INVERSE THEOREMS IN $\mathbb{Z}/p\mathbb{Z}$ WHEN A SUBSET IS CONTAINED IN A SHORT ARITHMETIC PROGRESSION

Mario Huicochea
Facultad de Ciencias, UNAM, Querétaro, México
dym@cimat.mx

Received: 7/2/16, Revised: 2/15/17, Accepted: 8/2/17, Published: 9/14/17

Abstract

In most of the proofs of the inverse theorems in $\mathbb{Z}/p\mathbb{Z}$, an important case is the one where one of the subsets is contained in a short arithmetic progression. In this paper we give nontrivial inverse results in $\mathbb{Z}/p\mathbb{Z}$ when one of the subsets is contained in a short arithmetic progression.

1. Introduction

Throughout 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. For any $x \in \mathbb{Z}$, we denote by $\overline{x}$ its projection into $\mathbb{Z}/p\mathbb{Z}$. We write $(\mathbb{Z}/p\mathbb{Z})^* := \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$. Given $d \in (\mathbb{Z}/p\mathbb{Z})^*$, we say that a subset A of $\mathbb{Z}/p\mathbb{Z}$ is an *arithmetic progression with difference* d if there is $a \in \mathbb{Z}/p\mathbb{Z}$ such that $A = \{a + \overline{i}d : \ 0 \leq i \leq |A| - 1\}$. For any nonempty subset A of $\mathbb{Z}/p\mathbb{Z}$, we denote by $l_d(A)$ the cardinality of the shortest arithmetic progression with difference d which contains A. For any subsets A and B of $\mathbb{Z}/p\mathbb{Z}$ and $c \in \mathbb{Z}/p\mathbb{Z}$, set

$$A + B := \{a + b : \ a \in A, \, b \in B\} \qquad \text{and} \qquad cA := \{ca : \ a \in A\};$$

in particular, $-A := \{-a : \ a \in A\}$. We write $A + c := A + \{c\}$. We say that (A, B, C) is a *trio* if A, B and C are nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $\overline{0} \notin A + B + C$. For a trio (A, B, C), we write $r(A, B, C) := p - |A| - |B| - |C|$; by the Cauchy-Davenport Theorem, $r(A, B, C) \geq -1$, see [1, Thm. 6.2]

In additive number theory, one of the most fruitful areas has been the one of the so called inverse theorems. In particular, there has been a great development in the inverse theorems in $\mathbb{Z}/p\mathbb{Z}$, see [1], [2], [3], [5]. An important conjecture in the area is the following one which was proposed by Hamidoune, Serra and Zémor in [3]. We give a trio formulation of it.

Conjecture 1.1. Let (A, B, C) be a trio of $\mathbb{Z}/p\mathbb{Z}$ and $r \in \mathbb{Z}$. Assume

- $|A| \geq r+3$.
- $\min\{|B|,|C|\} \geq r+4$.
- $r(A,B,C) \leq r$.

Then there is $d \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $l_d(A) \leq |A|+r+1, l_d(B) \leq |B|+r+1$ and $l_d(C) \leq |C|+r+1$.

In most of the proofs of the inverse theorems in $\mathbb{Z}/p\mathbb{Z}$, a fundamental part of them is the proof of the result when one of the sets is contained in a short arithmetic progression. Moreover, in the program proposed in [3] to show Conjecture 1.1, it is established that the first step to solve it is to prove this conjecture assuming that one of the sets is already contained in a short arithmetic progression. This problem is the motivation of this paper.

The first result of this paper is the following.

Theorem 1.2. *Let (A,B,C) be a trio of $\mathbb{Z}/p\mathbb{Z}$ and $r \in \mathbb{Z}$. Assume*

- $|A| \geq 2r+4$.
- $|B| \geq 3r+6$.
- $|C| \geq r+4$.
- $r(A,B,C) \leq r$.
- *There is $d \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $l_d(A) \leq |A|+r+1$.*

Then $l_d(B) \leq |B|+r+1$ and $l_d(C) \leq |C|+r+1$.

