# On reducible and primitive subsets of $\mathbb{F}_p$, II

**Katalin Gyarmati** and **András Sárközy**
Eötvös Loránd University, Department of Algebra and Number Theory
H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary
E-mail: gykati@cs.elte.hu and sarkozy@cs.elte.hu

**Abstract**

In Part I of this paper we introduced and studied the notion of reducibility and primitivity of subsets of $\mathbb{F}_p$: a set $\mathcal{A} \subset \mathbb{F}_p$ is said to be *reducible* if it can be represented in the form $\mathcal{A} = \mathcal{B} + \mathcal{C}$ with $\mathcal{B}, \mathcal{C} \subset \mathbb{F}_p$, $|\mathcal{B}|, |\mathcal{C}| \geqslant 2$; if there are no such sets $\mathcal{B}, \mathcal{C}$ then $\mathcal{A}$ is said to be *primitive*. Here we introduce and study strong form of primitivity and reducibility: a set $\mathcal{A} \subset \mathbb{F}_p$ is said to be *k-primitive* if changing at most $k$ elements of it we always get a primitive set, and it is said to be *k-reducible* if it has a representation in the form $\mathcal{A} = \mathcal{B}_1 + \mathcal{B}_2 + \dots + \mathcal{B}_k$ with $\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_k \subset \mathbb{F}_p$, $|\mathcal{B}_1|, |\mathcal{B}_2|, \dots, |\mathcal{B}_k| \geqslant 2$.

## 1 Introduction

In this paper we will use the following notations and definitions:

The set of the positive integers is denoted by $\mathbb{N}$, the finite field of $p$ elements is denoted by $\mathbb{F}_p$, and we write $\mathbb{F}_p^* = \mathbb{F}_p \backslash \{0\}$. If $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$, then their *distance* $D(\mathcal{A}, \mathcal{B})$ is defined as the cardinality of their symmetric difference (in other words, $D(\mathcal{A}, \mathcal{B})$ is the Hamming distance between $\mathcal{A}$ and $\mathcal{B}$). If $\mathcal{G}$ is an additive semigroup and $\mathcal{A} = \{a_1, a_2, \dots\}$ is a subset of $\mathcal{G}$ such that the sums $a_i + a_j$ with $1 \leqslant i < j$ are distinct, then $\mathcal{A}$ is called a *Sidon set*. In some of the proofs we will identify $\mathbb{F}_p$ with the field of the modulo $p$ residue classes, and a residue class and its representant element will be denoted in the same way.

We will also need

2010 Mathematics Subject Classification: Primary 11B13.

Keywords and phrases: sum sets, finite sets, reducible sets, primitive sets.

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K100291 and NK104183.

**Definition 1.** Let $\mathcal{G}$ be a semigroup with the group operation called and denoted as *addition* and $\mathcal{A}, \mathcal{B}_1, \dots, \mathcal{B}_k$ subsets of $\mathcal{G}$ with

$$|\mathcal{B}_i| \geqslant 2 \quad \text{for} \quad i = 1, 2, \dots, k. \tag{1.1}$$

If

$$\mathcal{A} = \mathcal{B}_1 + \mathcal{B}_2 + \dots + \mathcal{B}_k,$$

then this is called an (additive) *$k$-decomposition* of $\mathcal{A}$, while if the group operation in $\mathcal{G}$ is called and denoted as *multiplication* and (1.1) and

$$\mathcal{A} = \mathcal{B}_1 \cdot \mathcal{B}_2 \cdot \ldots \cdot \mathcal{B}_k \tag{1.2}$$

hold, then (1.2) is called a *multiplicative $k$-decomposition* of $\mathcal{A}$. (A decomposition will always mean a non-trivial one, i.e., a decomposition satisfying (1.1).)

