setminus \{0\}$ and $x \in \mathbb{Z}/p\mathbb{Z}$. We write

$$\mathrm{I}_m(x) := \left[x, x + \overline{m-1}\right].$$

We say that a subset $Y$ of $\mathbb{Z}/p\mathbb{Z}$ is $m-$*almost equidistributed* if it satisfies the following property: for any $x, y \in \mathbb{Z}/p\mathbb{Z}$ such that $\mathrm{I}_m(x)$ and $\mathrm{I}_m(y)$ are disjoint, we have that

$$\Big|\big|\mathrm{I}_m(x) \cap Y\big| - \big|\mathrm{I}_m(y) \cap Y\big|\Big| \leq 1.$$

Notice that if $Y$ is $m-$almost equidistributed, then $\mathbb{Z}/p\mathbb{Z} \setminus Y$ is also $m-$almost equidistributed. Whenever $Y$ is an $m-$almost equidistributed subset of $\mathbb{Z}/p\mathbb{Z}$, we define

$$\operatorname{ind}_m(Y) := \max_{0 \leq i \leq [\frac{p}{m}]-1} \left| \mathrm{I}_m\big(\overline{im}\big) \cap Y \right|.$$

Until the end this section, we fix $m \in \Gamma \setminus \{0\}$, and we write $\mathrm{I}(x) := \mathrm{I}_m(x)$ for each $x \in \mathbb{Z}/p\mathbb{Z}$ and $\operatorname{ind}(Y) := \operatorname{ind}_m(Y)$. The subsets $\mathrm{I}\big(\overline{0}\big), \mathrm{I}\big(\overline{m}\big), \mathrm{I}\big(\overline{2m}\big), \ldots, \mathrm{I}\Big(\overline{([\frac{p}{m}]-1)m}\Big)$ are pairwise disjoint; thus, for all $0 \leq i \leq [\frac{p}{m}] - 1$, we have that

$$\operatorname{ind}(Y) - 1 \leq \left| \mathrm{I}\big(\overline{im}\big) \cap Y \right| \leq \operatorname{ind}(Y). \tag{1}$$

We need four technical lemmas that will be used in the forthcoming results.

**Lemma 2.1.** *Let $Z$ and $W$ be subsets of $\mathbb{Z}/p\mathbb{Z}$, $k \in \mathbb{N} \cup \{0\}$, $n \in \Gamma$ and $Y$ be an $m-$almost equidistributed subset of $\mathbb{Z}/p\mathbb{Z}$. Assume that $\big[\overline{0}, \overline{n}\big] \setminus Z = Y \setminus W$ and $|Y \setminus W| > k + 2$. Define*

$$\alpha_1 := \left| \mathrm{I}\left( \overline{m\left[\frac{n}{m}\right]} \right) \cap \big[\overline{0}, \overline{n}\big] \cap Y \right|,$$

$$\alpha_2 := \left| \left[ \overline{m\left[\frac{p}{m}\right]}, \overline{p-1} \right] \cap \big[\overline{0}, \overline{n}\big] \cap Y \right|.$$

*(i) If $n < m\big[\frac{p}{m}\big]$, then*

$$\alpha_1 + \left[\frac{n}{m}\right] \operatorname{ind}(Y) > k + 2.$$

*(ii) If $n \geq m\big[\frac{p}{m}\big]$, then*

$$\alpha_2 + \left[\frac{n}{m}\right] \operatorname{ind}(Y) > k + 2.$$

*Proof.* Inasmuch as $Y \setminus W \subseteq \big[\overline{0}, \overline{n}\big]$, we conclude that

$$Y \setminus W \subseteq \big[\overline{0}, \overline{n}\big] \cap Y. \tag{2}$$

Since $\Big[\overline{m\big[\frac{p}{m}\big]}, \overline{p-1}\Big] \cup \bigcup_{i=0}^{[\frac{p}{m}]-1} \mathrm{I}(\overline{im})$ is a partition of $\mathbb{Z}/p\mathbb{Z}$, we get from (2) that

$$k + 2 < |Y \setminus W| \leq \alpha_2 + \sum_{i=0}^{[\frac{p}{m}]-1} \left| \mathrm{I}\big(\overline{im}\big) \cap \big[\overline{0}, \overline{n}\big] \cap Y \right|. \tag{3}$$

If $n < m\big[\frac{p}{m}\big]$, then $\left| \Big[\overline{m\big[\frac{p}{m}\big]}, \overline{p-1}\Big] \cap \big[\overline{0}, \overline{n}\big] \right| = \left| \mathrm{I}\big(\overline{im}\big) \cap \big[\overline{0}, \overline{n}\big] \right| = 0$ for all $\big[\frac{n}{m}\big] < i < \big[\frac{p}{m}\big]$, and then (i) is true by (1) and (3). If $n \geq m\big[\frac{p}{m}\big]$, then $\big[\frac{n}{m}\big] = \big[\frac{p}{m}\big]$ and (ii) follows from (1) and (3). □

**Lemma 2.2.** *Let $Z$ and $W$ be subsets of $\mathbb{Z}/p\mathbb{Z}$, $k \in \mathbb{N} \cup \{0\}$, $n \in \Gamma$ and $Y$ be an $m-$almost equidistributed subset of $\mathbb{Z}/p\mathbb{Z}$. Assume that $\big[\overline{0}, \overline{n}\big] \setminus Z = Y \setminus W$ and $|Z| \leq k$. Define*

$$\beta_1 := \left| \mathrm{I}\left( \overline{m\left[\frac{n}{m}\right]} \right) \cap \big[\overline{0}, \overline{n}\big] \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y) \right|,$$

$$\beta_2 := \left| \left[ \overline{m\left[\frac{p}{m}\right]}, \overline{p-1} \right] \cap \big[\overline{0}, \overline{n}\big] \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y) \right|.$$

*(i) If* $n < m\lceil \frac{p}{m} \rceil$, *then* $\beta_1 + \lceil \frac{n}{m} \rceil (m - \mathrm{ind}(Y)) \leq k$.

*(ii) If* $n \geq m\lceil \frac{p}{m} \rceil$, *then* $\beta_2 + \lceil \frac{n}{m} \rceil (m - \mathrm{ind}(Y)) \leq k$.

