ACTA ARITHMETICA
XCII.3 (2000)

# An inverse theorem mod $p$

by

Yahya Ould Hamidoune (Paris) and Øystein J. Rødseth (Bergen)

**1. Introduction.** Let $p$ be a prime number. Let $A$ and $B$ be two nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$. We write $|A|$ for the number of elements in the set $A$. The *sumset* $A+B$ is the set of all sums $a+b$ where $a \in A$ and $b \in B$.

If there exist elements $a, d \in \mathbb{Z}/p\mathbb{Z}$ such that

$$A = \{a + id \mid i = 0, 1, \ldots, |A| - 1\},$$

then $A$ is an *arithmetic progression* with difference $d$ (or a *$d$-progression*). If $A$ is a $d$-progression with one term removed, then $A$ is an *almost-progression* with difference $d$ (or an *almost $d$-progression*). If $A$ is the union of two $d$-progressions, then $A$ is a *double-progression* with difference $d$ (or a *double $d$-progression*). Note that an arithmetic progression is also an almost-progression, and that an almost-progression is also a double-progression.

A basic result on sumsets mod $p$ is the following well known theorem.

Theorem 1 (Cauchy–Davenport). $|A+B| \geq \min(p, |A| + |B| - 1)$.

This theorem was proved by Cauchy [1] in 1813 and rediscovered by Davenport [3], [4]. Both proofs were transformation proofs. Cauchy used a transform which is essentially the transform called the "Dyson $e$-transform" by Mann [7, p. 5] and the "$e$-transform" by Nathanson [8, p. 42]. Davenport used a quite different transform.

The Cauchy–Davenport theorem is an example of a *direct* addition theorem mod $p$. The corresponding *inverse* problem is to describe the structure of those sets $A$, $B$ for which the cardinality of the sumset $A+B$ is small. The first nontrivial inverse theorem mod $p$ was found by Vosper [9]. The essential part of Vosper's theorem is as follows.

Theorem 2 (Vosper). *Suppose that* $|A|, |B| \geq 2$, *and that*

$$|A+B| = |A| + |B| - 1 \leq p - 2.$$

*Then $A$ and $B$ are arithmetic progressions with the same difference.*

---

2000 *Mathematics Subject Classification*: 11A07, 11B13.

Vosper first used the Davenport transform in the proof of this result. Later he presented in [10] a simpler proof using the $e$-transform. Another transform was used by Chowla, Mann, and Straus in [2], where they also gave a nice application of Vosper's theorem to diagonal forms over $\mathbb{Z}/p\mathbb{Z}$ (cf. [7, Chap. 2], [8, p. 57]).

In this paper we use, among other things, the Davenport transform to give an elementary proof of the following theorem, which goes one step beyond the theorems of Cauchy–Davenport and Vosper.

Theorem 3. *Suppose that* $|A|, |B| \geq 3$, *and that*

$$7 \leq |A+B| = |A| + |B| \leq p-4. \tag{1}$$

*Then $A$ and $B$ are almost-progressions with the same difference.*

This can again be seen to imply the following: Suppose that $|A|, |B| \geq 3$, and that (1) holds. Then one of $A$ and $B$ is a $d$-progression while the other is an almost $d$-progression, or that $A = \{a, a+2d, a+3d, \ldots, a+|A|d\}$ and $B = \{b, b+2d, b+3d, \ldots, b+|B|d\}$ for some $a, b, d \in \mathbb{Z}/p\mathbb{Z}$.

Using exponential sums and analytic methods, Freiman [5], [6] proved a beautiful inverse theorem for sumsets of the special form $A + A$ (cf. [8, Theorem 2.11]).

Theorem 4 (Freiman). *Let $r$ be an integer*, $0 \leq r \leq \frac{2}{5}|A| - 2$. *If*

$$|A+A| = 2|A| - 1 + r \quad \textit{and} \quad |A| \leq p/35,$$

*then $A$ is contained in an arithmetic progression with $|A| + r$ elements.*

For certain applications it is of interest to relax the condition $|A| \leq p/35$. If $r = 0$, Theorem 2 shows that this condition can be replaced by $|A| \leq \frac{1}{2}(p-1)$. If $r = 1$, Theorem 3 shows that the condition can be replaced by $|A| \leq \frac{1}{2}(p-5)$.