In 1948 H. H. Ostmann [12], [13] introduced some definitions on additive properties of sequences of non-negative *integers* and studied some related problems. The most interesting definitions are:

**Definition 2.** A finite or infinite set $\mathcal{C}$ of non-negative integers is said to be *reducible* if it has an (additive) 2-decomposition

$$\mathcal{C} = \mathcal{A} + \mathcal{B} \quad \text{with} \quad |\mathcal{A}| \geqslant 2, \quad |\mathcal{B}| \geqslant 2.$$

If there are no sets $\mathcal{A}$, $\mathcal{B}$ with these properties, then $\mathcal{C}$ is said to be *primitive* (or irreducible).

**Definition 3.** Two infinite sets $\mathcal{A}$, $\mathcal{B}$ of non-negative integers are said to be *asymptotically equal* if there is a number $K$ such that $\mathcal{A} \cap [K + \infty) = \mathcal{B} \cap [K, +\infty)$ and then we write $\mathcal{A} \sim \mathcal{B}$.

**Definition 4.** An infinite set $\mathcal{C}$ of non-negative integers is said to be *totally primitive* if every $\mathcal{C}'$ with $\mathcal{C}' \sim \mathcal{C}$ is primitive.

Since 1948 many papers have been published on related problems; a short survey of some of these papers was presented in Part I of this paper [8]. In almost all of the papers written before 2000 *infinite* sequences of non-negative integers are studied. The intensive study of *finite* problems of this type, in particular, of analogous problems in $\mathbb{F}_p$ has started only in the last decade (again, see [8] for details). In [8] we wrote: "...the notions of additive and multiplicative decompositions, reducibility and primitivity can be extended from integers to any semigroup, in particular, to the additive group of $\mathbb{F}_p$ and multiplicative group of $\mathbb{F}_p^*$ for any prime $p$; in the rest of the paper we will use these definitions in this extended sense." (More precisely, the multiplicative group of $\mathbb{F}_p^*$ and multiplicative decompositions are considered only in the introduction (Section 1) of [8], after that only the additive group of $\mathbb{F}_p$ and additive decompositions of subsets of $\mathbb{F}_p$ are studied.) "In this paper our goal is to continue the study of the reducible and primitive subsets of $\mathbb{F}_p$ and the connection between them." We recall two results from [8] which we will also need here:

**Theorem A.** *If $\mathcal{A} = \{a_1, a_2, \dots, a_t\} \subset \mathbb{F}_p$ is a* Sidon set*, then it is primitive.*

**Theorem B.** *Let $\mathcal{A} \subset \mathbb{F}_p$, and for $d \in \mathbb{F}_p^*$ denote the number of solutions of*

$$a - a' = d, \qquad a \in \mathcal{A}, \quad a' \in \mathcal{A}$$

*by $f(\mathcal{A}, d)$. If*

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < |\mathcal{A}|^{1/2}, \tag{1.3}$$

*then $\mathcal{A}$ is primitive.*

While the notions of reducibility and primitivity can be extended to any semigroup, the second author wrote in [16]: "On the other hand, clearly the definition of totalprimitivity [Definition 4] cannot be adapted to *finite* sets, thus we will not use it." This is certainly so, however, one may replace this missing notion by another one which has a similar flavor and it can be also used in case of finite sets. In this paper our first goal is to introduce and study a notion of this type, called *$k$-primitivity*; this will be done in Section 2. The study of this notion will lead to another problem of independent interest: in Section 3 we will be looking for a possibly large reducible subset of a given subset $\mathcal{A}$ of $\mathbb{F}_p$. In Section 4 we will return to the study of $k$-primitivity. The $k$-primitivity can be considered as a strong form of *primitivity*; in Sections 5 and 6 we will also introduce and study a strong form of *reducibility* called *$k$-reducibility.* Finally, in Section 7 we will show (by adapting an idea used in Section 6) that large subsets of $\mathbb{F}_p$ also possess a large reducible subset $\mathcal{R}$ with a *balanced* 2-decomposition, i.e., with a decomposition $\mathcal{R} = \mathcal{B} + \mathcal{C}$ such that both $|\mathcal{B}|$ and $|\mathcal{C}|$ are large.