*Proof.* Since $\lceil \overline{0}, \overline{n} \rceil \setminus Z \subseteq Y$, we have that

$$\lceil \overline{0}, \overline{n} \rceil \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y) \subseteq Z. \tag{4}$$

Insomuch as $\left[\overline{m\lceil \frac{p}{m} \rceil}, \overline{p-1}\right] \cup \bigcup_{i=0}^{\lceil \frac{p}{m} \rceil - 1} \mathrm{I}(\overline{im})$ is a partition of $\mathbb{Z}/p\mathbb{Z}$, we get from (4) that

$$k \geq |Z| \geq \beta_2 + \sum_{i=0}^{\lceil \frac{p}{m} \rceil - 1} \left| \mathrm{I}\big(\overline{im}\big) \cap \lceil \overline{0}, \overline{n} \rceil \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y) \right|. \tag{5}$$

If $n < m\lceil \frac{p}{m} \rceil$, then $\left| \left[\overline{m\lceil \frac{p}{m} \rceil}, \overline{p-1}\right] \cap \lceil \overline{0}, \overline{n} \rceil \right| = \left| \mathrm{I}\big(\overline{im}\big) \cap \lceil \overline{0}, \overline{n} \rceil \right| = 0$ for all $\lceil \frac{n}{m} \rceil < i < \lceil \frac{p}{m} \rceil$, and then (i) is true by (1) and (5). If $n \geq m\lceil \frac{p}{m} \rceil$, then $\lceil \frac{n}{m} \rceil = \lceil \frac{p}{m} \rceil$ and (ii) follows from (1) and (5). □

**Lemma 2.3.** *Let* $Z$ *and* $W$ *be subsets of* $\mathbb{Z}/p\mathbb{Z}$, $k \in \mathbb{N} \cup \{0\}$, $n \in \Gamma$ *and* $Y$ *be an* $m-$*almost equidistributed subset of* $\mathbb{Z}/p\mathbb{Z}$. *Assume that* $\lceil \overline{0}, \overline{n} \rceil \setminus Z = Y \setminus W$ *and* $|W| \leq k$. *Define*

$$\gamma_1 := \left| \mathrm{I}\left(\overline{m\left\lceil \frac{n}{m} \right\rceil}\right) \cap \Big(\mathbb{Z}/p\mathbb{Z} \setminus \lceil \overline{0}, \overline{n} \rceil\Big) \cap Y \right|,$$

$$\gamma_2 := \left| \left[\overline{m\left\lceil \frac{p}{m} \right\rceil}, \overline{p-1}\right] \cap \Big(\mathbb{Z}/p\mathbb{Z} \setminus \lceil \overline{0}, \overline{n} \rceil\Big) \cap Y \right|.$$

*(i) If* $n < m\lceil \frac{p}{m} \rceil$, *then*

$$\gamma_1 + \gamma_2 + \left( \left\lceil \frac{p}{m} \right\rceil - \left\lceil \frac{n}{m} \right\rceil - 1 \right) (\mathrm{ind}(Y) - 1) \leq k.$$

*(ii) If* $n \geq m\lceil \frac{p}{m} \rceil$, *then*

$$\gamma_2 \leq k.$$

*Proof.* Since $Y \setminus W \subseteq \lceil \overline{0}, \overline{n} \rceil$, we get that

$$\Big(\mathbb{Z}/p\mathbb{Z} \setminus \lceil \overline{0}, \overline{n} \rceil\Big) \cap Y \subseteq W. \tag{6}$$

Insomuch as $\left[\overline{m\lceil \frac{p}{m} \rceil}, \overline{p-1}\right] \cup \bigcup_{i=0}^{\lceil \frac{p}{m} \rceil - 1} \mathrm{I}(\overline{im})$ is a partition of $\mathbb{Z}/p\mathbb{Z}$, we get from (6) that

$$\begin{aligned} k &\geq |W| \\ &\geq \gamma_2 + \sum_{i=0}^{\lceil \frac{p}{m} \rceil - 1} \left| \mathrm{I}\big(\overline{im}\big) \cap \Big(\mathbb{Z}/p\mathbb{Z} \setminus \lceil \overline{0}, \overline{n} \rceil\Big) \cap Y \right| \\ &= \gamma_2 + \sum_{i=\lceil \frac{n}{m} \rceil}^{\lceil \frac{p}{m} \rceil - 1} \left| \mathrm{I}\big(\overline{im}\big) \cap \Big(\mathbb{Z}/p\mathbb{Z} \setminus \lceil \overline{0}, \overline{n} \rceil\Big) \cap Y \right|. \end{aligned}$$

Then the statements follow from (1). □

**Lemma 2.4.** *Let $Z$ and $W$ be subsets of $\mathbb{Z}/p\mathbb{Z}$, $k \in \mathbb{N} \cup \{0\}$, $n \in \Gamma$ and $Y$ be an $m-$almost equidistributed subset of $\mathbb{Z}/p\mathbb{Z}$. Assume that $\big[\overline{0}, \overline{n}\big] \setminus Z = Y \setminus W$, $|Y \setminus W| < p - 4k - 9$ and $\max\{|W|, |Z|\} \leq k$. Define*

$$\delta_1 := \left| \mathrm{I}\left(\overline{m\left[\frac{n}{m}\right]}\right) \cap \Big(\mathbb{Z}/p\mathbb{Z} \setminus \big[\overline{0}, \overline{n}\big]\Big) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y) \right|,$$

$$\delta_2 := \left| \left[\overline{m\left[\frac{p}{m}\right]}, \overline{p-1}\right] \cap \Big(\mathbb{Z}/p\mathbb{Z} \setminus \big[\overline{0}, \overline{n}\big]\Big) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y) \right|.$$

*(i) If $n < m\big[\frac{p}{m}\big]$, then*

$$\delta_1 + \delta_2 + \left(\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] - 1\right)(m - \mathrm{ind}(Y) + 1) > 2k + 9.$$

*(ii) If $n \geq m\big[\frac{p}{m}\big]$, then*

$$\delta_2 > 2k + 9.$$

*Proof.* Insomuch as $|Y \setminus W| < p - 4k - 9$ and $|W| \leq k$, we have that

$$p - |Y| \geq p - (|Y \setminus W| + |W|) > 3k + 9. \tag{7}$$

Furthermore, since $Y \setminus W = \big[\overline{0}, \overline{n}\big] \setminus Z$, we have that $\big[\overline{0}, \overline{n}\big] \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y) \subseteq Z$, so

$$\Big|\big[\overline{0}, \overline{n}\big] \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\Big| \leq |Z| \leq k. \tag{8}$$

Since

$$\Big(\mathbb{Z}/p\mathbb{Z} \setminus \big[\overline{0}, \overline{n}\big]\Big) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y) = (\mathbb{Z}/p\mathbb{Z} \setminus Y) \setminus \big[\overline{0}, \overline{n}\big],$$

we get that

$$\Big|\Big(\mathbb{Z}/p\mathbb{Z} \setminus \big[\overline{0}, \overline{n}\big]\Big) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\Big| = p - |Y| - \Big|\big[\overline{0}, \overline{n}\big] \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\Big|. \tag{9}$$

We conclude that

$$\begin{aligned} 2k + 9 <& p - |Y| - \big|\big[\overline{0}, \overline{n}\big] \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\big| && \text{by (7) and (8)} \\ =& \Big|\Big(\mathbb{Z}/p\mathbb{Z} \setminus \big[\overline{0}, \overline{n}\big]\Big) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\Big| && \text{by (9).} \end{aligned} \tag{10}$$

Inasmuch as $\left[\overline{m\big[\frac{p}{m}\big]}, \overline{p-1}\right] \cup \bigcup_{i=0}^{[\frac{p}{m}]-1} \mathrm{I}(\overline{im})$ is a partition of $\mathbb{Z}/p\mathbb{Z}$, we get from (10) that

$$\begin{aligned} 2k + 9 <& \Big|\Big(\mathbb{Z}/p\mathbb{Z} \setminus \big[\overline{0}, \overline{n}\big]\Big) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\Big| \\ \leq& \delta_2 + \sum_{i=0}^{[\frac{p}{m}]-1} \Big|\mathrm{I}(\overline{im}) \cap \Big(\mathbb{Z}/p\mathbb{Z} \setminus \big[\overline{0}, \overline{n}\big]\Big) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\Big| \\ =& \delta_2 + \sum_{i=[\frac{n}{m}]}^{[\frac{p}{m}]-1} \Big|\mathrm{I}(\overline{im}) \cap \Big(\mathbb{Z}/p\mathbb{Z} \setminus \big[\overline{0}, \overline{n}\big]\Big) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\Big|. \end{aligned}$$

Hence the claims follow from (1). □

A consequence of the previous lemmas is the following corollary.