**2. Preliminaries.** Throughout this paper $A$ and $B$ will be nonempty sets of residue classes modulo $p$. The sumset $A+B$ was defined in Section 1. We put $2B = B + B$. We write $A - B$ for the set of differences $a - b$, $a \in A$, $b \in B$, and we also put $x \pm B = \{x\} \pm B$ for a residue class $x$. We write $A \setminus B$ for the complement of $B$ in $A$. If $r$ is an integer, we shall on some occasions feel free to write $r$ for the residue class modulo $p$ represented by $r$.

For residue classes $x \neq 0$ and $y$, the set $x * A + y = \{xa + y \mid a \in A\}$ is an affine image of $A$. Most of the results below on sumsets $A + B$ are such that if there are residue classes $x \neq 0, y, z$ such that a result holds for the affine images $x * A + y$ and $x * B + z$, then the result is also true for the sets $A, B$. This is the reason why it is on many occasions sufficient to prove a result for some special choice of an affine image of $A$ or $B$.

We shall say that a nonempty set $Y \subseteq A$ is a *d-component* of $A$ if $Y$ is a maximal $d$-progression contained in $A$. Thus $Y \neq \emptyset$ is a $d$-component of $A$ if and only if the following two conditions hold:

(i) $Y$ is a $d$-progression,
(ii) if $C$ is a $d$-progression such that $Y \subseteq C \subseteq A$, then $Y = C$.

Clearly, a set $A$ has a unique partition into $d$-components. By considering the residue classes mod $p$ as points on a circle, one readily makes the following observations:

(I) $|\{0,1\} + A| \le |A| + 1$ if and only if $A$ is a 1-progression.
(II) $|\{0,1\} + A| \le |A| + 2$ if and only if $A$ is a double 1-progression.
(III) If $|A| \le p - 3$, then $|\{0,1,2\} + A| \le |A| + 2$ if and only if $A$ is a 1-progression.
(IV) If $|A| \le p - 4$, then $|\{0,1,2\} + A| \le |A| + 3$ if and only if $A$ is an almost 1-progression.
(V) If $|A| \le p - 1$, then $|\{0,1\} + A| = |A| + k$, where $k$ is the number of 1-components of $A$.

Lemma 1. *Let $|B| \ge 3$, and suppose that*

$$|A + B| \le |A| + |B| \le p - 1. \tag{2}$$

*Also assume that $B$ is a $d$-progression. Then $A$ is an almost $d$-progression.*

Proof. It is sufficient to prove the result for $d = 1$, and we can assume that $B = \{0,1,\ldots,|B|-1\}$. Then $B = \{0,1,2\} + B'$, where $B' = \{0,1,\ldots,|B|-3\}$. By (2) and Theorem 1, we have

$$p-1 \ge |A| + |B| \ge |A+B| = |A + \{0,1,2\} + B'| \ge |A + \{0,1,2\}| + |B'| - 1,$$

and since $|B'| = |B| - 2$, we have $|A + \{0,1,2\}| \le |A| + 3$. By (2), we also have $|A| \le p-4$. Hence, by observation (IV), $A$ is an almost 1-progression. ∎

Lemma 2. *Let $|B| \ge 2$, and suppose that*

$$|A + B| \le |A| + |B| \le p - 1. \tag{3}$$

*Also assume that $B$ is a $d$-progression. Then $A$ is a double $d$-progression.*

Proof. If $|B| \ge 3$, this is clear by Lemma 1. If $|B| = 2$, we can assume that $B = \{0,1\}$. Then, by (3), we have $|A + \{0,1\}| \le |A| + 2$, and $A$ is a double 1-progression by observation (II). ∎

Lemma 3. *Suppose that $A + B$ is a $d$-progression such that*

$$|A + B| \le |A| + |B| \le p - 3. \tag{4}$$

*Then $A$ is an almost $d$-progression.*

Proof. We prove the result for $d = 1$. Using (4), observation (III), and Theorem 1, we get

$$\begin{aligned} p - 1 &\geq |A| + |B| + 2 \geq |A + B| + 2 \geq |\{0, 1, 2\} + A + B| \\ &\geq |\{0, 1, 2\} + A| + |B| - 1, \end{aligned}$$

so that $|\{0, 1, 2\} + A| \leq |A| + 3$, and the result follows by observation (IV). ■

