Abstract

We prove that there exists an absolute constant $c > 0$ such that if an arithmetic progression $P$ modulo a prime number $p$ does not contain zero and has the cardinality less than $cp$, then it cannot be represented as a product of two subsets of cardinality greater than 1, unless $P = -P$ or $P = \{-2r, r, 4r\}$ for some residue $r$ modulo $p$.

1 Introduction

Let $\mathbb{F}_p$ be the field of residue classes modulo a prime number $p$. Given two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$, their sum-set $\mathcal{A} + \mathcal{B}$ and product-set $\mathcal{A}\mathcal{B}$ are defined as

$$\mathcal{A} + \mathcal{B} = \{a + b; a \in \mathcal{A}, b \in \mathcal{B}\}; \quad \mathcal{A}\mathcal{B} = \{ab; a \in \mathcal{A}, b \in \mathcal{B}\}.$$
A set $S \subset \mathbb{F}_p$ is said to have a nontrivial additive decomposition, if

$$S = A + B$$

for some sets $A \subset \mathbb{F}_p$, $B \subset \mathbb{F}_p$ with $|A| \geq 2$, $|B| \geq 2$.

The problem of nontrivial additive decomposition of multiplicative subgroups of $\mathbb{F}_p^*$ has been recently investigated in several works. Sárközy [4] conjectured that the set of quadratic residues has no nontrivial additive decomposition and obtained several results on this problem. Further progress in this direction has been made by Shkredov [5] and Shparlinski [6].

In the present paper we are interested in multiplicative decomposition of intervals in $\mathbb{F}_p$. This problem has been investigated by Shparlinski [6]. Let

$$I = \{n + 1, n + 2, \ldots, n + N\} \pmod{p}$$

be an interval in $\mathbb{F}_p$. Shparlinski observed that if $N < (p - 1)/32$ and if there is a decomposition $I = AB$, $|A| \geq 2, |B| \geq 2$, then Bourgain’s sum-product estimate (see, Lemma 2 below) leads to the sharp bound

$$N \leq |A||B| \leq 32N.$$ 

Here, for a positive integer $k$ and a set $\mathcal{X}$, the notation $k\mathcal{X}$ is used to denote the $k$-fold sum of $\mathcal{X}$, that is

$$k\mathcal{X} = \{x_1 + \ldots + x_k; \; x_i \in \mathcal{X}\}.$$ 

Clearly, if $0 \in S \subset \mathbb{F}_p$, then one has the decomposition $S = \{0, 1\}S$. On the other hand, if for such a set $S$ we have $S \setminus \{0\} = AB$, then it follows that $S = \{A \cup \{0\}\}B$. We give the following definition.

**Definition 1.** We say that the set $S \subset \mathbb{F}_p$ has a nontrivial multiplicative decomposition if

$$S \setminus \{0\} = AB$$

(1)

for some sets $A \subset \mathbb{F}_p$, $B \subset \mathbb{F}_p$ with $|A| \geq 2$, $|B| \geq 2$.

Any nonzero set $S$ with $S = -S$ admits a nontrivial decomposition, namely (1) holds with $A = \{-1, 1\}$, $B = S \setminus \{0\}$. We also note that for $p \geq 5$ we have the following decomposition of a special interval of 3 elements:

$$\{3^* - 1, 3^*, 3^* + 1\} \pmod{p} = \{-1, 2\} \cdot \{-3^*, 1 - 3^*\} \pmod{p}.$$ 

Here and below $n^*$ denotes the multiplicative inverse of $n$ modulo $p$.

In the present paper we prove the following statement.
Theorem 1. There exists an absolute constant \( c > 0 \) such that if an interval \( I \subset \mathbb{F}_p \) of cardinality \( |I| < cp \) has a nontrivial multiplicative decomposition, then either
\[
I = \pm\{3^*-1, 3^*, 3^*+1\} \pmod{p},
\]
or
\[
I = -I.
\]
In the latter case any nontrivial decomposition \( I \setminus \{0\} = AB \) implies that one of the sets \( A \) or \( B \) coincides with \( \{-r, r\} \) for some residue class \( r \in \mathbb{F}_p \).

The following statement shows that the constant \( c \) in the condition of Theorem 1 can not be taken \( c = 1/2 \).

Theorem 2. Let \( p \equiv 1 \pmod{4} \), \( p \neq 5 \). Then for any integer \( L \) satisfying
\[
\frac{p-1}{2} \leq L \leq p-1
\]
the interval
\[
I = \{1, 2, \ldots, L\} \pmod{p}
\]
admits a nontrivial multiplicative decomposition.