**Corollary 2.5.** *Let $Z$ and $W$ be subsets of $\mathbb{Z}/p\mathbb{Z}$, $k \in \mathbb{N} \cup \{0\}$ , $n \in \Gamma$ and $Y$ be an $m-$almost equidistributed subset of $\mathbb{Z}/p\mathbb{Z}$. Assume:*

- $\left[\frac{p}{m}\right] > 1$.
- $\left[\overline{0}, \overline{n}\right] \setminus Z = Y \setminus W$.
- $k + 2 < |Y \setminus W| < p - 4k - 9$.
- $\max\{|W|, |Z|\} \leq k$.

*Then we have the following inequalities.*

*(i)* $\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] > 0$.

*(ii)* $\left(\left[\frac{n}{m}\right] + 1\right)\mathrm{ind}(Y) > k + 2$.

*(iii)* $\left[\frac{n}{m}\right](m - \mathrm{ind}(Y)) \leq k$.

*(iv)* $\left(\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] - 1\right)(\mathrm{ind}(Y) - 1) \leq k$.

*(v)* $\left(\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] + 1\right)(m - \mathrm{ind}(Y) + 1) > 2k + 8$.

*Proof.* Before we start with the proofs of the claims, recall that $\mathbb{Z}/p\mathbb{Z} \setminus Y$ is $m-$almost equidistributed since $Y$ is an $m-$almost equidistributed subset of $\mathbb{Z}/p\mathbb{Z}$. First we show (i) assuming it is false and arriving at a contradiction. Thus we assume that $\left[\frac{n}{m}\right] = \left[\frac{p}{m}\right]$ and consequently $n \geq m\left[\frac{p}{m}\right]$. Proceeding as in the first part of Lemma 2.4 (until (10)), we obtain that

$$\begin{aligned} 2k + 9 &< \left|\left(\mathbb{Z}/p\mathbb{Z} \setminus \left[\overline{0}, \overline{n}\right]\right) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\right| \\ &= \left|\left[\overline{m\left[\frac{p}{m}\right]}, \overline{p-1}\right] \cap \left(\mathbb{Z}/p\mathbb{Z} \setminus \left[\overline{0}, \overline{n}\right]\right) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\right|, \end{aligned}$$

and therefore

$$\begin{aligned} 2k + 9 &< \left|\left[\overline{m\left[\frac{p}{m}\right]}, \overline{p-1}\right] \cap \left(\mathbb{Z}/p\mathbb{Z} \setminus \left[\overline{0}, \overline{n}\right]\right) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\right| \\ &\leq \left|\mathrm{I}\left(\overline{m\left[\frac{p}{m}\right]}\right) \cap \left(\mathbb{Z}/p\mathbb{Z} \setminus \left[\overline{0}, \overline{n}\right]\right) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\right| \\ &\leq \left|\mathrm{I}\left(\overline{m\left[\frac{p}{m}\right]}\right) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\right| \\ &= \left|\mathrm{I}\left(\overline{m\left[\frac{n}{m}\right]}\right) \cap (\mathbb{Z}/p\mathbb{Z} \setminus Y)\right|. \end{aligned} \tag{11}$$

Now, since $\left[\frac{n}{m}\right] = \left[\frac{p}{m}\right] > 1$, we have that $\mathrm{I}\Big(\overline{m\big(\left[\frac{n}{m}\right]-1\big)}\Big)$ and $\mathrm{I}\Big(\overline{m\left[\frac{n}{m}\right]}\Big)$ are disjoint. Inasmuch as $\mathbb{Z}/p\mathbb{Z}\setminus Y$ is $m-$almost equidistributed, we conclude that

$$\left|\mathrm{I}\left(\overline{m\left[\frac{n}{m}\right]}\right)\cap(\mathbb{Z}/p\mathbb{Z}\setminus Y)\right| \leq \left|\mathrm{I}\left(\overline{m\left(\left[\frac{n}{m}\right]-1\right)}\right)\cap(\mathbb{Z}/p\mathbb{Z}\setminus Y)\right|+1. \tag{12}$$

On the other hand, as a consequence of Lemma 2.2 (ii), we get that

$$\left|\mathrm{I}\left(\overline{m\left(\left[\frac{n}{m}\right]-1\right)}\right)\cap(\mathbb{Z}/p\mathbb{Z}\setminus Y)\right|+1 \leq \left[\frac{n}{m}\right](m-\mathrm{ind}(Y))+1 \leq k+1. \tag{13}$$

From (11), (12) and (13), notice that $2k+9 < k+1$ which is impossible.

To show (ii), we use that $\left[\frac{n}{m}\right] < \left[\frac{p}{m}\right]$ by (i); thus $n < m\left[\frac{p}{m}\right]$. From this fact, we get that

$$\left|\mathrm{I}\left(\overline{m\left[\frac{n}{m}\right]}\right)\cap\left[\overline{0},\overline{n}\right]\cap Y\right| \leq \left|\mathrm{I}\left(\overline{m\left[\frac{n}{m}\right]}\right)\cap Y\right| \leq \mathrm{ind}(Y). \tag{14}$$

Then, from Lemma 2.1 (i) and (14), we have proven (ii).

Since $n < m\left[\frac{p}{m}\right]$ by (i), we get that (iii) is a consequence of Lemma 2.2 (i) (since $\beta_1 \geq 0$).

Also, insomuch as $n < m\left[\frac{p}{m}\right]$ by (i), we have that (iv) is a straight consequence of Lemma 2.3 (i) (since $\gamma_1, \gamma_2 \geq 0$).