Unfortunately the lower bounds of $|A|$ and $|B|$ in Theorem 1.2 are bigger than the ones in Conjecture 1.1. The next result deals with this.

Theorem 1.3. *Let (A,B,C) be a trio of $\mathbb{Z}/p\mathbb{Z}$ and $r \in \mathbb{Z}$. Assume*

- $|A| \geq r+3$.
- $\min\{|B|,|C|\} \geq r+4$.
- $r(A,B,C) \leq r$.
- *There is $d \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $l_d(A) \leq |A|+r+1$.*
- $|B| = \max\{|A|,|B|,|C|\}$ *or* $|C| = \max\{|A|,|B|,|C|\}$.
- $35r+45 \leq p$.

Then $l_d(B) \leq |B|+r+1$ and $l_d(C) \leq |C|+r+1$.

For $r \leq cp-2.2$ with $c = 3.1\cdot 10^{-1549}$, Conjecture 1.1 was proven by Grynkiewicz, see [1, Thm. 21.8]. However, due to the difference between 35 and $3.1^{-1}\cdot 10^{1549}$, Theorem 1.3 provides an important improvement when one of the sets of the trio which is not the biggest is contained in a short arithmetic progression.

This paper is organized as follows. In Section 2 we state some results that will be needed in the proof of our main results. Later, in Section 3, we prove Theorem 1.2 and a corollary of it. In Section 4 we define the concept of $A-$sparse (resp. $X-$sparse) in $\mathbb{Z}/p\mathbb{Z}$ (resp. $\mathbb{Z}$), and we show some properties used in the last section. The proof of Theorem 1.3 is completed in Section 5.

For the sake of comprehension, throughout this paper, the first letters of the alphabet $A, B, C, \ldots$ (resp. $a, b, c, \ldots$) will be subsets (resp. elements) of $\mathbb{Z}/p\mathbb{Z}$ while the last letters of the alphabet $Z, Y, X, \ldots$ (resp. $z, y, x, \ldots$) will be subsets (resp. elements) of $\mathbb{Z}$. Moreover, the symbols $\ldots, -1, 0, 1, 2, \ldots$ will denote the elements of $\mathbb{Z}$ while their respective projections in $\mathbb{Z}/p\mathbb{Z}$ will be denoted by $\ldots, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \ldots$.

2. Preliminaries

For any nonempty subsets X and Y of $\mathbb{Z}$ and $z \in \mathbb{Z}$, we write

$$X + Y := \{x + y : \ x \in X,\, y \in Y\} \qquad \text{and} \qquad zX := \{zx : \ x \in X\};$$

to abbreviate the notation, we write $X + z := X + \{z\}$. If X is finite, we denote by $\mathrm{GCD}(X)$ the greatest common divisor of the elements of X, and $\mathrm{GCD}^*(X) := \mathrm{GCD}(X - X)$; note that $\mathrm{GCD}^*(X) = \mathrm{GCD}(X - x)$ for any $x \in X$. We set $L(X) := 1 + \max X - \min X$ and $\overline{X} := \{\overline{x} : \ x \in X\}$. The first proposition is a particular case of some results that can be found in [4].

Proposition 2.1. *Let X and Y be nonempty finite subsets of $\mathbb{Z}$ such that $\mathrm{GCD}^*(X) = 1$ and $L(X) < L(Y)$.*

(i) If $\mathrm{GCD}^*(Y) > 1$, then

$$|X + Y| \geq |X| + 2|Y| - 2.$$

(ii) If $\mathrm{GCD}^*(Y) = 1$, then

$$|X + Y| \geq |X| + |Y| + \min\{|X| - 2, L(Y) - |Y| - 1\}.$$

Proof. For (i), see [4, Lemma 2]. For (ii), see [4, Thm. 2]. □

We will need a weak version of the Generalized $3k - 4$ Theorem of Grynkiewicz.

Theorem 2.2. *Let X and Y be nonempty finite subsets of $\mathbb{Z}$ such that $\mathrm{GCD}^*(X + Y) = 1$ and let $r \in \mathbb{Z}$. Assume*

- $|X| \geq r+3$.
- $|Y| \geq r+4$.
- $|X+Y| - |X| - |Y| \leq r$.