# 2 $k$-primitive subsets of $\mathbb{F}_p$

As we pointed out in the introduction the definition of totalprimitivity (Definition 4) cannot be adapted to finite sets. Instead, we propose to introduce the following definition in $\mathbb{F}_p$:

**Definition 5.** For $k \in \mathbb{N}$ a set $\mathcal{A} \subset \mathbb{F}_p$ is said to be *$k$-primitive* if every set $\mathcal{B} \subset \mathbb{F}_p$ with $D(\mathcal{A}, \mathcal{B}) \leqslant k$ is primitive. (In other words, $\mathcal{A}$ is $k$-primitive if changing at most $k$ elements of it we always get a primitive set.)

We will prove the following criterion for $k$-primitivity:

**Theorem 1.** *Let $\mathcal{A} \subset \mathbb{F}_p$, and define $f(\mathcal{A}, d)$ as in Theorem B: $f(\mathcal{A}, d) = \left|\left\{(a, a') : a \in \mathcal{A},\ a' \in \mathcal{A},\ a - a' = d\right\}\right|$. If*

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < \frac{1}{3}|\mathcal{A}|^{1/2} \tag{2.1}$$

*and $k \in \mathbb{N}$ with*

$$k \leqslant \frac{1}{4}|\mathcal{A}|^{1/2}, \tag{2.2}$$

*then $\mathcal{A}$ is $k$-primitive.*

If $\mathcal{A} \subset \mathbb{F}_p$ is a Sidon set and $|\mathcal{A}| \geqslant 16$, then the left-hand side of (2.1) is 1 and the right-hand side is greater than 1, thus it follows from Theorem 1 that

**Corollary 1.** *If $\mathcal{A} \subset \mathbb{F}_p$ is a Sidon set with $|\mathcal{A}| \geqslant 16$ and we write $k = \left[\frac{1}{4}|\mathcal{A}|^{1/2}\right]$, then $\mathcal{A}$ is $k$-primitive.*

*Proof of Theorem 1.* We have to show that any set $\mathcal{B} \subset \mathbb{F}_p$ with

$$D(\mathcal{A}, \mathcal{B}) \leqslant k \tag{2.3}$$

is primitive. By Theorem B it suffices to show that such a set $\mathcal{B}$ satisfies (1.3) with $\mathcal{B}$ in place of $\mathcal{A}$:

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{B}, d) < |\mathcal{B}|^{1/2}. \tag{2.4}$$

In order to prove this we have to give an upper bound for $f(\mathcal{B}, d)$, i.e., for the number of pairs $(b, b')$ with

$$b \in \mathcal{B}, \quad b' \in \mathcal{B}, \tag{2.5}$$

$$b - b' = d \tag{2.6}$$

(for any fixed $d \in \mathbb{F}_p^*$). By $\mathcal{B} = (\mathcal{A} \cap \mathcal{B}) \cup (\mathcal{B} \backslash \mathcal{A})$, any pair $b, b'$ satisfying (2.5) and (2.6) must satisfy one of the following pairs of conditions:

$$b, b' \in \mathcal{A} \cap B \subset \mathcal{A}, \quad b - b' = d, \tag{2.7}$$

$$b \in \mathcal{B}\backslash\mathcal{A}, \quad b' = b - d \tag{2.8}$$

and

$$b' \in \mathcal{B}\backslash\mathcal{A}, \quad b = b' + d. \tag{2.9}$$

By (2.1), the number of pairs $b, b'$ satisfying (2.7) is at most

$$f(\mathcal{A}, d) < \frac{1}{3}|\mathcal{A}|^{1/2}.$$

Moreover, by (2.3) the number of $b$'s satisfying (2.8) is at most

$$|\mathcal{B}\backslash\mathcal{A}| \leqslant D(\mathcal{A}, \mathcal{B}) \leqslant k$$

and $b$ determines $b' = b - d$ uniquely, thus (2.8) has at most $k$ solutions, and in the same way, the number of solutions of (2.9) is at most $k$. Combining these estimates, by (2.2) we get that

$$f(\mathcal{B}, d) < \frac{1}{3}|\mathcal{A}|^{1/2} + 2k \leqslant \frac{5}{6}|\mathcal{A}|^{1/2}. \tag{2.10}$$