For arbitrary prime \( p \geq 3 \), we have the following result.

Theorem 3. Let \( p \geq 3 \) and \( k_1, k_2 \) be integers satisfying
\[
k_1 \geq 0.4(p-1), \quad k_2 \geq 0.4(p-1).
\]
Then the interval
\[
I = \{n \in \mathbb{Z}; -k_1 \leq n \leq k_2\} \pmod{p}
\]
admits a nontrivial multiplicative decomposition.

The idea behind the proof of Theorem 1 is as follows. As Shparlinski, we use Bourgain’s sum product estimate. Here, we apply it to the sets \( kA \) and \( B \) for a suitable integer \( k \) (which can be as large as constant times \( p/(|A||B|) \)). Then we use some arguments from additive combinatorics and show that the set \( A \) (and \( B \)) forms a positive proportion of some arithmetic progression modulo \( p \). Using this information we eventually reduce our problem to its analogy in \( \mathbb{Q} \) (the set of rational numbers).

Throughout the paper some absolute constants are indicated explicitly in order to make the arguments more transparent.
2 The case of rational numbers

Lemma 1. Let \( \mathcal{P} \subset \mathbb{Q} \) be a finite arithmetic progression such that
\[
\mathcal{P} \setminus \{0\} = \mathcal{A}\mathcal{B}
\]
for some sets \( \mathcal{A} \subset \mathbb{Q} \), \( \mathcal{B} \subset \mathbb{Q} \) with \( |\mathcal{A}| \geq 2 \), \( |\mathcal{B}| \geq 2 \). Then there exist rational numbers \( r, r_1, r_2 \) such that either
\[
\mathcal{A} = \{-r_1, 2r_1\}, \quad \mathcal{B} = \{-r_2, 2r_2\},
\]
or one of the sets \( \mathcal{A} \) or \( \mathcal{B} \) coincides with the set \( \{-r, r\} \).

Proof. Assume contrary, let \( \mathcal{P} \setminus \{0\} = \mathcal{A}\mathcal{B} \) be such that the sets \( \mathcal{A} \) and \( \mathcal{B} \) do not satisfy the conclusion of the lemma. We dilate the set \( \mathcal{A} \) such that the new set \( \mathcal{A}' \) consists on integers that are relatively prime. Similarly we construct the set \( \mathcal{B}' \). Then \( \mathcal{A}'\mathcal{B}' \) is also a set of integers that are relatively prime and we have \( \mathcal{P}' \setminus \{0\} = \mathcal{A}'\mathcal{B}' \), where \( \mathcal{P}' \subset \mathbb{Q} \) is an arithmetic progression (\( \mathcal{P}' \) is a dilation of \( \mathcal{P} \)). Let \( d \) be the difference of this progression. We rewrite \( \mathcal{A} = \mathcal{A}', \mathcal{B} = \mathcal{B}', \mathcal{P} = \mathcal{P}' \).

Let \( a_1, a_2 \in \mathcal{A} \). For any element \( b \in \mathcal{B} \) we have \( (a_1 - a_2)b \in \mathcal{P} \setminus \mathcal{P} \), implying \( (a_1 - a_2)b \equiv 0 \) (mod \( d \)). It then follows from the construction of \( \mathcal{B} \) that \( a_1 - a_2 \equiv 0 \) (mod \( d \)). Thus, the set \( \mathcal{A} \) is contained in a progression with difference \( d \). Analogously the set \( \mathcal{B} \) is contained in a progression with difference \( d \).

Define \( a_0 \) and \( b_0 \) to be the maximal by absolute value elements of \( \mathcal{A} \) and \( \mathcal{B} \) correspondingly. Without loss of generality we can assume that \( a_0 > 0 \), \( b_0 > 0 \). Since \( \mathcal{A} \neq \{-a_0, a_0\}, \mathcal{B} \neq \{-b_0, b_0\} \), we have
\[
 a_0 \geq \max\left\{2, \frac{d + 1}{2}\right\}, \quad b_0 \geq \max\left\{2, \frac{d + 1}{2}\right\}.
\]
(2)

Then \( a_0b_0 \) is the largest element of \( \mathcal{P} \) and \( a_0b_0 > d \). From
\[
a_0b_0 - d \in \mathcal{P} \setminus \{0\} = \mathcal{A}\mathcal{B},
\]
it follows that for some \( a_1 \in \mathcal{A}, b_1 \in \mathcal{B} \) we have
\[
a_0b_0 - d = a_1b_1.
\]
(3)
If $|a_1| = a_0$, then

$$d = a_0(b_0 - |b_1|) \geq (b_0 - |b_1|) \frac{d + 1}{2}.$$ 

This implies that $b_0 - |b_1| = 1$ and $a_0 = d$. Since by the assumption, $A \neq \{-d, d\}$ and $0 \not\in A$, we get a contradiction with the maximality property of $a_0$.