We prove (v). From (i), $n < m\left[\frac{p}{m}\right]$. Insomuch as $\mathbb{Z}/p\mathbb{Z}\setminus Y$ is almost equidistributed and $\left[\frac{n}{m}\right] < \left[\frac{p}{m}\right]$, we conclude that

$$\begin{aligned}
&\left|\mathrm{I}\left(\overline{m\left[\frac{n}{m}\right]}\right)\cap\Big(\mathbb{Z}/p\mathbb{Z}\setminus\left[\overline{0},\overline{n}\right]\Big)\cap(\mathbb{Z}/p\mathbb{Z}\setminus Y)\right| \\
\leq&\left|\mathrm{I}\left(\overline{m\left[\frac{n}{m}\right]}\right)\cap(\mathbb{Z}/p\mathbb{Z}\setminus Y)\right| \\
\leq& m-\mathrm{ind}(Y)+1.
\end{aligned} \tag{15}$$

Furthermore, the inequality $\left[\frac{p}{m}\right] > 1$ yields $\mathrm{I}\Big(\overline{m\left[\frac{p}{m}\right]}\Big)$ and $\mathrm{I}\Big(\overline{m\big(\left[\frac{p}{m}\right]-1\big)}\Big)$ are disjoint. Thus, inasmuch as $\mathbb{Z}/p\mathbb{Z}\setminus Y$ is almost equidistributed, we conclude that

$$\begin{aligned}
&\left|\left[\overline{m\left[\frac{p}{m}\right]},\overline{p-1}\right]\cap\Big(\mathbb{Z}/p\mathbb{Z}\setminus\left[\overline{0},\overline{n}\right]\Big)\cap(\mathbb{Z}/p\mathbb{Z}\setminus Y)\right| \\
\leq&\left|\mathrm{I}\left(\overline{m\left[\frac{p}{m}\right]}\right)\cap\Big(\mathbb{Z}/p\mathbb{Z}\setminus\left[\overline{0},\overline{n}\right]\Big)\cap(\mathbb{Z}/p\mathbb{Z}\setminus Y)\right| \\
\leq&\left|\mathrm{I}\left(\overline{m\left[\frac{p}{m}\right]}\right)\cap(\mathbb{Z}/p\mathbb{Z}\setminus Y)\right| \\
\leq&\left|\mathrm{I}\left(\overline{m\left(\left[\frac{p}{m}\right]-1\right)}\right)\cap(\mathbb{Z}/p\mathbb{Z}\setminus Y)\right|+1 \\
\leq& m-\mathrm{ind}(Y)+2.
\end{aligned} \tag{16}$$

As a consequence of Lemma 2.4 (i), (15) and (16), we have shown (v). □

# 3 Main property

In this section we state and prove Lemma 3.2 which is the main property of the almost equidistributed subsets that we need in the proof of Theorem 1.1. Before we present Lemma 3.2, we need a particular case of it.

**Lemma 3.1.** *Let $Z$ and $W$ be subsets of $\mathbb{Z}/p\mathbb{Z}$, $k \in \mathbb{N} \cup \{0\}$ , $n \in \Gamma$, $m \in \Gamma \setminus \{0\}$ and $Y$ be an $m-$almost equidistributed subset of $\mathbb{Z}/p\mathbb{Z}$. Assume:*

- $\left[\frac{p}{m}\right] \geq m$.
- $\left[\overline{0}, \overline{n}\right] \setminus Z = Y \setminus W$.
- $k + 2 < |Y \setminus W| < p - 4k - 9$.
- $\max\{|W|, |Z|\} \leq k$.

*If* $\min\left\{\left[\frac{n}{m}\right], \left[\frac{p}{m}\right] - \left[\frac{n}{m}\right], \mathrm{ind}_m(Y), m - \mathrm{ind}_m(Y)\right\} = 0$, *then* $m = 1$.

*Proof.* Write $l := \min\left\{\left[\frac{n}{m}\right], \left[\frac{p}{m}\right] - \left[\frac{n}{m}\right], \mathrm{ind}_m(Y), m - \mathrm{ind}_m(Y)\right\}$. Since $\left[\frac{p}{m}\right] \geq m$ and $p \neq 1$, we conclude that $\left[\frac{p}{m}\right] > 1$, and then the assumptions of Corollary 2.5 are satisfied. On one hand, Corollary 2.5 (i) yields $\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] > 0$. On the other hand, the definition of $\mathrm{ind}_m(Y)$ implies it is not zero and therefore we have to study two cases:

- Suppose that $l = \left[\frac{n}{m}\right]$. Then Corollary 2.5 (ii) implies that $\mathrm{ind}_m(Y) > k + 2$. Hence Corollary 2.5 (iv) leads to $\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] - 1 = 0$ and thereby Corollary 2.5 (v) yields $m - \mathrm{ind}_m(Y) > k + 3$. Adding $\left[\frac{n}{m}\right]$ with $\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right]$ and $\mathrm{ind}_m(Y)$ with $m - \mathrm{ind}_m(Y)$, we get that
$$1 = \left[\frac{p}{m}\right] \geq m > 2k + 5,$$
which is impossible.
- Suppose that $l = m - \mathrm{ind}_m(Y)$. Corollary 2.5 (v) yields $\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] > 2k + 7$. Then Corollary 2.5 (iv) implies that $\mathrm{ind}_m(Y) - 1 = 0$ and consequently $m = 1$. □

**Lemma 3.2.** *Let $Z$ and $W$ be subsets of $\mathbb{Z}/p\mathbb{Z}$, $k \in \mathbb{N} \cup \{0\}$ , $n \in \Gamma$, $m \in \Gamma \setminus \{0\}$ and $Y$ be an $m-$almost equidistributed subset of $\mathbb{Z}/p\mathbb{Z}$. Assume:*

- $\left[\frac{p}{m}\right] \geq m$.
- $\left[\overline{0}, \overline{n}\right] \setminus Z = Y \setminus W$.
- $k + 2 < |Y \setminus W| < p - 4k - 9$.
- $\max\{|W|, |Z|\} \leq k$.

*Then* $m = 1$.

*Proof.* Write $l := \min\left\{\left[\frac{n}{m}\right], \left[\frac{p}{m}\right] - \left[\frac{n}{m}\right], \operatorname{ind}_m(Y), m - \operatorname{ind}_m(Y)\right\}$. We shall show that if $l > 0$, then we contradict one of the assumptions; this will be enough to conclude the proof since we will have that $l = 0$ and hence the assertion will be a consequence of Lemma 3.1. Assume, from now on, that $l > 0$. Insomuch as $\left[\frac{p}{m}\right] \geq m$ and $p \neq 1$, we have that $\left[\frac{p}{m}\right] > 1$, and then the assumptions of Corollary 2.5 are satisfied. Now see that $l^2 \leq k$ by Corollary 2.5 (iii). We proceed studying four cases:

- Suppose that $l = \left[\frac{n}{m}\right]$. Corollary 2.5 (ii) yields $\operatorname{ind}_m(Y) > \frac{k+2}{l+1}$. Hence

$$\operatorname{ind}_m(Y) - 1 \geq \left[\frac{k+2}{l+1}\right].$$

  Then Corollary 2.5 (iv) leads to

$$\begin{aligned} k &\geq (\operatorname{ind}_m(Y) - 1)\left(\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] - 1\right) \\ &\geq \left[\frac{k+2}{l+1}\right]\left(\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] - 1\right); \end{aligned}$$

  thus, inasmuch as $l^2 \leq k$, we get that $\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] - 1 \leq l + 1$. Insomuch as $\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] \geq l$, we have that there is $\delta \in \{0, 1, 2\}$ such that $\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] = l + \delta$. Corollary 2.5 (iii) implies that $m - \operatorname{ind}_m(Y) \leq \frac{k}{l}$. Corollary 2.5 (v) lets us conclude that $m - \operatorname{ind}_m(Y) > \frac{2k+8-(l+\delta+1)}{l+\delta+1}$, and thus

$$\frac{2k + 8 - (l + \delta + 1)}{l + \delta + 1} < m - \operatorname{ind}_m(Y) \leq \frac{k}{l}. \tag{17}$$

  Nonetheless, insomuch as $l^2 \leq k$ and $\delta \in \{0, 1, 2\}$, (17) is false.