**3. An inverse theorem.** In this section we prove the following inverse theorem mod $p$.

THEOREM 5. *Suppose that $|B| \geq 2$, and that*

$$|A + B| = |A| + |B| \leq p - 4. \tag{5}$$

*Then $A$ is a double-progression.*

Proof. Suppose that there exist pairs $(A, B)$ such that $|B| \geq 2$, (5) is satisfied, and $A$ is not a double-progression. Choose such a pair where $|B|$ is minimal. It is no restriction to assume $0 \in B$. Then $A + B \subseteq A + 2B$. Since $A + B \neq \mathbb{Z}/p\mathbb{Z}$ and $B$ generates $\mathbb{Z}/p\mathbb{Z}$, we have $A + B \neq A + 2B$. Putting

$$X = (A + 2B) \setminus (A + B),$$

we thus have $X \neq \emptyset$.

For $x \in X$, let

$$B_x^* = \{b \in B \mid x - b \in A + B\}, \qquad B_x = B \setminus B_x^*.$$

Then $0 \notin B_x^* \neq \emptyset$, and $0 \in B_x \neq B$. (Here $B_x$ is the transform of $B$ employed by Davenport in his proof of Theorem 1.)

Moreover, it is easily seen that

$$(A + B_x) \cup (x - B_x^*) \subseteq A + B, \qquad (A + B_x) \cap (x - B_x^*) = \emptyset,$$

so that

$$|A + B| \geq |A + B_x| + |x - B_x^*| = |A + B_x| + |B| - |B_x|.$$

Thus we have

$$p - 4 \geq |A| + |B| = |A + B| \geq |A + B_x| + |B| - |B_x|,$$

so that

$$|A + B_x| \leq |A| + |B_x| \leq p - 5.$$

By the minimality of $|B|$, we thus have $B_x = \{0\}$ for any $x \in X$. Hence

$$B_x^* = B' \qquad (x \in X),$$

where $B' = B \setminus \{0\}$.

Thus $X - B' \subseteq A + B$, and we see that

$$A \cup (X - B') \subseteq A + B \quad \text{and} \quad A \cap (X - B') = \emptyset.$$

Hence, using (5) and Theorem 1, we get

$$|A|+|B|=|A+B|\ge|A|+|X-B'|\ge|A|+|X|+|B|-2,$$

that is, $|X|\le 2$.

Now we have

$$2\ge|X|=|A+2B|-|A+B|\ge|A+2B|-(p-4),$$

so that $|A+2B|\le p-2$. By Lemma 2, $B$ is not an arithmetic progression. Since $|A+B|\ge 2$, Theorems 1 and 2 thus give

$$|A+2B|\ge|A+B|+|B|,$$

so that

$$2\ge|X|=|A+2B|-|A+B|\ge|B|,$$

which contradicts the fact that $B$ is not an arithmetic progression. ■

## 4. More lemmas

LEMMA 4. *Suppose that* $|A|\ge 3$, *and that*

$$|A+B|=|A|+|B|\le p-4. \tag{6}$$

*Also assume that $A$ is a double* 1*-progression. Then one of the following holds.*

(i) *$B$ is a double* 1*-progression.*

(ii) *$A$ and $B$ are almost-progressions with the same difference.*

(iii) $|A|=3$, *$B$ has three* 1*-components* $B_1,B_2,B_3$, *and there exists an $a\in A$ such that $A+B$ has the three* 1*-components* $a+\{0,1\}+B_i$, $i=1,2,3$.

Proof. If $A$ is a $d$-progression, then, by Lemma 1, $B$ is an almost $d$-progression. We therefore assume that $A$ is not a $d$-progression for any $d$. In particular, $A$ has two 1-components $A_1$, $A_2$, $|A_1|\le|A_2|$.

We also assume that (i) is false, so that $B$ is not a double 1-progression. Thus $B$ has at least three 1-components, and by observation (V),

$$|\{0,1\}+B|\ge|B|+3. \tag{7}$$

We look separately at the cases $|A_1|\ge 2$ and $|A_1|=1$.