Thus, in (3) we have $|a_1| \neq a_0$. Similarly, $|b_1| \neq b_0$. It then follows that

$$d = a_0b_0 - |a_1||b_1| \geq a_0b_0 - (a_0 - 1)(b_0 - 1) = a_0 + b_0 - 1.$$ 

Combining this with (2) we get that

$$a_0 = \frac{d + 1}{2}; \quad b_0 = \frac{d + 1}{2}; \quad d \geq 3.$$ 

Therefore, the maximality properties of $a_0$ and $b_0$ imply that

$$A = B = \left\{ \frac{1 - d}{2}, \frac{1 + d}{2} \right\}.$$ 

Hence,

$$P \setminus \{0\} = AB = \left\{ \frac{1 - d^2}{4}, \frac{(1 - d)^2}{4}, \frac{(1 + d)^2}{4} \right\}.$$ 

Since $(1 - d^2)/4 \neq d$, we get

$$\frac{1 - d^2}{4} = \frac{(1 - d)^2}{4} - d.$$ 

This implies $d = 3$, $A = B = \{-1, 2\}$ and concludes the proof of our lemma.

\[\square\]

3 Some facts from additive combinatorics

We need several facts from additive combinatorics.

**Lemma 2.** Let $\mathcal{X} \subset \mathbb{F}_p$, $\mathcal{Y} \subset \mathbb{F}_p$ and $\mathcal{X} \neq \{0\}$, $\mathcal{Y} \neq \{0\}$. Then

$$|8\mathcal{X}\mathcal{Y} - 8\mathcal{X}\mathcal{Y}| \geq \frac{1}{2} \min\{|\mathcal{X}| |\mathcal{Y}|, p - 1\}.$$ 

5
Lemma 3. For a sufficiently large $p$, let $\mathcal{X}$ be a subset of $\mathbb{F}_p$ such that $|\mathcal{X}| < p/35$ and

$$|2\mathcal{X}| < \frac{12}{5}|\mathcal{X}| - 3.$$ 

Then $\mathcal{X}$ is contained in an arithmetic progression of at most $|2\mathcal{X}| - |\mathcal{X}| + 1$ terms.

Lemma 2 is Bourgain’s sum product estimate from [1]. Lemma 3 is Freiman’s result on additive structure of sets with small doubling (see, for example, [3, Theorem 2.11]).

Lemma 4. Let $\mathcal{X}$ be a subset of $\mathbb{F}_p$ and $m$ be a positive integer such that $|m\mathcal{X}| < \min\{33m|\mathcal{X}|, \frac{p-1}{8}\}$.

Assume that $m\mathcal{X}$ is contained in an arithmetic progression of at most $2|m\mathcal{X}|$ terms. Then $\mathcal{X}$ is contained in an arithmetic progression of at most $132|\mathcal{X}|$ terms.

Proof. By a suitable dilation of the set $\mathcal{X}$, we can assume that $m\mathcal{X}$ forms at least a half of an arithmetic progression with difference equal to 1. In particular, the diameter of this progression is not greater than $2|m\mathcal{X}|$. Thus,

$$m\mathcal{X} - m\mathcal{X} \subset [-2|m\mathcal{X}|, 2|m\mathcal{X}|] \pmod{p}.$$ 

Let $x_1, x_2 \in \mathcal{X}$ and $x_1 - x_2 = d \pmod{p}$ with $|d| \leq (p-1)/2$. It suffices to prove that $|d| < 66|\mathcal{X}|$. Observe that all the elements $id \pmod{p}$, $1 \leq i \leq m$, are contained in the set $m\mathcal{X} - m\mathcal{X}$. Thus,

$$\{d, 2d, \ldots, md\} \pmod{p} \subset [-2|m\mathcal{X}|, 2|m\mathcal{X}|] \pmod{p}.$$ 