- Suppose that $l = \left[\frac{p}{m}\right] - \left[\frac{n}{m}\right]$. If $l = \left[\frac{n}{m}\right]$, we proceed as above; then we assume that $\left[\frac{n}{m}\right] \geq l + 1$. Corollary 2.5 (v) implies that $m - \operatorname{ind}_m(Y) > \frac{2k+7-l}{l+1}$. Insomuch as $\left[\frac{n}{m}\right] \geq l + 1$, Corollary 2.5 (iii) leads to $m - \operatorname{ind}_m(Y) \leq \frac{k}{l+1}$. Thus

$$\frac{2k + 7 - l}{l + 1} < m - \operatorname{ind}_m(Y) \leq \frac{k}{l + 1}$$

  which is impossible since $l^2 \leq k$.

- Suppose that $l = \operatorname{ind}_m(Y)$. From Corollary 2.5 (ii), we get that $\left[\frac{n}{m}\right] > \frac{k+2-l}{l}$. Corollary 2.5 (iii) leads to

$$k \geq \left[\frac{n}{m}\right](m - \operatorname{ind}_m(Y)) > \left(\frac{k + 2 - l}{l}\right)(m - \operatorname{ind}_m(Y));$$

  thus, inasmuch as $l^2 \leq k$, we get $m - \operatorname{ind}_m(Y) \leq l$. Therefore $m - \operatorname{ind}_m(Y) = l$ by the definition of $l$. Thus, insomuch as $m - \operatorname{ind}_m(Y) = l = \operatorname{ind}_m(Y)$, Corollary 2.5 (ii) and Corollary 2.5 (iii) yield $l \geq 2$. On one hand, Corollary 2.5 (iv) leads to $\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] \leq \frac{k+l-1}{l-1}$. On the other hand, Corollary 2.5 (v) implies that $\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] > \frac{2k+7-l}{l+1}$. Thus

$$\frac{2k + 7 - l}{l + 1} < \left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] \leq \frac{k + l - 1}{l - 1}; \tag{18}$$

  however, (18) is impossible since $l^2 \leq k$ and $l \geq 2$.

- Suppose that $l = m - \mathrm{ind}_m(Y)$. If $l = \mathrm{ind}_m(Y)$, then we proceed as above. Thus we assume that $\mathrm{ind}_m(Y) - 1 \geq l$. From Corollary 2.5 (v), we have that $\left[\frac{p}{m}\right] - \left[\frac{n}{m}\right] > \frac{2k+7-l}{l+1}$; then, from this inequality and Corollary 2.5 (iv), we conclude that $\mathrm{ind}_m(Y) - 1 < \frac{k(l+1)}{2k+6-2l}$. Hence
$$l \leq \mathrm{ind}_m(Y) - 1 < \frac{k(l+1)}{2k+6-2l}$$
which is impossible since $l^2 \leq k$. □

# 4 Examples of almost equidistributed subsets

In this section we show two families of examples of almost equidistributed subsets. Throughout this section, $s \in (\mathbb{Z}/p\mathbb{Z})^*$, $m \in \Gamma$ is such that $\overline{m} = s$ and $l := \min\{m, p-m\}$. Furthermore, for any $n \in \mathbb{Z}$ and $x \in \mathbb{Z}/p\mathbb{Z}$, if confusion is possible with the overline, we write $x \cdot \overline{n}$ (resp. $\overline{n} \cdot x$) instead of $x\overline{n}$ (resp. $\overline{n}x$).

**Lemma 4.1.** *Let $x \in \mathbb{Z}/p\mathbb{Z}$ and $X \in \mathrm{AAP}\big(\overline{1}, 0\big)$.*

*(i) If $|X| \leq \left[\frac{p}{l}\right]$, then $|\mathrm{I}_l(x) \cap sX| \leq 1$.*

*(ii) If $|X| \geq \left[\frac{p}{l}\right] + 1$, then $|\mathrm{I}_l(x) \cap sX| \geq 1$.*

*Proof.* Let $n \in \mathbb{Z}$ be such that $X = \left\{\overline{n}, \overline{n+1}, \ldots, \overline{n+|X|-1}\right\}$. First we show (i). Since $|X| \leq \left[\frac{p}{l}\right]$, there is $q \in \mathbb{Z}$ such that
$$\{ln, l(n+1), \ldots l(n+|X|-1)\} \subseteq \{q, q+1, \ldots, q+p-1\}.$$
As a consequence of this fact, for all $j, k \in \{0, \ldots, |X|-1\}$ such that $j \neq k$, we have that
$$l \leq |l(n+j) - l(n+k)| < p.$$
Thus, for any $w \in \mathbb{Z}/p\mathbb{Z}$ and $y, z \in X$, if $\overline{l} \cdot y, \overline{l} \cdot z \in \left[w, w + \overline{l-1}\right]$, then $y = z$. Since $\overline{l} \in \{\pm s\}$, claim (i) follows.

We assume that (ii) is false and we will arrive at a contradiction. Thus assume that $\mathrm{I}_l(x) \cap sX = \emptyset$. Write $Y := \left\{\overline{n}, \overline{n+1}, \ldots, \overline{n+\left[\frac{p}{l}\right]}\right\}$, $Y' := Y \setminus \left\{\overline{n+\left[\frac{p}{l}\right]}\right\}$ and $Y'' := Y \setminus \{\overline{n}\}$; hence $|Y'| = |Y''| = [\frac{p}{l}]$. Since $x$ is arbitrary in (i), we may apply (i) with $Y'$ (resp. $Y''$) and $x + \overline{jl}$ for each $1 \leq j \leq [\frac{p}{l}]$; consequently, for each $1 \leq j \leq [\frac{p}{l}]$,
$$\left|\mathrm{I}_l\big(x + \overline{jl}\big) \cap sY'\right| \leq 1 \qquad \text{and} \qquad \left|\mathrm{I}_l\big(x + \overline{jl}\big) \cap sY''\right| \leq 1. \tag{19}$$
On the other hand,
$$\mathbb{Z}/p\mathbb{Z} = \bigcup_{j=0}^{[\frac{p}{l}]} \mathrm{I}_l\big(x + \overline{jl}\big),$$
and then
$$sY = \bigcup_{j=0}^{[\frac{p}{l}]} \big(\mathrm{I}_l\big(x + \overline{jl}\big) \cap sY\big). \tag{20}$$

Note that $\mathrm{I}_l(x) \cap sY \subseteq \mathrm{I}_l(x) \cap sX = \emptyset$. Since $|Y| = \left[\frac{p}{l}\right] + 1$, the Pigeonhole Principle and the equalities in (20) yield at least one of the following cases:

- There is $1 \leq j \leq [\frac{p}{l}]$ such that $\left|\mathrm{I}_l\big(x + \overline{jl}\big) \cap sY\right| \geq 3$.
- There are $1 \leq j < k \leq [\frac{p}{l}]$ such that $\min\left\{\left|\mathrm{I}_l\big(x + \overline{jl}\big) \cap sY\right|, \left|\mathrm{I}_l\big(x + \overline{kl}\big) \cap sY\right|\right\} \geq 2$.