Then $L(X) \leq |X| + r + 1$, $L(Y) \leq |Y| + r + 1$ *and there is* $z \in \mathbb{Z}$ *such that* $\{z, z+1, \ldots, z+|X|+|Y|-2\} \subseteq X+Y$.

Proof. See [1, Thm. 7.1]. □

For any nonempty subset A of $\mathbb{Z}/p\mathbb{Z}$, we abbreviate writing $l(A) := l_{\overline{1}}(A)$. We write $\Gamma := \{z \in \mathbb{Z} : \ 0 \leq z \leq p-1\}$ so there is one and only one representative in Γ of each class of $\mathbb{Z}/p\mathbb{Z}$. For any $a, b \in \mathbb{Z}/p\mathbb{Z}$, let $z \in \Gamma$ be such that $\overline{z} = b - a$ and set

$$[a, b] := \big\{a + \overline{x} \in \mathbb{Z}/p\mathbb{Z} : \ x \in \Gamma, \ x \leq z\big\}.$$

With this notation, A is an arithmetic progression with difference $d \in (\mathbb{Z}/p\mathbb{Z})^*$ if and only if there are $a, b \in \mathbb{Z}/p\mathbb{Z}$ such that $A = d[a, b]$. An easy consequence of Theorem 2.2 is the following statement in $\mathbb{Z}/p\mathbb{Z}$.

Corollary 2.3. *Let* (A, B, C) *be a trio of* $\mathbb{Z}/p\mathbb{Z}$ *and* $r \in \mathbb{Z}$. *Assume*

- $|A| \geq r+3$.
- $\min\{|B|, |C|\} \geq r+4$.
- $r(A, B, C) \leq r$.
- $l(A) \leq |A| + r + 1$.
- $l(A) + l(C) \leq p$.

Then $l(B) \leq |B| + r + 1$ *and* $l(C) \leq |C| + r + 1$.

Proof. Let $a', a, c', c \in \mathbb{Z}/p\mathbb{Z}$ be such that $A \subseteq [a', a]$, $C \subseteq [c', c]$, $l(A) = |[a', a]|$ and $l(C) = |[c', c]|$. Translating A and C if necessary, assume that $a' = c' = \overline{0}$. If A, B and C are fixed and the statement holds for r, then the statement is true for $r+1$. Thus it suffices to show the theorem assuming that

$$r = r(A, B, C). \tag{1}$$

Let X and Y be the subsets of Γ such that $\overline{X} = A$ and $\overline{Y} = C$. Since $l(A) + l(C) \leq p$, we have that $X + Y \subseteq \Gamma$. Therefore

$$|X + Y| = |A + C|.$$

Moreover, since (A, B, C) is a trio, $B \subseteq \mathbb{Z}/p\mathbb{Z} \setminus -(A + C)$ and thus

$$|X + Y| - |X| - |Y| = |A + C| - |A| - |C| \leq r(A, B, C) = r. \tag{2}$$

Insomuch as $l(A) \leq |A| + r + 1$ and $|A| \geq r + 3$, X has two consecutive numbers so $\mathrm{GCD}^*(X) = 1$ and therefore

$$\mathrm{GCD}^*(X + Y) = 1. \tag{3}$$

From (2) and (3), the assumptions of Theorem 2.2 are fulfilled by X, Y and r, and therefore there is $z \in \mathbb{Z}$ such that

$$\{z, z + 1, \ldots, z + |X| + |Y| - 2\} \subseteq X + Y. \tag{4}$$

Inasmuch as $\overline{X + Y} = A + C$, (4) yields that there are $b', b \in \mathbb{Z}$ such that $\mathbb{Z}/p\mathbb{Z} \setminus -(A + C) \subseteq [b', b]$ and

$$|[b', b]| \leq p - |A| - |C| + 1. \tag{5}$$

Hence $B \subseteq \mathbb{Z}/p\mathbb{Z} \setminus -(A + C) \subseteq [b', b]$. We conclude that $l(B) \leq |B| + r + 1$ because

$$\begin{aligned} |[b', b]| &\leq p - |A| - |C| + 1 && \Big(\text{by (5)}\Big) \\ &= |B| + r(A, B, C) + 1 \\ &= |B| + r + 1. && \Big(\text{by (1)}\Big) \end{aligned}$$