It then follows that we actually have $id \in [-2|m\mathcal{X}|, 2|m\mathcal{X}|]$ for all $1 \leq i \leq m$. Indeed, this is trivial for $i = 1$. Assume that for some $1 \leq i \leq m-1$ we have $id \in [-2|m\mathcal{X}|, 2|m\mathcal{X}|]$ and let

$$(i+1)d \equiv z_{i+1} \pmod{p} \quad (4)$$

for some $z_{i+1} \in [-2|m\mathcal{X}|, 2|m\mathcal{X}|]$. Since, by the induction hypothesis,

$$|(i+1)d| \leq 2|id| \leq 4|m\mathcal{X}| \leq (p-1)/2,$$

the congruence (4) is converted to an equality, as desired.

In particular, $md \subset [-2|m\mathcal{X}|, 2|m\mathcal{X}|]$, implying $|d| \leq \frac{2}{m}|m\mathcal{X}| < 66|\mathcal{X}|$. \qed
The following statement is known as the Cauchy-Davenport theorem (see, for example, [3, Theorem 2.2]).

**Lemma 5.** For any nonempty subsets $X$ and $Y$ of $\mathbb{F}_p$ the following bound holds:

$$|X + Y| \geq \min\{p, |X| + |Y| - 1\}.$$  

We will also need the following simple statement.

**Lemma 6.** Let $0 < \delta < 1$ and let $L$ be an integer with $L > \delta^{-1}$. Assume that the set $\mathcal{X} \subset \{r + 1, r + 2, \ldots, r + L\}$ is such that $|\mathcal{X}| \geq \delta L$. Then for any positive integer $k$ with $\delta^{-k} < L$ there exist elements $x_1, x_2 \in \mathcal{X}$ such that

$$\frac{\delta^{-(k-1)}}{2} \leq x_1 - x_2 < 2\delta^{-k}.$$ 

**Proof.** We split the interval $[r + 1, r + L]$ into $[\delta^k L] - 1$ subintervals of length

$$\frac{L - 1}{[\delta^k L] - 1} < \frac{L}{(\delta^k L/2)} = 2\delta^{-k}.$$ 

From the pigeon-hole principle, one of this intervals (denote it by $\mathcal{R}$) contains at least

$$\frac{|\mathcal{X}|}{[\delta^k L - 1]} > \frac{\delta L}{\delta^k L} = \delta^{-(k-1)}$$ 

elements of $\mathcal{X}$. Therefore, if $x_1$ and $x_2$ are the largest and the smallest elements of $\mathcal{R} \cap \mathcal{X}$ then

$$2\delta^{-k} > x_1 - x_2 \geq \max\{1, \delta^{-(k-1)} - 1\} \geq \frac{\delta^{-(k-1)}}{2}.$$ 

\qed

4 Proof of Theorem \[ ]

Let $N < cp$ and assume that the interval

$$\mathcal{I} = \{n + 1, n + 2, \ldots, n + N\} \pmod{p}$$

is such that $\mathcal{I}_0 = \mathcal{I} \setminus \{0\} = \mathcal{A}\mathcal{B}$ for some subsets $\mathcal{A} \subset \mathbb{F}_p$, $\mathcal{B} \subset \mathbb{F}_p$ with $\min\{|\mathcal{A}|, |\mathcal{B}|\} \geq 2$. Here $c$ is a small positive constant (the smallness of the constant $c$ is at our disposal).
Let $k$ be the largest integer such that $2^kN = 2^k|\mathcal{I}| < p/33$. Observe that for any positive integer $m$

$$(m\mathcal{A})\mathcal{B} \subset m\mathcal{A}\mathcal{B} \subset m\mathcal{I}.$$ 

Hence, since $\mathcal{I}$ is an interval, from Lemma 2 we get, for any nonnegative integer $\nu \leq k$,

$$\min\{p - 1, |2^\nu \mathcal{A}||\mathcal{B}|\} \leq 2|\mathcal{8}(2^\nu \mathcal{A})\mathcal{B} - 8(2^\nu \mathcal{A})\mathcal{B}|$$

$$\leq 2|2^{\nu+3}\mathcal{I} - 2^{\nu+3}\mathcal{I}| \leq 32 \times 2^{\nu}(|\mathcal{I}| - 1) + 2 < 33 \times 2^{\nu}\mathcal{A}||\mathcal{B}|.$$ 