CASE 1: $|A_1|\ge 2$. Then $A=\{0,1\}+A'$, where $|A'|=|A|-2\ge 2$. By (6), Theorem 1, and (7), we have

$$\begin{aligned}p-4\ge|A|+|B|=|A+B|&=|A'+\{0,1\}+B|\\&\ge|A'|+|\{0,1\}+B|-1\ge|A|+|B|,\end{aligned}$$

so that

$$|A'+(\{0,1\}+B)|=|A'|+|\{0,1\}+B|-1\le p-4.$$

Hence, by Theorem 2, both $A'$ and $\{0,1\}+B$ are $d$-progressions for some $d$. Thus $A+B=A'+\{0,1\}+B$ is a $d$-progression, and, by Lemma 3, (ii) holds.

Case 2: $|A_1| = 1$. Then there is an $a \in A$ such that $A_2 = a + \{0,1,\ldots,|A|-2\}$. Thus $A_2 = \{0,1\}+A_2'$, where $A_2' = a+\{0,1,\ldots,|A|-3\}$ and $|A_2'| = |A|-2$.

By (6), Theorem 1, and (7), we have

$$\begin{aligned} p-4 &\ge |A|+|B| = |A+B| \ge |A_2+B| = |A_2'+\{0,1\}+B| \\ &\ge |A_2'|+|\{0,1\}+B|-1 \ge |A|-2+|B|+3-1 = |A|+|B|. \end{aligned}$$

We see that $A+B=A_2+B$. We also have $|\{0,1\}+B| = |B|+3$, so that, by observation (V), $B$ has three 1-components $B_1,B_2,B_3$. Moreover,

$$p-4 \ge |A_2'+\{0,1\}+B| = |A_2'|+|\{0,1\}+B|-1.$$

If $|A|\ge 4$, then $|A_2'|\ge 2$. Hence by Theorem 2, both $A_2'$ and $\{0,1\}+B$ are $d$-progressions. Thus $A+B=A_2+B=A_2'+\{0,1\}+B$ is a $d$-progression, and by Lemma 3, (ii) holds.

Finally, suppose that $|A|=3$. Then $A$ is not an arithmetic progression. If

$$|\{0,1\}+A+B| \le |A+B|+2,$$

we thus have by (6), Theorems 1 and 2, and (7),

$$\begin{aligned} p-2 &\ge 3+|B|+2 = |A+B|+2 \ge |\{0,1\}+A+B| \\ &\ge |A|+|B+\{0,1\}| \ge 3+|B|+3, \end{aligned}$$

a contradiction. Hence,

$$|\{0,1\}+A+B| \ge |A+B|+3,$$

and, by observation (V), $A+B$ has at least three 1-components. Now, $A+B = A_2+B = a+\{0,1\}+B = \bigcup_{i=1}^{3}(a+\{0,1\}+B_i)$. Since each set $a+\{0,1\}+B_i$ is a 1-progression, $A+B$ has the three 1-components $a+\{0,1\}+B_i$, $i=1,2,3$. ∎

Lemma 5. *Let $|A|,|B|\ge 3$, and suppose that*

$$7 \le |A+B| = |A|+|B| \le p-4.$$

*Also assume that $A$ is an almost-progression. Then $A$ and $B$ are almost-progressions with the same difference.*

Proof. Suppose that $A$ is an almost 1-progression, and that $A$ and $B$ are not almost-progressions with the same difference. By Lemma 1, neither $A$ nor $B$ is an arithmetic progression. In particular, $A$ has two 1-components $A_1, A_2$, $|A_1|\le|A_2|$. We look separately at cases (i) and (iii) in Lemma 4.

We first consider (i). Then $B$ is a double 1-progression. Since $B$ is not an arithmetic progression, it has two 1-components $B_1, B_2$, $|B_1| \le |B_2|$. Since $|B| \ge 3$, we have $|B_2| \ge 2$.

We have

$$A + B = (A_1 + B_1) \cup (A_2 + B_1) \cup (A + B_2). \tag{8}$$

Both $A_1 + B_1$ and $A_2 + B_1$ are 1-progressions. Since $A$ is an almost 1-progression and $B_2$ is a 1-progression with at least two elements, we also find that $A+B_2$ is a 1-progression. Thus $A+B$ has at most three 1-components.