By $\mathcal{A} \subset B \cup (\mathcal{A}\backslash\mathcal{B})$ we have

$$|\mathcal{A}| \leqslant |\mathcal{B}| + |\mathcal{A}\backslash\mathcal{B}| \leqslant |\mathcal{B}| + D(\mathcal{A}, \mathcal{B})$$

whence, by (2.2) and (2.3),

$$|\mathcal{B}| \geqslant |\mathcal{A}| - D(\mathcal{A}, \mathcal{B}) \geqslant |\mathcal{A}| - k \geqslant |\mathcal{A}| - \frac{1}{4}|\mathcal{A}|^{1/2} \geqslant |\mathcal{A}| - \frac{1}{4}|\mathcal{A}| = \frac{3}{4}|\mathcal{A}|. \tag{2.11}$$

It follows from (2.10) and (2.11) that

$$f(\mathcal{B}, d) < \frac{5}{6}|\mathcal{A}|^{1/2} \leqslant \frac{5}{6}\left(\frac{4}{3}|\mathcal{B}|\right)^{1/2} = \left(\frac{25}{27}\right)^{1/2} |\mathcal{B}|^{1/2} < |\mathcal{B}|^{1/2}$$

which proves (2.4) and this completes the proof of Theorem 1. □

If $p$ is a prime then let $M(p)$ denote the greatest integer $k$ such that there is a $k$-primitive set $\mathcal{A}$ in $\mathbb{F}_p$. Our next goal is to estimate this function $M(p)$. However, in order to give an upper bound for $M(p)$, we will need the answer to the following question of independent interest: if $\mathcal{A}$ is a subset of $\mathbb{F}_p$ then, depending on the cardinality of $\mathcal{A}$, what can be said about the size of the greatest reducible subset of $\mathcal{A}$? Thus first in the next section we will study this problem, and we will return to the estimate of $M(p)$ in Section 4.

# 3 The size of the greatest reducible subset of a given subset of $\mathbb{F}_p$

If $\mathcal{A}$ is a Sidon set, then its subsets are also Sidon sets, thus by Theorem A they are primitive so that $\mathcal{A}$ has no reducible subset.

The cardinality of a Sidon set in $\mathbb{F}_p$ can be $\gg p^{1/2}$ (if $\mathcal{S}$ is a maximal Sidon set selected from $\{1, 2, \ldots, [p/2]\}$, then the residue classes represented by the elements of $\mathcal{S}$ form a Sidon set in $\mathbb{F}_p$, and by theorems of Erdős and Turán [5], Chowla [2] and Erdős [4] we have $|\mathcal{S}| = (1 + o(1))(p/2)^{1/2}$), thus there are subsets $\mathcal{A} \subset \mathbb{F}_p$ with $|\mathcal{A}| > c_1 p^{1/2}$ which do not contain a reducible subset. On the other hand, we can prove that every subset $\mathcal{A}$ with $|\mathcal{A}| > c_2 p^{1/2}$ must contain a reducible set. This follows from

**Theorem 2.** *If $\mathcal{A}$ is a subset of $\mathbb{F}_p$ with*

$$|\mathcal{A}|^2 - |\mathcal{A}| > p - 1, \tag{3.1}$$

*then it contains a reducible subset of form $\mathcal{B} + \mathcal{C}$ with*

$$|\mathcal{B} + \mathcal{C}| \geqslant |\mathcal{B}| \geqslant \frac{|\mathcal{A}|^2 - |\mathcal{A}|}{p - 1}, \tag{3.2}$$

$$|\mathcal{B}| \geqslant 2 \tag{3.3}$$

*and*

$$|\mathcal{C}| = 2. \tag{3.4}$$

*Proof of Theorem 2.* Defining $f(\mathcal{A}, d)$ in the same way as in Theorem B, clearly we have

$$\begin{aligned} \sum_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) &= \sum_{d \in \mathbb{F}_p^*} \big|\{(a, a') :\ a \in \mathcal{A},\ a' \in \mathcal{A},\ a - a' = d\}\big| \\ &= \big|\{(a, a') :\ a \in \mathcal{A},\ a' \in \mathcal{A},\ a \neq a'\}\big| = |\mathcal{A}|^2 - |\mathcal{A}|. \end{aligned} \tag{3.5}$$