In particular, if

$$p - 1 \leq 2|\mathcal{8}(2^\nu \mathcal{A})\mathcal{B} - 8(2^\nu \mathcal{A})\mathcal{B}|,$$

then we get

$$p - 1 \leq 32 \times 2^{\nu}(|\mathcal{I}| - 1) + 2 < 32 \times p/33.$$ 

This contradiction shows that actually

$$|2^\nu \mathcal{A}||\mathcal{B}| \leq 2|\mathcal{8}(2^\nu \mathcal{A})\mathcal{B} - 8(2^\nu \mathcal{A})\mathcal{B}|.$$ 

Therefore,

$$|2^\nu \mathcal{A}||\mathcal{B}| \leq 33 \times 2^{\nu}\mathcal{A}||\mathcal{B}|; \quad |\mathcal{A}||\mathcal{B}| \leq 2|\mathcal{8}\mathcal{I} - 8\mathcal{I}| < 32N \leq 32cp.$$ 

Thus,

$$|2^\nu \mathcal{A}| < 33 \times 2^{\nu}|\mathcal{A}| \quad \text{for any} \quad \nu = 0, 1, 2, \ldots, k \quad (5)$$

and we also have

$$N - 1 \leq |\mathcal{A}||\mathcal{B}| < 32cp. \quad (6)$$

Since $c$ is small, $k$ is large. From (5) we get

$$\prod_{\ell=4}^{k-1} |2^{\ell+1} \mathcal{A}| = \frac{|2^k \mathcal{A}|}{|2^4 \mathcal{A}|} < 33 \times 2^k.$$ 

Hence, since $k$ is large enough, there exists $4 \leq \ell < k$ such that

$$|2^{\ell+1} \mathcal{A}| < 2.1 \times |2^\ell \mathcal{A}| < \frac{12}{5} |2^\ell \mathcal{A}| - 3. \quad (7)$$

Here we also used the inequality $|2^\ell \mathcal{A}| \geq |2^4 \mathcal{A}| > 10$ which follows from Lemma 5.
Since $|2^{\ell+1}A| < p/32$, Lemma 3 implies that $|2^\ell A| < p/35$. Then applying Lemma 3 with $X = 2^\ell A$ we get that the set $2^\ell A$ forms at least a half of an arithmetic progression. Therefore, inequality (5) with $\nu = \ell$ and Lemma 4 implies that the set $A$ is contained in an arithmetic progression of at most $132|A|$ terms. By completing the progression, we can assume that $A$ is contained in an arithmetic progression of $132|A|$ terms.

Analogously, the set $B$ is contained in an arithmetic progression of $132|B|$ terms.

We recall that $AB = \mathcal{I} \setminus \{0\}$ and, by (6), $|A||B| < 32cp$, where $c$ is a small positive constant. We can dilate $A$ and $B$ and assume, without loss of generality, that for some integer $r$

$$A \subset \{r + 1, r + 2, \ldots, r + 132|A|\} \pmod{p}.$$  

We shall now prove that for any element $b \in B$ there are integers $u$ and $v$ such that

$$|u| \leq 264^2|B|; \quad 1 \leq v \leq 264; \quad b \equiv \frac{u}{v} \pmod{p}.$$

Let $K$ be the integer defined from

$$|A| \leq 132^K < 132|A|.$$  

We associate the elements of $A$ with their representatives from the interval $\{r + 1, r + 2, \ldots, r + 132|A|\}$. Note that for any $a_1 \in A, a_2 \in A$ we have

$$(a_1 - a_2)b \in AB - AB \subset \mathcal{I} - \mathcal{I} \subset [-N + 1, N - 1] \pmod{p}.$$  

It then follows from Lemma 6 with $\delta = 1/132$ that

$$b \equiv \frac{u_1}{v_1} \equiv \frac{u_2}{v_2} \equiv \ldots \equiv \frac{u_K}{v_K} \pmod{p},$$

for some integers $u_1, \ldots, u_K, v_1, \ldots, v_K$ with

$$|u_j| < N; \quad \frac{132^{j-1}}{2} \leq v_j < 2 \times 132^j.$$  

Moreover, we can assume that $\gcd(u_1, v_1) = 1$.  