Inasmuch as $|Y \setminus Y'| = |Y \setminus Y''| = 1$, in any of these cases we contradict (19), and hence (ii) is true. □

**Lemma 4.2.** *Let $X \in \mathrm{AAP}\big(\overline{1}, 0\big)$. Then $sX$ is $l-$almost equidistributed.*

*Proof.* Let $n \in \mathbb{Z}$ be such that $X = \left\{\overline{n}, \overline{n+1}, \ldots, \overline{n+|X|-1}\right\}$. We prove the statement by induction on $|X|$. If $|X| \leq \left[\frac{p}{l}\right]$, then the claim is true by Lemma 4.1 (i). From now on, we assume that $|X| > \left[\frac{p}{l}\right]$ and that the statement is true for all $Z \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $|Z| < |X|$. Define $X' := X \setminus \{\overline{n}\}$. To complete the induction, we assume that the claim is false and we will arrive at a contradiction; thus we assume that there are $x, y \in \mathbb{Z}/p\mathbb{Z}$ such that $\mathrm{I}_l(x) \cap \mathrm{I}_l(y) = \emptyset$ and $|\mathrm{I}_l(x) \cap sX| > |\mathrm{I}_l(y) \cap sX| + 1$. Since $|X'| < |X|$, the induction basis yields

$$\Big||\mathrm{I}_l(x) \cap sX'| - |\mathrm{I}_l(y) \cap sX'|\Big| \leq 1.$$

Thus $s \cdot \overline{n} \in \mathrm{I}_l(x)$. Define $Y' := \left\{\overline{n}, \overline{n+1}, \ldots, \overline{n + \left[\frac{p}{l}\right]}\right\}$ and $Y'' := Y' \setminus \left\{\overline{n + \left[\frac{p}{l}\right]}\right\}$. From Lemma 4.1 (ii), we have that

$$|\mathrm{I}_l(y) \cap sY'| \geq 1;$$

hence there is $0 \leq k \leq \left[\frac{p}{l}\right]$ such that $s \cdot \overline{n+k} \in \mathrm{I}_l(y)$. Let $k_0$ be the smallest $k \in \mathbb{N} \cup \{0\}$ such that $s \cdot \overline{n+k} \in \mathrm{I}_l(y)$, so $0 < k_0 \leq \left[\frac{p}{l}\right]$. From Lemma 4.1 (i), we obtain that

$$|\mathrm{I}_l(x) \cap sY''| \leq 1;$$

since $s \cdot \overline{n} \in \mathrm{I}_l(x)$, $s \cdot \overline{n+k} \notin \mathrm{I}_l(x)$ for all $1 \leq k \leq \left[\frac{p}{l}\right] - 1$. Thus, insomuch as $\mathrm{I}_l(x) \cap \mathrm{I}_l(y) = \emptyset$, we conclude that $s \cdot \overline{n+k} \notin \mathrm{I}_l(x)$ for all $0 < k \leq k_0$. Hence, defining

$$Y := \left\{\overline{n+k_0+1}, \overline{n+k_0+2}, \ldots, \overline{n+|X|-1}\right\},$$

we have by induction that

$$|\mathrm{I}_l(x) \cap sY| = \left|(\mathrm{I}_l(x) \cap sX) \setminus \left\{s \cdot \overline{n}\right\}\right| = |\mathrm{I}_l(x) \cap sX| - 1$$

and

$$|\mathrm{I}_l(y) \cap sY| = \left|(\mathrm{I}_l(y) \cap sX) \setminus \left\{s \cdot \overline{n+k_0}\right\}\right| = |\mathrm{I}_l(y) \cap sX| - 1$$

so $|\mathrm{I}_l(x) \cap sY| > |\mathrm{I}_l(y) \cap sY| + 1$; however, since $|Y| < |X|$, we have that

$$\Big||\mathrm{I}_l(x) \cap sY| - |\mathrm{I}_l(y) \cap sY|\Big| \leq 1,$$

and this contradiction completes the proof. □

We start the construction of the second family of examples of almost equidistributed subsets.

**Lemma 4.3.** *Let $x \in \mathbb{Z}/p\mathbb{Z}$ and $X \in \mathrm{AAP}\big(\overline{1}, 0\big)$.*

*(i) If $|X| \leq l$, then $|\mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}X| \leq 1$.*

*(ii) If $|X| \geq l+1$, then $|\mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}X| \geq 1$.*

*Proof.* Let $n \in \mathbb{Z}$ be such that $X = \left\{\overline{n}, \overline{n+1}, \ldots, \overline{n+|X|-1}\right\}$ and $h \in \Gamma$ such that $\overline{h} = s^{-1}$. Assume that $l = m$ (the case $l = p - m$ is solved in the same way changing the signs where it is necessary). First we show (i). Suppose that there are $0 \leq k \leq j \leq l-1$ such that $\overline{h(n+j)}, \overline{h(n+k)} \in \mathrm{I}_{[\frac{p}{l}]}(x)$. This means that there is $q \in \mathbb{Z}$ with $0 \leq q \leq \left[\frac{p}{l}\right]$ such that $\overline{q} = \overline{h(k-j)}$ or $\overline{q} = \overline{h(j-k)}$; without loss of generality, we assume that $\overline{q} = \overline{h(j-k)}$. On one hand, $\overline{l} = \overline{m} = s$; thus there is $g \in \Gamma$ such that

$$hl = gp + 1. \tag{21}$$

On the other hand, since $\overline{q} = \overline{h(j-k)}$, there is $f \in \Gamma$ such that

$$h(j-k) = fp + q. \tag{22}$$

Inasmuch as $j - k < l$, we get that $f \leq g$. If we multiply (21) by $j-k$ and (22) by $l$, we conclude that

$$(j-k)gp + (j-k) = hl(j-k) = flp + lq. \tag{23}$$

Since $q \leq \left[\frac{p}{l}\right]$, we have that $j - k, lq \in \Gamma$ and therefore (23) yields $j - k = lq$. Moreover, by this equality and (23), we have that $(j-k)gp = flp$. From the equalities $j - k = lq$ and $(j-k)gp = flp$, we deduce that $f = gq$. Since $gq = f \leq g$ and $j - k < l$, we obtain from (21) and (22) that $q = 0$. Therefore $\overline{h(n+j)} = \overline{h(n+k)}$ and (i) is proven.