Let $d_0$ be an element of $\mathbb{F}_p^*$ for which $f(\mathcal{A}, d)$ is maximal: $f(\mathcal{A}, d_0) \geqslant f(\mathcal{A}, d)$ for all $d \in \mathbb{F}_p^*$. Then by (3.5) we have

$$|\mathcal{A}|^2 - |\mathcal{A}| = \sum_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) \leqslant \sum_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d_0) = (p - 1) f(\mathcal{A}, d_0)$$

whence

$$f(\mathcal{A}, d_0) \geqslant \frac{|\mathcal{A}|^2 - |\mathcal{A}|}{p - 1}. \tag{3.6}$$

Write $\mathcal{B} = \{a' : \ a' \in \mathcal{A}, \ a' + d_0 \in \mathcal{A}\}$ and $\mathcal{C} = \{0, d_0\}$. Then clearly we have

$$\mathcal{B} + \mathcal{C} = \mathcal{B} + \{0, d_0\} = \mathcal{B} \cup \big(\mathcal{B} + \{d_0\}\big) \subset \mathcal{A},$$

by (3.6) we have

$$\begin{aligned} |\mathcal{B} + \mathcal{C}| &= \big|\mathcal{B} \cup (\mathcal{B} + \{d_0\})\big| \geqslant |\mathcal{B}| \\ &= \big|\{a' : \ a' \in \mathcal{A}, \ a' + d_0 \in \mathcal{A}\}\big| = f(\mathcal{A}, d_0) \geqslant \frac{|\mathcal{A}|^2 - |\mathcal{A}|}{p-1}, \end{aligned} \tag{3.7}$$

which proves (3.2), (3.3) follows from (3.1) and (3.7), and (3.4) also holds trivially, and this completes the proof of Theorem 2. □

Observe that the decomposition $\mathcal{B} + \mathcal{C}$ in Theorem 2 is of very special type: one of the two summands $\mathcal{B}$, $\mathcal{C}$ is a 2-element subset. One may expect that if $|\mathcal{A}|$ increases, then there are also better balanced decompositions of a large reducible subset of $\mathcal{A}$ where both $\mathcal{B}$ and $\mathcal{C}$ are large. Indeed, we will prove such a theorem in Section 7.

# 4 The estimate of $M(p)$

Now we are ready to estimate the function $M(p)$ defined at the end of Section 2:

**Theorem 3.** *For $p > p_0$ we have*

$$0.0029p < M(p) < \frac{1}{4}p. \tag{4.1}$$

*Proof of Theorem 3.* First we will prove the upper bound in (4.1). Let us write

$$K(\mathcal{A}) = \max\{k : \ k \in \mathbb{N}, \ \mathcal{A} \text{ is } k\text{-primitive}\}$$

for $\mathcal{A} \subset \mathbb{F}_p$ so that

$$M(p) = \max_{\mathcal{A} \subset \mathbb{F}_p} K(\mathcal{A}).$$

By the definition of $K(\mathcal{A})$ for every reducible set $\mathcal{A}' \subset \mathbb{F}_p$ we must have

$$D(\mathcal{A}, \mathcal{A}') \geqslant K(\mathcal{A}) + 1$$

or, in equivalent form,

$$K(\mathcal{A}) \leqslant D(\mathcal{A}, \mathcal{A}') - 1.$$

Thus in order to prove the upper bound in (4.1) it suffices to show that for every $\mathcal{A} \subset \mathbb{F}_p$ there is a reducible set $\mathcal{A}'$ with

$$D(\mathcal{A}, \mathcal{A}') - 1 < \frac{1}{4}p. \tag{4.2}$$

We have to distinguish two cases.