9
We claim that for any $j \in \{1, 2, \ldots, K\}$ there exists an integer $t_j$ such that

$$u_j = t_j u_1; \quad v_j = t_j v_1. \tag{8}$$

We prove this by induction on $j$. The claim is trivial for $j = 1$. Assume that (8) is true for some $1 \leq j \leq K - 1$. Then from

$$\frac{132^{j-1}}{2} \leq v_j = t_j v_1 \leq 264t_j$$

we have $t_j \geq 132^{j-1}/528$ and therefore

$$|u_1| = \frac{|u_j|}{t_j} < \frac{N}{t_j} \leq \frac{528N}{132^{j-1}}.$$ 

Next, we have

$$u_1 v_{j+1} \equiv v_1 u_{j+1} \pmod{p}.$$ 

The absolute value of the left hand side is bounded by

$$\frac{528N}{132^{j-1}} \times 2 \times 132^{j+1} \leq 1056 \times 132^2 cp \leq p/3.$$ 

The absolute value of the right hand side is bounded by $264N < p/3$. Thus, our congruence is converted to the equality

$$u_1 v_{j+1} = v_1 u_{j+1}.$$ 

Since $\gcd(u_1, v_1) = 1$, there is an integer $t_{j+1}$ such that

$$u_{j+1} = t_{j+1} u_1; \quad v_{j+1} = t_{j+1} v_1.$$ 

Thus, (8) holds for all $j = 1, 2, \ldots, K$. In particular, for $j = K$ we have

$$u_K = t_K u_1; \quad v_K = t_K v_1.$$ 

Therefore,

$$t_K = \frac{v_K}{v_1} \geq \frac{132^{K-1}}{528} \geq \frac{|A|}{264^2}$$ 

implying

$$|u_1| = \frac{|u_K|}{t_K} \leq \frac{N - 1}{t_K} \leq \frac{264^2 (N - 1)}{|A|} \leq 264^2 |B|.$$
Since we also have $1 \leq v_1 \leq 264$, our claim on the structure of $b \in \mathcal{B}$ follows from $b \equiv u_1/v_1 \pmod{p}$.

Denote by $\mathcal{A}'$ and $\mathcal{B}'$ the dilations of $\mathcal{A}$ and $\mathcal{B}$ defined from

$$
\mathcal{A}' = \{ (264!)^*a; a \in \mathcal{A} \}; \quad \mathcal{B}' = \{ 264!b; b \in \mathcal{B} \}.
$$

We have

$$
\mathcal{A}'\mathcal{B}' = \mathcal{A}\mathcal{B} = \mathcal{I} \setminus \{0\}.
$$

Furthermore,

$$
\mathcal{B}' \subset \{ n \in \mathbb{Z}; -266!|\mathcal{B}'| \leq n \leq 266!|\mathcal{B}'| - 1 \} \pmod{p}.
$$

We shall prove that for any $a \in \mathcal{A}'$ there are integers $u', v'$ such that

$$
|u'| \leq (267!)^2|\mathcal{A}'|; \quad 1 \leq v' \leq 267!; \quad a \equiv \frac{u'}{v'} \pmod{p}.
$$

Let $K'$ be the integer defined from

$$
|\mathcal{B}'| \leq (2 \times 266!)^{K'} < (2 \times 266!)|\mathcal{B}'|.
$$

Let $a \in \mathcal{A}'$. We note that for any $b_1 \in \mathcal{B}', b_2 \in \mathcal{B}'$ we have

$$(b_1 - b_2)a \in \mathcal{A}'\mathcal{B}' - \mathcal{A}'\mathcal{B}' \subset \mathcal{I} - \mathcal{I} \subset [-N + 1, N - 1] \pmod{p}.$$}

As before, from Lemma $\Box$ with $\delta = 1/(2 \times 266!)$ it follows that

$$
a \equiv \frac{u'_1}{v'_1} \equiv \frac{u'_2}{v'_2} \equiv \ldots \equiv \frac{u'_{K'}}{v'_{K'}} \pmod{p},
$$

for some integers $u'_1, \ldots, u'_K, v'_1, \ldots, v'_K$ with

$$
|u'_j| < N; \quad \frac{(2 \times 266!)^{j-1}}{2} \leq v'_j < 2 \times (2 \times 266!)^j; \quad \gcd(u'_1, v'_1) = 1.
$$

Exactly as before, it follows by induction on $j$, that for any $j \in \{1, 2, \ldots, K'\}$ there is an integer $t'_j$ such that

$$
\quad u'_j = t'_j u'_1; \quad v'_j = t'_j v'_1.
$$

In particular, taking $j = K'$ we get that

$$
t'_{K'} = \frac{v'_{K'}}{v'_1} \geq \frac{(2 \times 266!)^{K'-1}}{4 \times 266!} \geq \frac{|\mathcal{B}'|}{(267!)^2}.
$$
Thus,

\[ |u'_1| = \frac{|u'_K|}{t_K} \leq \frac{(267!)^2(N - 1)}{|B'|} \leq (267!)^2|A'|. \]

Our claim on the structure of \( a \in A' \) follows from \( a \equiv u'_1/v'_1 \pmod{p} \).