In particular,

$$\begin{aligned} l(A) + l(B) &\leq |A| + |B| + 2r + 2 \\ &= p - |C| - r(A, B, C) + 2r + 2 \\ &= p - |C| + r + 2 && \Big(\text{by (1)}\Big) \\ &\leq p. \end{aligned} \tag{6}$$

From (6), we can proceed with the pair (A, B) as we did with (A, C), and we conclude that $l(C) \leq |C| + r + 1$. □

3. Proof of Theorem 1.2

In this section we show Theorem 1.2. At the end of this section, we state a corollary used in the proof of Theorem 1.3.

Proof. (Theorem 1.2) Assume without loss of generality that $d = \overline{1}$ (otherwise we make a dilation by d^{-1} to A, B and C). Let $a', a \in \mathbb{Z}/p\mathbb{Z}$ be such that $A \subseteq [a', a]$ and $l(A) = |[a', a]|$. Translating A if necessary, assume that $a' = \overline{0}$. Also, translating B

if necessary, assume that $\overline{p-1} \notin A+B$. Define $B' := B \cap \big[\overline{0}, \overline{p-2}-a\big]$. Insomuch as $B' \subseteq \big[\overline{0}, \overline{p-2}-a\big]$,

$$l(A)+l(B') \le p. \tag{7}$$

Inasmuch as $\overline{p-1} \notin A+B$, we have that $(\overline{p-1}-A) \cap B = \emptyset$. Hence

$$B \cap \big[\overline{p-1}-a, \overline{p-1}\big] \subseteq \overline{p-1} - \big(\big[\overline{0}, a\big] \setminus A\big),$$

and therefore

$$\begin{aligned} |B'| &\ge |B| - \big|\big[\overline{0}, a\big] \setminus A\big| \\ &\ge |B| - r - 1. \qquad \Big(\text{since } l(A) \le |A| + r + 1\Big) \end{aligned} \tag{8}$$

Since $B' \subseteq B$, we get that $|A+B'| \le |A+B|$. Insomuch as (A,B,C) is a trio, $C \subseteq \mathbb{Z}/p\mathbb{Z} \setminus -(A+B)$. Hence (8) leads to

$$|A+B'| - |A| - |B'| \le |A+B| - |A| - |B'| \le r(A,B,C) + r + 1 \le 2r+1. \tag{9}$$

Recall that $\Gamma := \{z \in \mathbb{Z} : \ 0 \le z \le p-1\}$. Let X and Y be the subsets of Γ such that $\overline{X} = A$ and $\overline{Y} = B'$. Thus

$$|X| = |A| \ge 2r+4 \tag{10}$$

and from (8)

$$|Y| = |B'| \ge 2r+5. \tag{11}$$

Insomuch as $l(A) \le |A| + r + 1$ and $|A| \ge 2r+4$, X has two consecutive numbers and therefore $\mathrm{GCD}^*(X) = 1$. In particular,

$$\mathrm{GCD}^*(X+Y) = 1. \tag{12}$$

From (7), $X+Y \subseteq \Gamma$. Since $\overline{X+Y} = A+B'$,

$$|X+Y| = |A+B'|,$$

and (9) implies that

$$|X+Y| - |X| - |Y| \le 2r+1. \tag{13}$$

From (10), (11), (12) and (13), we can apply Theorem 2.2 to X, Y and $2r+1$. Hence, by Theorem 2.2, there is $z \in \mathbb{Z}$ such that

$$\{z, z+1, \dots, z+|X|+|Y|-2\} \subseteq X+Y. \tag{14}$$

Inasmuch as $\overline{X+Y} = A+B' \subseteq A+B$, (14) yields that there are $c', c \in \mathbb{Z}$ such that $\mathbb{Z}/p\mathbb{Z} \setminus -(A+B) \subseteq [c', c]$ and