By Lemma 3, $A+B$ has at least two 1-components. Thus $A+B$ has two or three 1-components. If they are three, then they are given in (8). Then we must have $|B_1| = 1$, for otherwise $(A_1+B_1)\cup(A_2+B_1) = A+B_1$ would be a 1-progression. We have

$$|A + B_2| = |A| + |B_2| = |A| + |B| - 1,$$

and

$$\begin{aligned} |A| + |B| = |A + B| &= |A_1 + B_1| + |A_2 + B_1| + |A + B_2| \\ &= |A_1| + |A_2| + |A| + |B| - 1 = 2|A| + |B| - 1 \ge |A| + |B| + 2, \end{aligned}$$

a contradiction. Thus $A + B$ has two 1-components.

By observation (V), we have $|\{0,1\}+A| = |A|+2$ and $|\{0,1\}+A+B| = |A+B|+2$, so that

$$p - 2 \ge |\{0,1\} + A| + |B| = |A| + |B| + 2 = |A + B| + 2 = |\{0,1\} + A + B|;$$

that is,

$$|\{0,1\} + A + B| = |\{0,1\} + A| + |B| \le p - 2.$$

Since $A$ is an almost 1-progression, $\{0,1\} + A$ is a 1-progression. It follows by Lemma 1 that $B$ is an almost 1-progression, which is a contradiction.

We now consider case (iii) of Lemma 4. Then $|A| = 3$ and $|B| \ge 4$. Let the three components of $B$ satisfy $|B_1| \le |B_2| \le |B_3|$. Then $|B_3| \ge 2$, and $A+B_3$ is a 1-progression contained in some 1-component $a+\{0,1\}+B_i$ of $A+B$. Thus we have

$$1 + |B_i| = |a + \{0,1\} + B_i| \ge |A + B_3| = 3 + |B_3|,$$

a contradiction. ∎

Lemma 6. *Let* $|A|, |B| \ge 3$, *and suppose that*

$$|A + B| = |A| + |B| \le p - 4. \tag{9}$$

*Also assume that both* $A$ *and* $B$ *are double* 1*-progressions, and that* $B$ *is not an almost* 1*-progression. Let* $A_1$ *be a* 1*-component of* $A$, *and let* $B_1$, $B_2$ *be the two* 1*-components of* $B$. *Then* $A_1 + B_1$ *and* $A_1 + B_2$ *lie in distinct* 1*-components of* $A + B$. *Moreover*,

$$|A_1| \ge \tfrac{1}{2}|A| - 1. \tag{10}$$

Proof. By Lemma 1, $A$ is not a 1-progression. Thus $A$ has one more 1-component $A_2 = A \setminus A_1$.

Suppose that $A_1 + B_1$ and $A_1 + B_2$ are contained in one 1-component $C$ of $A + B$. We can assume that $A_1 = \{0, 1, \ldots, |A_1| - 1\}$. Since $C$ is a 1-progression containing $A_1 + B$ and $B$ is not an almost-progression, it is then easy to see that

$$|C| \geq |A_1| + |B| + 1. \tag{11}$$

If $C = A + B$, then $A + B$ is a 1-progression, so that, by Lemma 3, $B$ is an almost 1-progression, a contradiction. Thus $A + B$ contains a 1-component $C' \neq C$.

We have

$$A + B = (A_1 + B_1) \cup (A_1 + B_2) \cup (A_2 + B_1) \cup (A_2 + B_2),$$

where $(A_1 + B_1) \cup (A_1 + B_2) \subseteq C$, and both $A_2 + B_1$ and $A_2 + B_2$ are 1-progressions. Either for $i = 1$ or for $i = 2$, we have $A_2 + B_i \subseteq C'$, so that, by (9), (11), and Theorem 1,

$$\begin{aligned} p - 4 &\geq |A| + |B| \geq |C| + |C'| \geq |A_1| + |B| + 1 + |A_2 + B_i| \\ &\geq |A_1| + |B| + 1 + |A_2| + |B_i| - 1 = |A| + |B| + |B_i|, \end{aligned}$$

hence $|B_i| \leq 0$, a contradiction. Thus $A_1 + B_1$ and $A_1 + B_2$ lie in distinct 1-components of $A + B$.