Let now \( A'' \) be the dilation of \( A' \) defined as

\[ A'' = \{(267)!a; a \in A'\}. \]

Since \( A'B' = \mathbb{F} \setminus \{0\} \), it follows that \( A''B' = \mathcal{P} \setminus \{0\} \) for some arithmetic progression \( \mathcal{P} \subset \mathbb{F}_p \). Note that now we have

\[ A'' \subset \{n \in \mathbb{Z}; |n| \leq (268!)|A'| \} \pmod{p}. \]

Let

\[ A'' \subset \{n \in \mathbb{Z}; |n| \leq (268!)|A'| \}, \quad B'' \subset \{n \in \mathbb{Z}; |n| \leq 266!|B'| \} \]

be such that

\[ A'' = A'' \pmod{p}, \quad B' = B'' \pmod{p}. \quad (9) \]

Then either \( A''B'' \) or \( A''B'' \cup \{0\} \) is a set \( \{x_1, x_2, \ldots, x_{N'}\} \), with integers \( x_i \) satisfying \( |x_i| \leq (269!)!cp < 0.1p \) and

\[ x_{i+2} - x_{i+1} \equiv x_{i+1} - x_i \pmod{p}; \quad i = 1, 2, \ldots, N' - 2. \]

Then the congruence is converted to the equality

\[ x_{i+2} - x_{i+1} = x_{i+1} - x_i; \quad i = 1, 2, \ldots, N' - 2. \]

Thus, we have that either \( A''B'' \) or \( A''B'' \cup \{0\} \) is an arithmetic progression of integers. Since \( |A''| \geq 2, |B''| \geq 2 \), we can apply Lemma 1. It follows that there exists rational numbers \( r, r_1, r_2 \) such that either

\[ A'' = \{-r_1, 2r_1\}, \quad B'' = \{-r_2, 2r_2\}, \]

or one of the sets \( A'' \) or \( B'' \) coincides with the set \( \{-r, r\} \). In the latter case (9) implies that either \( A'' \) or \( B'' \) coincides with the set \( \{-r, r\} \pmod{p} \) and the result follows from the fact that \( A \) and \( B \) are the dilations of \( A'' \) and \( B'' \) correspondingly.
In former case, for some $h \in \mathbb{F}_p$ we have
\[ \mathcal{I} \setminus \{0\} = \{-2h, h, 4h\}. \]
It follows that $\{0\} \not\subseteq \mathcal{I}$ and we get, for some $h_1$,
\[ \mathcal{I} = \{h_1(3^* - 1), h_13^*, h_1(3^* + 1)\} \pmod{p}. \]
From this it follows that either $h_1(3^* - 1)$ and $h_13^*$ or $h_13^*$ and $h_1(3^* + 1)$
are consecutive elements of $\mathcal{I}$. Thus, $h_1 \in \{-1, 1\} \pmod{p}$. This finishes
the proof of Theorem 1.

5 Proof of Theorems 2 and 3

The proof of Theorems 2 and 3 uses ideas from [2].

We first prove Theorem 2. We can assume that $L < p - 1$. Define positive
integers $u$ and $v$ from the representation $p = u^2 + v^2$. Let $h$ be an integer
defined from
\[ h \equiv u/v \pmod{p}. \]
Note that the set
\[ \mathcal{A} = \{x \in \mathcal{I}; \ hx \in \mathcal{I}\} \]
is nonempty (indeed $v \in \mathcal{A}$). Let $\mathcal{B} = \{1, h\} \pmod{p}$. Let us prove that
\[ \mathcal{I} = \mathcal{A}\mathcal{B}. \] Assume contrary. Since $\mathcal{A}\mathcal{B} \subseteq \mathcal{I}$, there is an element
\[ x \in \mathcal{I} \setminus \mathcal{A}\mathcal{B}. \]
Note that
\[ hx \notin \mathcal{I}; \ h^*x \notin \mathcal{I}. \]
Indeed, if $hx \in \mathcal{I}$, then $x \in \mathcal{A}$ and thus $x \in \mathcal{A}\mathcal{B}$, contradiction. If $h^*x \in \mathcal{I}$,
then from $h(h^*x) = x \in \mathcal{I}$ it follows that $h^*x \in \mathcal{A}$ and thus $x \in \mathcal{A}\mathcal{B}$, contradiction.