We assume that (ii) is false and we will arrive at a contradiction. Thus assume that $\mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}X = \emptyset$. Write $Y := \left\{\overline{n}, \overline{n+1}, \ldots, \overline{n+l}\right\}$, $Y' := Y \setminus \left\{\overline{n+l}\right\}$ and $Y'' := Y \setminus \{\overline{n}\}$; hence $|Y'| = |Y''| = l$. Since $x$ is arbitrary in (i), we may apply (i) with $Y'$ (resp. $Y''$) and $x + \overline{jl}$ for each $1 \leq j \leq l$; consequently, for each $1 \leq j \leq l$,

$$\left|\mathrm{I}_{[\frac{p}{l}]}\left(x + j\overline{\left[\frac{p}{l}\right]}\right) \cap s^{-1}Y'\right| \leq 1 \qquad \text{and} \qquad \left|\mathrm{I}_{[\frac{p}{l}]}\left(x + j\overline{\left[\frac{p}{l}\right]}\right) \cap s^{-1}Y''\right| \leq 1. \tag{24}$$

See that

$$\mathbb{Z}/p\mathbb{Z} = \bigcup_{j=0}^{l} \mathrm{I}_{[\frac{p}{l}]}\left(x + j\overline{\left[\frac{p}{l}\right]}\right),$$

and then

$$sY = \bigcup_{j=0}^{l} \left(\mathrm{I}_{[\frac{p}{l}]}\left(x + j\overline{\left[\frac{p}{l}\right]}\right) \cap s^{-1}Y\right). \tag{25}$$

Notice that $\mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}Y \subseteq \mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}X = \emptyset$. Insomuch as $|Y| = l + 1$, the Pigeonhole Principle and (25) imply that at least one of the following assertions holds:

- The existence of $1 \leq j \leq l$ such that $\left|\mathrm{I}_{[\frac{p}{l}]}\left(x + \overline{j\left[\frac{p}{l}\right]}\right) \cap s^{-1}Y\right| \geq 3$.
- The existence of $1 \leq j < k \leq l$ such that $\min\left\{\left|\mathrm{I}_{[\frac{p}{l}]}\left(x+\overline{j\left[\frac{p}{l}\right]}\right)\cap s^{-1}Y\right|, \left|\mathrm{I}_{[\frac{p}{l}]}\left(x+\overline{k\left[\frac{p}{l}\right]}\right)\cap s^{-1}Y\right|\right\} \geq 2$.

Inasmuch as $|Y \setminus Y'| = |Y \setminus Y''| = 1$, any of these assertions contradicts (24); hence (ii) is true. □

**Lemma 4.4.** *Let $X \in \mathrm{AAP}(\overline{1}, 0)$. Then $s^{-1}X$ is $\left[\frac{p}{l}\right]-$almost equidistributed.*

*Proof.* Let $n \in \mathbb{Z}$ be such that $X = \left\{\overline{n}, \overline{n+1}, \ldots, \overline{n+|X|-1}\right\}$. The proof is done by induction on $|X|$. If $|X| \leq l$, then the claim is true by Lemma 4.3 (i). We assume that $|X| > l$ and that the statement is true for all $Z \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $|Z| < |X|$. Define $X' := X \setminus \{\overline{n}\}$. We complete the induction assuming that the claim is false and, as a consequence of this, arriving at a contradiction. Let $x, y \in \mathbb{Z}/p\mathbb{Z}$ be such that $\mathrm{I}_{[\frac{p}{l}]}(x) \cap \mathrm{I}_{[\frac{p}{l}]}(y) = \emptyset$, and assume, without loss of generality, that $|\mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}X| > |\mathrm{I}_{[\frac{p}{l}]}(y) \cap s^{-1}X| + 1$. Insomuch as $|X'| < |X|$, we notice that

$$\left|\left|\mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}X'\right| - \left|\mathrm{I}_{[\frac{p}{l}]}(y) \cap s^{-1}X'\right|\right| \leq 1,$$

and therefore $s^{-1} \cdot \overline{n} \in \mathrm{I}_{[\frac{p}{n}]}(x)$. Define $Y' := \left\{\overline{n}, \overline{n+1}, \ldots, \overline{n+l}\right\}$ and $Y'' := Y \setminus \left\{\overline{n+l}\right\}$. Lemma 4.3 (ii) yields

$$\left|\mathrm{I}_{[\frac{p}{l}]}(y) \cap s^{-1}Y'\right| \geq 1;$$

hence there is $0 \leq k \leq l$ such that $s^{-1} \cdot \overline{n+k} \in \mathrm{I}_{[\frac{p}{l}]}(y)$. Let $k_0$ be the smallest $k \in \mathbb{N} \cup \{0\}$ such that $s^{-1} \cdot \overline{n+k} \in \mathrm{I}_{[\frac{p}{l}]}(y)$ so $0 < k_0 \leq l$. On the other hand, Lemma 4.3 (i) implies that

$$\left|\mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}Y''\right| \leq 1;$$

since $s^{-1}\cdot\overline{n} \in \mathrm{I}_{[\frac{p}{l}]}(x)$, $s^{-1}\cdot\overline{n+k} \notin \mathrm{I}_{[\frac{p}{l}]}(x)$ for all $1 \leq k \leq l-1$. Insomuch as $\mathrm{I}_{[\frac{p}{l}]}(x) \cap \mathrm{I}_{[\frac{p}{l}]}(y) = \emptyset$, we conclude that $s^{-1} \cdot \overline{n+k} \notin \mathrm{I}_{[\frac{p}{l}]}(x)$ for all $0 < k \leq k_0$. Set

$$Y := \left\{\overline{n+k_0+1}, \overline{n+k_0+2}, \ldots, \overline{n+|X|-1}\right\},$$

and note that

$$\left|\mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}Y\right| = \left|(\mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}X) \setminus \{s^{-1} \cdot \overline{n}\}\right| = \left|\mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}X\right| - 1$$

and

$$\left|\mathrm{I}_{[\frac{p}{l}]}(y) \cap s^{-1}Y\right| = \left|(\mathrm{I}_{[\frac{p}{l}]}(y) \cap s^{-1}X) \setminus \left\{s^{-1} \cdot \overline{n+k_0}\right\}\right| = \left|\mathrm{I}_{[\frac{p}{l}]}(y) \cap s^{-1}X\right| - 1.$$

This means that $|\mathrm{I}_{[\frac{p}{l}]}(x) \cap s^{-1}Y| > |\mathrm{I}_{[\frac{p}{l}]} \cap s^{-1}Y| + 1$; nevertheless, insomuch as $|Y| < |X|$, this contradicts the induction hypothesis and the proof is completed. □

# 5 Proof of Theorem 1.1

In this section we complete the proof of Theorem 1.1 and we show that it is sharp. Before we complete its proof, we need the following remark.

**Remark 5.1.** *Let $X$ be a nonempty subset of $\mathbb{Z}/p\mathbb{Z}$, $k \in \mathbb{N} \cup \{0\}$, $s \in (\mathbb{Z}/p\mathbb{Z})^*$ and $u \in \mathbb{Z}/p\mathbb{Z}$. The following statements are equivalent:*

- $X \in \mathrm{AAP}(s,k)$.
- $X + u \in \mathrm{AAP}(s,k)$.
- $s^{-1}X \in \mathrm{AAP}\big(\overline{1},k\big)$.