$$|[c', c]| \le p - |A| - |B'| + 1. \tag{15}$$

Thus $C \subseteq \mathbb{Z}/p\mathbb{Z} \setminus -(A+B) \subseteq [c', c]$, and

$$\begin{aligned} l(A)+l(C) &\leq l(A)+|[c',c]| \\ &= l(A)+p-|A|-|B'|+1 && \Big(\text{by (15)}\Big) \\ &\leq p-|B'|+r+2 && \Big(\text{since } l(A) \leq |A|+r+1\Big) \\ &\leq p-r-3 && \Big(\text{by (8)}\Big) \\ &\leq p. && (16) \end{aligned}$$

From (16), we can apply Corollary 2.3 to (A, B, C), and we get the desired result. □

Corollary 3.1. *Let (A, B, C) be a trio of $\mathbb{Z}/p\mathbb{Z}$ and $r \in \mathbb{Z}$. Assume*

- $|A| \geq 2r+4$.
- $\min\{|B|, |C|\} \geq r+4$.
- $r(A, B, C) \leq r$.
- *There is $d \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $l_d(A) \leq |A|+r+1$.*
- $|B| = \max\{|A|, |B|, |C|\}$ *or* $|C| = \max\{|A|, |B|, |C|\}$.
- $10r+18 \leq p$.

Then $l_d(B) \leq |B|+r+1$ and $l_d(C) \leq |C|+r+1$.

Proof. Assume without loss of generality that $|B| = \max\{|A|, |B|, |C|\}$. Then

$$\begin{aligned} |B| &\geq \frac{|A|+|B|+|C|}{3} \\ &\geq \frac{p-r}{3} \\ &\geq 3r+6. \end{aligned}$$

Thus (A, B, C) satisfies the assumptions of Theorem 1.2, and we have proven the claim. □

4. Sparse Sets

Let X and Y be nonempty finite subsets of $\mathbb{Z}$. We say that Y is $X-$*sparse* if $L(Y) \geq 2L(X)$ and $L(Z)-|Z| \geq |X|$ for any subset Z of Y such that $L(Z) \geq 2L(X)$. Let A and B be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$. We say that B is $A-$*sparse* if $|[a, b] \setminus B| \geq |A|$ for any $a, b \in \mathbb{Z}/p\mathbb{Z}$ such that $|[a, b]| \geq 2l(A)$. There is a trivial relation between the concept of sparse in $\mathbb{Z}$ and sparse in $\mathbb{Z}/p\mathbb{Z}$ which is the following remark.

Remark 4.1. Let A and B be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$, and let X and Y be the subsets of Γ such that $\overline{X} = A$ and $\overline{Y} = B$. If B is $A-$sparse and $L(Y) \geq 2L(X)$, then Y is $X-$sparse.

We will need the following lemma in the next section.

Lemma 4.2. *Let X and Y be nonempty finite subsets of $\mathbb{Z}$. Assume that $L(X) - |X| + 2 \leq |X|$ and Y is X-sparse. If $|Y| \geq 5L(X)$, then*

$$|X + Y| \geq |X| + |Y| + 2|X| - 2.$$

Proof. Write $Y = \{y_1, y_2, \ldots, y_{|Y|}\}$ with $y_1 < y_2 < \ldots < y_{|Y|}$. Define

$$\begin{aligned} Y_1 &:= \{y_1, \ldots, y_{2L(X)}\}, \\ Y_2 &:= Y \cap \{y_{2L(X)} + 1, y_{2L(X)} + 2, \ldots, y_{2L(X)} + L(X)\}, \\ Y_3 &:= \{y \in Y : \ y > y_{2L(X)} + L(X)\}, \end{aligned}$$

and notice that $Y = Y_1 \cup Y_2 \cup Y_3$ where the right-hand side is a disjoint union. Furthermore, since $\max Y_1 + L(X) < \min Y_3$, $X + Y_1$ and $X + Y_3$ are disjoint, and hence

$$|X + Y| \geq |X + Y_1| + |X + Y_3|. \tag{17}$$

Insomuch as $L(X) - |X| + 2 \leq |X|$, X has two consecutive numbers and thereby $\mathrm{GCD}^*(X) = 1$.