Moreover, by Theorem 1, we now have

$$p - 4 \geq |A| + |B| = |A + B| \geq |A_1 + B_1| + |A_1 + B_2| \geq 2|A_1| + |B| - 2,$$

so that $|A| \geq 2|A_1| - 2$. This also holds for the other 1-component $A_2 = A \setminus A_1$ of $A$, so that $|A| \geq 2|A \setminus A_1| - 2$, and (10) follows. ∎

Lemma 7. *Let $|A|, |B| \geq 3$, and suppose that*

$$7 \leq |A + B| = |A| + |B| \leq p - 4.$$

*Let $A_1, A_2$ be the distinct 1-components of $A$, and let $B_1$, $B_2$ be the distinct 1-components of $B$. Also suppose that $B$ is not an almost $d$-progression for any $d$. The 1-components of $A + B$ are then $(A_1 + B_1) \cup (A_2 + B_2)$ and $(A_2 + B_1) \cup (A_1 + B_2)$.*

Proof. We can assume that $|A_1| \geq |A_2|$ and $|B_1| \geq |B_2|$. By Lemma 6, $A_1 + B_1$ and $A_1 + B_2$ lie in distinct 1-components of $A + B$, so that $A + B$ has at least two 1-components.

Suppose that $A+B$ has at least three 1-components. A third 1-component must then contain $A_2 + B_i$ for $i = 1$ or 2, and using Theorem 1, we get

$$\begin{aligned} p - 4 &\geq |A| + |B| \geq |A_1 + B_1| + |A_1 + B_2| + |A_2 + B_i| \\ &\geq |A_1| + |B_1| - 1 + |A_1| + |B_2| - 1 + |A_2| + |B_i| - 1 \\ &\geq |A| + |B| + |A_1| + |B_2| - 3, \end{aligned}$$

so that

$$|A_1| + |B_2| \le 3. \tag{12}$$

By Lemma 5, since $B$ is not an almost-progression, neither is $A$. Hence, by symmetry, we also have

$$|A_2| + |B_1| \le 3, \tag{13}$$

and adding (12) and (13), we get $|A| + |B| \le 6$, which is against the hypotheses. Therefore, $A + B$ has exactly two distinct 1-components $C_1, C_2$.

Assume that $A_1 + B_1 \subseteq C_1$ and $A_1 + B_2 \subseteq C_2$. By Lemma 6, $A_1 + B_1$ and $A_2 + B_1$ lie in distinct 1-components of $A + B$. Thus $A_2 + B_1 \subseteq C_2$. Similarly, $A_2 + B_2 \subseteq C_1$. ∎

LEMMA 8. *Let $|A|, |B| \ge 3$, and suppose that*

$$7 \le |A + B| = |A| + |B| \le \min(p - 4, 8).$$

*Then $B$ is an almost-progression.*

Proof. By Lemma 5, if $A$ is an almost-progression, so is $B$. Therefore it is sufficient to show that one of $A$ and $B$ is an almost-progression. We can assume $|A| \ge |B|$. Then $|A| \ge 4$. Also assume that neither $A$ nor $B$ is an almost-progression.

By Theorem 5, $A$ is a double $d$-progression for some $d$. We can assume that $d = 1$. Thus $A$ is a double 1-progression. By Lemma 4, so is $B$.

After some suitable affine transformations of $A$ and $B$, we get to consider the following cases.

CASE I: $|A| = 4, |B| = 3$.

CASE I.1: $A = \{0, 1, 2, u\}, B = \{0, 1, v\}$. By Lemma 7, $A + B$ has the two 1-components

$$C_1 = \{0, 1, 2, 3\} \cup \{u + v\}, \quad C_2 = \{u, u + 1\} \cup \{v, v + 1, v + 2\}.$$

We have $|C_1| + |C_2| = |A + B| = |A| + |B| = 7$. Since $p \ge 11$, we have $|C_1| \ge 4$ and $|C_2| \ge 3$; thus $|C_1| = 4$ and $|C_2| = 3$. By looking at $C_1$, we see that $u + v = 0, 1, 2$, or 3. From $C_2$, we see that $u = v$ or $u = v + 1$.

If $u = v$, then $2v = 0, 1, 2$, or 3. Since $v \ne 0, 1$, we have $v = 1/2$ or $v = 3/2$, and

$$B = \{0, 1/2, 1\} = \{0, d, 2d\} \quad \text{or} \quad B = \{0, 1, 3/2\} = \{0, 2d, 3d\},$$

where $d = (p + 1)/2$. This contradicts the fact that $B$ is not an almost-progression.