First consider the case when

$$|\mathcal{A}| > 2p^{1/2}. \tag{4.3}$$

It follows from this assumption that

$$|\mathcal{A}|^2 - |\mathcal{A}| > 4p - |\mathcal{A}| \geqslant 3p > p - 1$$

thus (3.1) holds so that Theorem 2 can be applied. Let $\mathcal{B} + \mathcal{C}$ be a reducible set of the type described in Theorem 2, and take $\mathcal{A}' = \mathcal{B} + \mathcal{C}$. Then $\mathcal{A}'$ is reducible, and by (3.2) for $p > 5$ we have

$$\begin{aligned} D(\mathcal{A}, \mathcal{A}') &= |\mathcal{A} \backslash (\mathcal{B} + \mathcal{C})| = |\mathcal{A}| - |\mathcal{B} + \mathcal{C}| \\ &\leqslant |\mathcal{A}| - \frac{|\mathcal{A}|^2 - |\mathcal{A}|}{p-1} = -\left( \frac{|\mathcal{A}|}{(p-1)^{1/2}} - \frac{(p-1)^{1/2}}{2} \right)^2 + \frac{p-1}{4} + \frac{|\mathcal{A}|}{p-1} \\ &\leqslant \frac{p-1}{4} + \frac{p}{p-1} = \frac{p}{4} + 1 + \left( \frac{1}{p-1} - \frac{1}{4} \right) < \frac{p}{4} + 1, \end{aligned}$$

which proves (4.2) in this case.

Assume now that

$$|\mathcal{A}| \leqslant 2p^{1/2}.$$

Then the set

$$\mathcal{A}' = \{0, 1, 2\} = \{0, 1\} + \{0, 1\}$$

is reducible and for $p > 100$ we have

$$D(\mathcal{A}, \mathcal{A}') = |\mathcal{A} \backslash \mathcal{A}'| + |\mathcal{A}' \backslash \mathcal{A}| \leqslant |\mathcal{A}| + |\mathcal{A}'| \leqslant 2p^{1/2} + 3 < \frac{p}{5} + \frac{p}{30} < \frac{p}{4}$$

which again proves (4.2) and this completes the proof of the upper bound in (4.1).

The proof of the lower bound will be based on the following result of Alon, Granville and Ubis [1]:

**Lemma 1.** *The number of reducible subsets of* $\mathbb{F}_p$ *is less than* $1.9602^p$ *if* $p$ *is large enough.*

(See Theorem 3 and Corollary 1 in [1].)

Assume that contrary to the lower bound stated in (4.1) we have

$$M(p) \leqslant 0.0029p, \tag{4.4}$$

and write

$$k = [0.0029p] + 1. \tag{4.5}$$

Then by the definition of $M(p)$ and (4.4), there is no $k$-primitive $\mathcal{A} \subset \mathbb{F}_p$ for this $k$, so that denoting the set of the reducible subsets of $\mathbb{F}_p$ by $\mathbb{R}_p$, for every $\mathcal{A} \subset \mathbb{F}_p$ there exists a set $\mathcal{R} = \mathcal{R}(\mathcal{A}) \subset \mathbb{R}_p$ with

$$D(\mathcal{A}, \mathcal{R}) \leqslant k. \tag{4.6}$$

For a fixed set $\mathcal{R} \subset \mathbb{F}_p$ let $\mathbb{A}(\mathcal{R})$ denote the set of the subsets $\mathcal{A}$ of $\mathbb{F}_p$ for which (4.6) holds. If $\mathcal{R}$ is fixed then every $\mathcal{A} \subset \mathbb{A}(R)$ can be obtained from $\mathcal{R}$ by changing (dropping or adding) exactly $i$ elements for some $i \leqslant k$; these $i$ elements of $\mathbb{F}_p$ can be chosen in $\binom{p}{i}$ ways. Thus we have

$$|\mathbb{A}(\mathcal{R})| = \sum_{i=0}^{k} \binom{p}{i} \leqslant (k+1)\binom{p}{k}. \tag{4.7}$$