Now we bound $|X + Y_1|$. We have that

$$L(Y_1) \geq |Y_1| = 2L(X) > L(X).$$

Since Y is $X-$sparse and $L(Y_1) \geq 2L(X)$, we get that

$$L(Y_1) - |Y_1| \geq |X|. \tag{18}$$

Suppose that $\mathrm{GCD}^*(Y_1) > 1$. Then we can apply Proposition 2.1 (i) to X and Y_1, and it yields

$$|X + Y_1| \geq |X| + |Y_1| + |Y_1| - 2 = |X| + |Y_1| + 2L(X) - 2;$$

furthermore, since $L(X) \geq |X|$,

$$|X + Y_1| \geq |X| + |Y_1| + |X| - 2.$$

Suppose that $\mathrm{GCD}^*(Y_1) = 1$. Then we are able to apply Proposition 2.1 (ii) to X and Y_1, and it implies that

$$|X + Y_1| \geq |X| + |Y_1| + \min\{|X| - 2, L(Y_1) - |Y_1| - 1\};$$

furthermore, (18) leads to

$$|X + Y_1| \geq |X| + |Y_1| + |X| - 2.$$

Thus, in any case, we have that

$$|X + Y_1| \geq |X| + |Y_1| + |X| - 2. \tag{19}$$

Also we need to bound $|X + Y_3|$. Since $|Y| \geq 5L(X)$, we conclude that $|Y_3| = |Y| - |Y_1| - |Y_2| \geq 2L(X)$. Insomuch as $L(Y_3) \geq |Y_3| \geq 2L(X) > L(X)$ and Y is $X-$sparse, we notice that

$$L(Y_3) - |Y_3| \geq |X|. \tag{20}$$

Suppose that $\mathrm{GCD}^*(Y_3) > 1$. Then the assumptions of Proposition 2.1 (i) are fulfilled by X and Y_3, and it yields

$$|X + Y_3| \geq |X| + |Y_3| + |Y_3| - 2 \geq |X| + |Y_3| + 2L(X) - 2;$$

thereby, since $L(X) \geq |X|$,

$$|X + Y_3| \geq |X| + |Y_3| + |X| - 2.$$

Suppose that $\mathrm{GCD}^*(Y_3) = 1$. Then we can apply Proposition 2.1 (ii) to X and Y_3, and it leads to

$$|X + Y_3| \geq |X| + |Y_3| + \min\{|X| - 2, L(Y_3) - |Y_3| - 1\};$$

moreover, (20) implies that $|X + Y_1| \geq |X| + |Y_3| + |X| - 2$. In any case, we have that

$$|X + Y_3| \geq |X| + |Y_3| + |X| - 2. \tag{21}$$

Finally

$$\begin{aligned}
|X + Y| &\geq |X + Y_1| + |X + Y_3| && \Big(\text{by (17)}\Big)\\
&\geq |Y_1| + |Y_3| + 4|X| - 4 && \Big(\text{by (19) and (21)}\Big)\\
&\geq |X| + |Y| + 4|X| - 4 - L(X) && \Big(\text{since } |Y_2| \leq L(X)\Big)\\
&\geq |X| + |Y| + 2|X| - 2 && \Big(\text{since } L(X) - |X| + 2 \leq |X|\Big)
\end{aligned}$$

concluding the proof. □

Before we state the principal result of this section, we need a technical lemma.

Lemma 4.3. *Let A and B be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ and let $b \in \mathbb{Z}/p\mathbb{Z}$ be such that $B \subseteq \big[\overline{0}, b\big]$ and $2l(A) \leq \big|\big[\overline{0}, b\big]\big| < |A| + |B|$. Then there is $c \in \mathbb{Z}/p\mathbb{Z}$ such that $\Big[c, c + \overline{l(A) - 1}\Big] \subseteq A + B$.*

Proof. Let $a, a' \in \mathbb{Z}/p\mathbb{Z}$ be such that $A \subseteq [a', a]$ and $|[a', a]| = l(A)$; translating A if necessary, assume that $a' = \overline{0}$.