If $u = v + 1$, then $2v + 1 = 0, 1, 2$, or 3, so that $v = \pm 1/2$. Thus $B = \{-1/2, 0, 1\} = \{b, b + d, b + 3d\}$ for $b = (p - 1)/2, d = (p + 1)/2$, or $B = \{0, 1/2, 1\}$, and again we have reached a contradiction.

CASE I.2: $A = \{0, 1, u, u + 1\}$, $B = \{0, 1, v\}$. By Lemma 7, $A + B$ has the two 1-components

$$C_1 = \{0, 1, 2\} \cup \{u + v, u + v + 1\}, \quad C_2 = \{u, u + 1, u + 2\} \cup \{v, v + 1\}.$$

We still have $|C_1| + |C_2| = 7$. By symmetry, we can assume that $|C_1| \ge |C_2|$. Then $|C_1| = 4, |C_2| = 3$. We see that $u + v = -1$ or $2$, and that $u = v$ or $u = v - 1$. If $u = v$, we find that $B = \{-1/2, 0, 1\}$, a contradiction. If $u = v - 1$, then $B = \{0, 1, 3/2\}$, which is also a contradiction.

CASE II: $|A| = 5$, $|B| = 3$. Let $A_1, A_2$ be the two 1-components of $A$, $|A_1| \le |A_2|$. By Lemma 6, we then have $|A_1| \ge \frac{1}{2}|A| - 1 = 3/2$, so that $|A_1| \ge 2$; hence $|A_1| = 2$ and $|A_2| = 3$. Thus we can assume that

$$A = \{0, 1, 2, u, u + 1\}, \quad B = \{0, 1, v\}.$$

By Lemma 7, $A + B$ then has the two 1-components

$$C_1 = \{0, 1, 2, 3\} \cup \{u + v, u + v + 1\}, \quad C_2 = \{u, u + 1, u + 2\} \cup \{v, v + 1, v + 2\}.$$

We have $|C_1| + |C_2| = |A + B| = |A| + |B| = 8$. Clearly, we also have $|C_1| \ge 4$, $|C_2| \ge 3$.

CASE II.1: $|C_1| = 5$, $|C_2| = 3$. We have $u + v = -1$ or $3$, and $u = v$. Then $B = \{-1/2, 0, 1\}$ or $B = \{0, 1, 3/2\}$, a contradiction.

CASE II.2: $|C_1| = |C_2| = 4$. We have $u + v = 0, 1$, or $2$, and $u = v \pm 1$. If $u = v - 1$, we have $B = \{0, 1/2, 1\}$ or $B = \{0, 1, 3/2\}$, a contradiction. If $u = v + 1$, we have $B = \{-1/2, 0, 1\}$ or $B = \{0, 1/2, 1\}$, a contradiction.

CASE III: $|A| = |B| = 4$.

CASE III.1: $A = \{0, 1, 2, u\}$, $B = \{0, 1, 2, v\}$. By Lemma 7, $A + B$ has the two 1-components

$$C_1 = \{0, 1, 2, 3, 4\} \cup \{u + v\}, \quad C_2 = \{u, u + 1, u + 2\} \cup \{v, v + 1, v + 2\}.$$

We have $|C_1| + |C_2| = 8, |C_1| \ge 5, |C_2| \ge 3$, so that $|C_1| = 5, |C_2| = 3$. Thus $u + v = 0, 1, 2, 3$, or $4$, and $u = v$. It follows that $v = 1/2$ or $3/2$, so that $B = \{0, 1/2, 1, 2\}$ or $B = \{0, 1, 3/2, 2\}$, a contradiction.

CASE III.2: $A = \{0, 1, u, u + 1\}$, $B = \{0, 1, 2, v\}$. Similarly to Case III.1, we find that $B = \{0, 1/2, 1, 2\}$ or $B = \{0, 1, 3/2, 2\}$, a contradiction.

CASE III.3: $A = \{0, 1, u, u + 1\}$, $B = \{0, 1, v, v + 1\}$. By Lemma 7, $A + B$ has the two 1-components

$$C_1 = \{0, 1, 2\} \cup \{u + v, u + v + 1, u + v + 2\},$$
$$C_2 = \{u, u + 1, u + 2\} \cup \{v, v + 1, v + 2\}.$$

By symmetry, we can assume that $|C_1| \ge |C_2|$. We have $|C_1| + |C_2| = 8$, and $|C_2| \ge 3$.