Therefore, for some $1 \leq s_1 \leq p - L - 1$ and $1 \leq s_2 \leq p - L - 1$ we have
\[ hx \equiv -s_1 \pmod{p}; \ h^*x \equiv -s_2 \pmod{p}. \]
Since $h^2 + 1 \equiv 0 \pmod{p}$, it follows that $s_1 + s_2 \equiv 0 \pmod{p}$. Impossible.
Thus, we have that $\mathcal{I} = \mathcal{A}\mathcal{B}$. In particular,

$$|\mathcal{A}| \geq \frac{L}{|\mathcal{B}|} \geq \frac{p-1}{4} \geq 3,$$

which shows that the decomposition is nontrivial and finishes the proof of Theorem 2.

Let us prove Theorem 3. Since $\mathbb{F}_p^* = \mathbb{F}_p^* \cdot \mathbb{F}_p^*$, we can assume that $k_1 + k_2 < p - 1$. In particular, it follows that $p \geq 11$.

We make the following observation: for any integer $x$ one of the elements $2x \pmod{p}$ or $2^* x \pmod{p}$ belongs to the interval $\mathcal{I}$. Indeed, if $2^* x \not\in \mathcal{I}$, it follows that $x \equiv 2n \pmod{p}$ for some integer $n$ with $k_2 < n < p - k_1$. Then

$$2x \equiv 4n \equiv 4n - 2p \pmod{p}.$$ 

Since

$$-0.4(p - 1) < 4n - 2p < 0.4(p - 1),$$

it follows that $2x \pmod{p} \in \mathcal{I}$.

Now we repeat the proof of Theorem 2. Let

$$\mathcal{A} = \{x \in \mathcal{I} \setminus \{0\}; \ 2x \in \mathcal{I} \setminus \{0\}\}.$$

Since $1 \in \mathcal{A}$, the set $\mathcal{A}$ is nonempty. Let $\mathcal{B} = \{1, 2\} \pmod{p}$. Let us prove that $\mathcal{I} \setminus \{0\} = \mathcal{A}\mathcal{B}$. Assume contrary. Since $\mathcal{A}\mathcal{B} \subset \mathcal{I} \setminus \{0\}$, there is an element

$$x \in \{\mathcal{I} \setminus \{0\}\} \setminus \mathcal{A}\mathcal{B}.$$

If $2x \in \mathcal{I} \setminus \{0\}$, then $x \in \mathcal{A}$ and thus $x \in \mathcal{A}\mathcal{B}$, contradiction. If $2^* x \in \mathcal{I} \setminus \{0\}$, then $2^* x \in \mathcal{A}$ and thus $x \in \mathcal{A}\mathcal{B}$, contradiction.

Then $2x \in \mathcal{I} \setminus \{0\}$ and $2^* x \in \mathcal{I} \setminus \{0\}$ which contradicts to the above made observation.

Thus, we have

$$\mathcal{I} \setminus \{0\} = \mathcal{A}\mathcal{B},$$

with $|\mathcal{B}| = |\{1, 2\}| = 2$. In particular,

$$|\mathcal{A}| \geq \frac{k_1 + k_2}{2} \geq 0.4(p - 1) > 2,$$

which shows that the decomposition is nontrivial and finishes the proof of Theorem 3.
References

[1] J. Bourgain, ‘Multilinear exponential sums in prime fields under optimal entropy condition on the sources’, *Geom. Funct. Anal.* 18 (2009), 1477–1502.

[2] K. Gyarmati, S. Konyagin, A. Sárközy, ‘On the reducibility of large sets of residues modulo $p$’, *J. Number Theory* 133 (2013), 2374–2397.

[3] M. B. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets*, Grad. Texts in Math., Vol 165, Springer-Verlag, New York 1996, 293 pp.

[4] A. Sárközy, ‘On additive decompositions of the set of quadratic residues modulo $p$’, *Acta Arith.*, 155 (2012), 41–51.

[5] I. D. Shkredov, ‘Sumsets in quadratic residues’, *Preprint*, 2013.

[6] I. E. Shparlinski, ‘Additive decompositions of subgroups of finite fields’, *Preprint*, 2013.