Since $\big|\big[\overline{0}, b\big]\big| \geq 2l(A) = 2\big|\big[\overline{0}, a\big]\big|$, we get that

$$|[a, b]| \geq l(A). \tag{22}$$

Define $C := [a, b] \setminus (A + B)$. We shall show that $C = \emptyset$. Assume that there exists $c \in C$. Since $C \subseteq \mathbb{Z}/p\mathbb{Z} \setminus (A + B)$, we get that $c - A \subseteq \mathbb{Z}/p\mathbb{Z} \setminus B$. Insomuch as $c \in [a, b]$, $c - \big[\overline{0}, a\big] \subseteq \big[\overline{0}, b\big]$. Thus $c - A \subseteq \big[\overline{0}, b\big] \setminus B$, and therefore

$$|A| = |c - A| \leq \big|\big[\overline{0}, b\big] \setminus B\big|$$

contrary to hypothesis. Then $C = \emptyset$ and consequently $[a, b] \subseteq A + B$. From (22), we conclude that

$$\Big[a, a + \overline{l(A) - 1}\Big] \subseteq [a, b] \subseteq A + B,$$

and therefore a satisfies the desired property. □

We conclude this section with the following lemma.

Lemma 4.4. *Let (A, B, C) be a trio of $\mathbb{Z}/p\mathbb{Z}$ and $r \in \mathbb{Z}$. Assume*

- $|A| \geq r + 3$.
- $\min\{|B|, |C|\} \geq r + 4$.
- $r(A, B, C) \leq r$.
- $l(A) \leq |A| + r + 1$.
- *B or C is not $A-$sparse.*

Then $l(B) \leq |B| + r + 1$ and $l(C) \leq |C| + r + 1$.

Proof. Assume without loss of generality that B is not $A-$sparse (otherwise we swap B and C in the proof). Insomuch as B is not $A-$sparse, there exist $a, b \in \mathbb{Z}/p\mathbb{Z}$ such that

$$|[a, b]| \geq 2l(A) \qquad \text{and} \qquad |[a, b] \setminus B| < |A|.$$

Translating A and B if necessary, we assume that $a = \overline{0}$. Set $D := \big[\overline{0}, b\big] \cap B$; thus $D \subseteq \big[\overline{0}, b\big]$ and $\big|\big[\overline{0}, b\big] \setminus D\big| < |A|$. Hence we can apply Lemma 4.3 to the sets A, D and $\big[\overline{0}, b\big]$, and it implies the existence of $c \in \mathbb{Z}/p\mathbb{Z}$ such that $\Big[c, c + \overline{l(A) - 1}\Big] \subseteq A + D \subseteq A + B$. Hence

$$\mathbb{Z}/p\mathbb{Z} \setminus -(A + B) \subseteq \Big[-c + \overline{1}, -c + \overline{p - l(A)}\Big];$$

in particular,

$$l(\mathbb{Z}/p\mathbb{Z} \setminus -(A + B)) \leq p - l(A). \tag{23}$$

Since (A, B, C) is a trio, $C \subseteq \mathbb{Z}/p\mathbb{Z} \setminus -(A + B)$. Then (23) leads to $l(A) + l(C) \leq p$. Finally we can apply Corollary 2.3 to (A, B, C), and we are done. □

5. Proof of Theorem 1.3

In this section we conclude the proof of Theorem 1.3.

Proof. (Theorem 1.3) Assume without loss of generality that $d = \overline{1}$ (otherwise we make a dilation by d^{-1} to A, B and C). Also assume without loss of generality that $|B| = \max\{|A|, |B|, |C|\}$ (otherwise we swap B and C in the proof). Let $a', a \in \mathbb{Z}/p\mathbb{Z}$ be such that $A \subseteq [a', a]$ and $l(A) = |[a', a]|$. Translating A if necessary, assume that $a' = \overline{0}$. Also, translating B if necessary, assume that $\overline{p-1} \notin A + B$. Define $B' := B \cap \big[\overline{0}, \overline{p-2} - a\big]$. Insomuch as $B' \subseteq \big[\overline{0}, \overline{p-2} - a\big]$,