Since for every $\mathcal{A} \subset \mathbb{F}_p$ there is an $\mathcal{R} \in \mathbb{F}_p$ with $\mathcal{A} \in \mathbb{A}(\mathcal{R})$ thus by (4.7) and Lemma 1 we have

$$\begin{aligned} 2^p &= \left|\{\mathcal{A} :\ \mathcal{A} \subset \mathbb{F}_p\}\right| = \Big|\bigcup_{\mathcal{R} \in \mathbb{R}_p} \{\mathcal{A} :\ \mathcal{A} \in \mathbb{A}(\mathcal{R})\}\Big| \\ &\leqslant \sum_{\mathcal{R} \in \mathbb{R}_p} |\mathbb{A}(\mathcal{R})| \leqslant \sum_{\mathcal{R} \in \mathbb{R}_p} (k+1)\binom{p}{k} = (k+1)\binom{p}{k}|\mathbb{R}_p| < (k+1)\binom{p}{k} 1.9602^p \end{aligned}$$

whence

$$(k+1)\binom{p}{k} > \left(\frac{2}{1.9602}\right)^p. \tag{4.8}$$

Now we need the following lemma which is Lemma 3 in [15] and can be proved easily by using Stirling's formula:

**Lemma 2.** *Let* $0 \leqslant a < b$ *and* $\varepsilon > 0$. *Then there exist a positive number* $\delta = \delta(a, b, \varepsilon)$ *and a positive integer* $m_0(a, b, \varepsilon)$ *such that if* $m \geqslant m_0(a, b, \varepsilon)$, $|u - bm| < \delta m$ *and* $|v - am| < \delta m$, *then*

$$\binom{u}{v} < 2^{(bd(a/b)+\varepsilon)m},$$

*where the function* $d(x)$ *is defined by* $d(x) = -\frac{1}{\log 2}(x \log x + (1-x)\log(1-x))$ *for* $0 < x < 1$ *and* $d(0) = d(1) = 0$.

By (4.5), it follows from Lemma 2 (with $m = u = p$, $v = k$, $a = 0.0029$, $b = 1$) that for $p \to \infty$ we have

$$(k+1)\binom{p}{k} < 2^{(d(0.0029)+o(1))p}. \tag{4.9}$$

It follows from (4.8) and (4.9) that we must have

$$\frac{2}{1.9602} \leqslant 2^{d(0.0029)},$$

whence

$$(\log 2)d(0.0029) + \log 0.9801 \geqslant 0,$$

$$-0.0029 \log 0.0029 - 0.9971 \log 0.9971 + \log 0.9801 \geqslant 0. \tag{4.10}$$

However, a little computation shows that the left-hand side of (4.10) is less than

$$0.01695 + 0.00290 - 0.02010 = -0.00025 < 0,$$

so that (4.10) does not hold. This contradiction shows that (4.4) does not hold either, and this completes the proof of Theorem 3. □

# 5 $k$-reducible subsets of $\mathbb{F}_p$

Roughly speaking, $k$-primitivity is a strong form of *primitivity.* Now we will introduce a strong form of *reducibility*, called $k$-reducibility:

**Definition 6.** If $k \in \mathbb{N}$ and the set $\mathcal{A} \subset \mathbb{F}_p$ has a $k$-decomposition

$$\mathcal{A} = \mathcal{B}_1 + \mathcal{B}_2 + \cdots + \mathcal{B}_k \quad (\text{with } |\mathcal{B}_1|, |\mathcal{B}_2|, \ldots, |\mathcal{B}_k| \geqslant 2), \tag{5.1}$$

then $\mathcal{A}$ is said to be *$k$-reducible.*

But is $k$-reducibility really a strong form of reducibility, in other words, does it follow from the $k$-reducibility of $\mathcal{A}$ that it is also 2-reducible or briefly reducible? It follows from (5.1) that