Case III.3.1: $|C_1| = 5$, $|C_2| = 3$. We see that $u + v = \pm 2$, and that $u = v$. Thus $v = \pm 1$, which is impossible.

Case III.3.2: $|C_1| = |C_2| = 4$. We have $u + v = \pm 1$, and $u = v \pm 1$. If $u = v - 1$, we get $v = 0$ or 1, which is impossible. If $u = v + 1$, we get $v = -1$ or 0, which is also impossible. ∎

**5. Proof of Theorem 3, concluded.** Assume the theorem is false, and let $(A, B)$ be a counterexample with $|A| + |B|$ minimal and $|A| \geq |B|$. Then (1) holds, $|A| \geq 4$, $|B| \geq 3$, and $A$ and $B$ are not almost-progressions with the same difference. By Lemma 5, neither $A$ nor $B$ is an almost-progression.

By Theorem 5, $A$ is a double $d$-progression for some $d$. We can assume $d = 1$. Thus $A$ is a double 1-progression. By Lemma 4, so is $B$.

Let $A_1, A_2$ be the two 1-components of $A$. By Lemma 8, we have $|A| + |B| \geq 9$, so that $|A| \geq 5$. By Lemma 6, we have $|A_i| \geq \frac{1}{2}|A| - 1 \geq 3/2$, so that $|A_i| \geq 2$ for $i = 1, 2$. Hence, $A = \{0, 1\} + A'$, where $A'$ is a double 1-progression with $|A'| = |A| - 2 \geq 3$.

Let $k$ be the number of 1-components of $A' + B$. If $k = 1$, then $A' + B$ is a 1-progression, and so is $A + B = \{0, 1\} + A' + B$. By Lemma 3, $A$ is an almost-progression, a contradiction. Hence $k \geq 2$.

Since $|A'| \geq 3$ and $B$ is not an arithmetic progression, we have by (1), observation (V), and Theorems 1 and 2,

$$\begin{aligned} p - 4 \geq |A| + |B| = |A + B| &= |\{0, 1\} + A' + B| \\ &= |A' + B| + k \geq |A'| + |B| + k = |A| - 2 + |B| + k, \end{aligned}$$

so that $k \leq 2$; hence $k = 2$. It follows that

$$7 \leq |A' + B| = |A'| + |B| \leq p - 6.$$

We also have $|A'| \geq 3$, $|B| \geq 3$. By the minimality of $|A| + |B|$, we now deduce that $A'$ and $B$ are almost-progressions, a contradiction. ∎

## References


[1] A. L. Cauchy, *Recherches sur les nombres*, J. École Polytech. 9 (1813), 99–116.

[2] S. Chowla, H. B. Mann, and E. G. Straus, *Some applications of the Cauchy–Davenport theorem*, Norske Vid. Selsk. Forh. 32 (1959), 74–80.

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

[4] —, *A historical note*, ibid. 22 (1947), 100–101.

[5] G. A. Freiman, *Inverse problems of additive number theory. On the addition of sets of residues with respect to a prime modulus*, Dokl. Akad. Nauk SSSR 141 (1961), 571–573 (in Russian).

[6] —, *Inverse problems of additive number theory. On the addition of sets of residues with respect to a prime modulus*, Soviet Math. Dokl. 2 (1961), 1520–1522.

[7] H. B. Mann, *Addition Theorems*: *The Addition Theorems of Group Theory and Number Theory*, Interscience Publ., New York, 1965.

[8] M. B. Nathanson, *Additive Number Theory*: *Inverse Problems and the Geometry of Sumsets*, Springer, New York, 1996.

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

[10] —, *Addendum to "The critical pairs of subsets of a group of prime order"*, ibid. 31 (1956), 280–282.

E. Combinatoire
Université P. et M. Curie
4 Place Jussieu
75005 Paris, France
E-mail: yha@ccr.jussieu.fr

Department of Mathematics
University of Bergen
Johs. Brunsgt. 12
N-5008 Bergen, Norway
E-mail: rodseth@mi.uib.no

*Received on 16.4.1999*
*and in revised form on 30.9.1999* (3593)