$$l(A) + l(B') \leq p. \tag{24}$$

Inasmuch as $\overline{p-1} \notin A + B$, we have that $(\overline{p-1} - A) \cap B = \emptyset$. Hence

$$B \cap \big[\overline{p-1} - a, \overline{p-1}\big] \subseteq \overline{p-1} - \big([\overline{0}, a] \setminus A\big),$$

and therefore, since $l(A) \leq |A| + r + 1$, we have

$$|B'| \geq |B| - \big|[\overline{0}, a] \setminus A\big| \geq |B| - r - 1. \tag{25}$$

Let X and Y be the subsets of Γ such that $\overline{X} = A$ and $\overline{Y} = B'$. From (24), $X + Y \subseteq \Gamma$. Since $\overline{X + Y} = A + B'$,

$$|X + Y| = |A + B'|. \tag{26}$$

Notice that if $|A| \geq 2r + 4$, the claim follows from Corollary 3.1 (recall that $-1 \leq r(A, B, C) \leq r$ by Cauchy-Davenport Theorem so $p \geq 35r + 45 > 10r + 18$). Thus, from now on, we assume that

$$|A| \leq 2r + 3. \tag{27}$$

Then

$$\begin{aligned} |B| \geq \frac{|B| + |C|}{2} &\geq \frac{p - |A| - r}{2} \\ &\geq \frac{p - 3r - 3}{2} && \Big(\text{by (27)}\Big) \\ &\geq 16r + 21. \end{aligned} \tag{28}$$

Thus

$$\begin{aligned} |Y| = |B'| &\geq |B| - r - 1 && \Big(\text{by (25)}\Big) \\ &\geq 15r + 20 && \Big(\text{by (28)}\Big) \\ &\geq 5|A| + 5r + 5 && \Big(\text{by (27)}\Big) \\ &\geq 5l(A) && \Big(\text{since } l(A) \leq |A| + r + 1\Big) \\ &= 5L(X). \end{aligned} \tag{29}$$

Notice that

$$\begin{aligned} L(X) - |X| + 2 = l(A) - |A| + 2 &\leq r + 3 \qquad \Big(\text{since } l(A) \leq |A| + r + 1\Big) \\ &\leq |A| \\ &= |X|. \end{aligned} \tag{30}$$

We shall show that B is not $A-$sparse. Assume that B is $A-$sparse. Then B' is $A-$sparse insomuch as $B' \subseteq B$. From (29), we have that $L(Y) \geq |Y| \geq 5L(X)$; thus we can apply Remark 4.1 to X and Y, and then we conclude that Y is $X-$sparse. Furthermore, since Y is $X-$sparse, (29) and (30) imply that we can apply Lemma 4.2 to X and Y. Next

$$\begin{aligned} r \geq r(A,B,C) &\geq |A+B| - |A| - |B| \qquad \Big(\text{since } (A,B,C) \text{ is a trio}\Big) \\ &\geq |A+B'| - |A| - |B| \qquad \Big(\text{since } B' \subseteq B\Big) \\ &= |X+Y| - |X| - |B| \qquad \Big(\text{by (26)}\Big) \\ &\geq 2|X| - 2 + |Y| - |B| \qquad \Big(\text{by Lemma 4.2}\Big) \\ &= 2|A| - 2 + |B'| - |B| \\ &\geq 2|A| - r - 3, \qquad \Big(\text{by(25)}\Big) \\ &\geq r + 3. \end{aligned}$$

and this contradiction shows B is not $A-$sparse. Now, insomuch as B is not $A-$sparse, all the conditions of Lemma 4.4 are satisfied by (A,B,C), and this concludes the proof. □

Acknowledgements. We thank the referee for his useful suggestions to improve this paper and also for letting us know about the existence of results that reduced considerably the length of our proofs.

References

[1] D. J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics 30 Springer, Switzerland, 2013.

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

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

[4] V. F. Lev and P. Y. Smeliansky, On addition of two distinct sets of integers, *Acta Arith.* **70** (1995), 85-91.

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