We start with the proof of our main theorem.

*Proof. (Theorem 1.1)* Let $s := rt^{-1}$, $q \in \Gamma$ be such that $\overline{q} = s$ and $l := \min\{q, p-q\}$. First we shall show that $\left[\frac{p}{l}\right] \geq l$; we assume that $\left[\frac{p}{l}\right] < l$ and we arrive at a contradiction. Since $X \in \mathrm{AAP}(r,k) \cap \mathrm{AAP}(t,k)$, Remark 5.1 yields $r^{-1}X \in \mathrm{AAP}\big(\overline{1},k\big) \cap \mathrm{AAP}(s^{-1},k)$. Furthermore, inasmuch as $r^{-1}X \in \mathrm{AAP}\big(\overline{1},k\big)$, Remark 5.1 lets us translate $r^{-1}X$, if necessary, so we may assume that there are $n \in \mathbb{N} \cup \{0\}$ and $Z \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $r^{-1}X = \big[\overline{0},\overline{n}\big] \setminus Z$ and $|Z| \leq k$. Insomuch as $r^{-1}X \in \mathrm{AAP}(s^{-1},k)$, there are $Y \in \mathrm{AAP}(s^{-1},0)$ and $W \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $r^{-1}X = Y \setminus W$ and $|W| \leq k$. Inasmuch as $Y \in \mathrm{AAP}(s^{-1},0)$, Remark 5.1 and Lemma 4.4 yield $Y$ is $\left[\frac{p}{l}\right]-$almost equidistributed. Since $\left[\frac{p}{l}\right] < l$, we have that $\left[\frac{p}{\left[\frac{p}{l}\right]}\right] \geq \left[\frac{p}{l}\right]$. Thus all the assumptions of Lemma 3.2 are fulfilled by $m = \left[\frac{p}{l}\right]$ and the subsets $\big[\overline{0},\overline{n}\big], Z, Y, W$. Lemma 3.2 leads to $\left[\frac{p}{l}\right] = 1$; however, inasmuch as $l = \min\{q, p-q\} \leq \frac{p}{2}$, we have that $\left[\frac{p}{l}\right] \geq 2$ and this contradiction implies that $\left[\frac{p}{l}\right] \geq l$.

We conclude the proof with a very similar idea to the one of the previous paragraph. Insomuch $X \in \mathrm{AAP}(r,k) \cap \mathrm{AAP}(t,k)$, Remark 5.1 yields $t^{-1}X \in \mathrm{AAP}(s,k) \cap \mathrm{AAP}\big(\overline{1},k\big)$. Moreover, inasmuch as $t^{-1}X \in \mathrm{AAP}\big(\overline{1},k\big)$, Remark 5.1 lets us translate $t^{-1}X$, if necessary, so we may assume that there are $n' \in \mathbb{N} \cup \{0\}$ and $Z' \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $t^{-1}X = \big[\overline{0},\overline{n'}\big] \setminus Z'$ and $|Z'| \leq k$. Since $t^{-1}X \in \mathrm{AAP}(s,k)$, there are $Y' \in \mathrm{AAP}(s,0)$ and $W' \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $t^{-1}X = Y' \setminus W'$ and $|W'| \leq k$. Insomuch as $Y' \in \mathrm{AAP}(s,0)$, Remark 5.1 and Lemma 4.2 imply that $Y'$ is $l-$almost equidistributed. Inasmuch as $\left[\frac{p}{l}\right] \geq l$, all the assumptions of Lemma 3.2 are fulfilled by $m = l$ and the subsets $\big[\overline{0},\overline{n'}\big], Z', Y', W'$. Lemma 3.2 implies that $l = 1$; hence $t \in \{\pm r\}$. $\square$

We conclude this section with examples which show that Theorem 1.1 is sharp.

**Example 5.2.** *Let $p > 91$ be such that there is $q \in \mathbb{N} \cup \{0\}$ satisfying that $p = 12q + 7$ (there is an infinite number of these primes by Dirichlet's prime number theorem, see [4]). Set $k := 2q+2$ and define*

$$Z := \left\{\overline{4m+2}, \overline{4m+3} : \ m \in \mathbb{Z},\ 0 \leq m \leq q\right\}$$
$$W := \overline{4}\left[\overline{q+2}, \overline{3q+1}\right]$$
$$Y := \overline{4}\left[\overline{0}, \overline{4q+3}\right].$$

*Then* $\big[\overline{0}, \overline{4q+5}\big] \setminus Z = Y \setminus W$. *This means that if* $X := \big[\overline{0}, \overline{4q+5}\big] \setminus Z$, *then* $X \in \mathrm{AAP}\big(\overline{4}, k\big) \cap \mathrm{AAP}\big(\overline{1}, k\big)$. *Finally*

$$k + 2 = |X| = p - 5k + 7 < p - 4k - 9$$

*where the inequality is a consequence of* $p > 91$.

Example 5.2 shows that the lower bound $|X| > k + 2$ in Theorem 1.1 is optimal. The next example shows that the upper bound $|X| < p - 4k - 9$ in Theorem 1.1 is sharp; however, we do not know if it is optimal.

**Example 5.3.** *Let* $p > 11$ *be such that there is* $k \in \mathbb{N} \cup \{0\}$ *satisfying that* $p = 6k - 1$. *Define*

$$\begin{aligned} Z &:= \Big\{\overline{3m+2} : \ m \in \mathbb{Z},\, 0 \leq m \leq k-2\Big\} \\ W &:= \overline{3}\Big[\overline{k}, \overline{2k-1}\Big] \\ Y &:= \overline{3}\Big[\overline{0}, \overline{3k-1}\Big]. \end{aligned}$$

*Then* $\big[\overline{0}, \overline{3k-2}\big] \setminus Z = Y \setminus W$. *This means that if* $X := \big[\overline{0}, \overline{3k-2}\big] \setminus Z$, *then* $X \in \mathrm{AAP}\big(\overline{3}, k\big) \cap \mathrm{AAP}\big(\overline{1}, k\big)$. *Hence*

$$k + 2 < 2k = |X| = p - 4k + 1$$

*where the inequality comes from the fact* $p > 11$.

# References


[1] Hamidoune, Y., & Rødseth, Ø. (2000) An inverse theorem mod $p$, *Acta Arithmetica*, 92, 251–262.

[2] Hamidoune, Y., Serra, O., & Zémor, G. (2006) On the critical pair theory in $\mathbb{Z}/p\mathbb{Z}$, *Acta Arithmetica*, 121, 99–115.

[3] Huicochea, M., & Montejano, A. (2015) The structure of rainbow-free colorings for linear equations on three variables in $\mathbb{Z}_p$, *Integers: Electronic Journal of Combinatorial Number Theory*, 15A, A8.

[4] Neukirch, J. (2002) *Algebraic Number Theory (Grundlehren der mathematischen Wissenschaften*, Vol. 322, Spinger-Verlag.

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