$$\mathcal{A} = \mathcal{B}_1 + (\mathcal{B}_2 + \cdots + \mathcal{B}_k)$$

which is a 2-decomposition of $\mathcal{A}$ thus $\mathcal{A}$ is trivially reducible, so that the answer to this question is affirmative. But is $k$-reducibility *much stronger* than reducibility, in particular, are there many reducible sets which are not 3-*reducible*? This is an important question to answer since there are several papers [3], [16], [17], [18] where it is conjectured that a certain special subset of $\mathbb{F}_p$ is primitive, i.e., it is *not* 2*-reducible.* Then it turns out that the conjecture is beyond reach, thus partial results are proved; among others, it is proved that the given subset is *not* 3*-reducible.* Is this partial result close to the conjectured fact or is there still a long way to go? We will show by a construction that the second half of this alternative seems to be closer to the truth since there are many 2-reducible subsets which are not 3-reducible:

**Theorem 4.** *Let $p$ be a prime number with $p > 22$, and let $\mathcal{A}$ be a subset of $\mathbb{F}_p$ which is of the form*

$$\mathcal{A} = \{0,1\} \cup \mathcal{A}_0 \tag{5.2}$$

*where $\mathcal{A}_0$ is a subset of $\mathbb{F}_p$ with*

$$\mathcal{A}_0 \subset \left[\frac{p}{4}, \frac{p}{2}\right) \tag{5.3}$$

*and it is of the form*

$$\mathcal{A}_0 = \bigcup_{j=1}^{r} \{a_j, a_j+1, \dots, a'_j\} \tag{5.4}$$

*with $r \geqslant 1$,*

$$a'_j > a_j \quad \textit{for} \;\; j = 1,2,\dots,r \tag{5.5}$$

*and*

$$a_{j+1} \geqslant a'_j + 2 \quad \textit{for} \;\; j = 1,2,\dots,r-1. \tag{5.6}$$

*Then $\mathcal{A}$ is* 2*-reducible but it is not* 3*-reducible. Moreover, if $\mathbb{G}$ denotes the set of the subsets $\mathcal{A} \subset \mathbb{F}_p$ of the type described above, then we have*

$$|\mathbb{G}| > 2^{p/8-2}. \tag{5.7}$$

*Proof of Theorem 4.* If we define $\mathcal{B} \subset \mathbb{F}_p$ by

$$\mathcal{B} = \{0\} \cup \left( \bigcup_{j=1}^{r} \{a_j, a_{j+1}, \dots, a'_j - 1\} \right),$$

then clearly

$$\mathcal{A} = \{0,1\} + \mathcal{B}$$

is a non-trivial 2-decomposition of $\mathcal{A}$.

Now assume that contrary to the statement of the theorem $\mathcal{A}$ is not 3-reducible, i.e., it has a non-trivial 3-decomposition

$$\mathcal{A} = \mathcal{B} + \mathcal{C} + \mathcal{D}. \tag{5.8}$$

By $0 \in \mathcal{A}$ and (5.8) there are $b \in \mathcal{B}$, $c \in \mathcal{C}$, $d \in \mathcal{D}$ such that $0 = b + c + d$. Then writing $\mathcal{B}' = \mathcal{B} - \{b\}$, $\mathcal{C}' = \mathcal{C} - \{c\}$ and $\mathcal{D}' = \mathcal{D} - \{d\}$, clearly

$$\mathcal{A} = \mathcal{B}' + \mathcal{C}' + \mathcal{D}' \tag{5.9}$$

is a non-trivial 3-decomposition of $\mathcal{A}$ with

$$0 \in \mathcal{B}', \mathcal{C}', \mathcal{D}'. \tag{5.10}$$

Since (5.9) is a *non-trivial* 3-decomposition of $\mathcal{A}$ thus there exist $b'$, $c'$, $d'$ with

$$b' \neq 0, \quad c' \neq 0, \quad d' \neq 0 \tag{5.11}$$

and

$$b' \in \mathcal{B}', \quad c' \in \mathcal{C}', \quad d' \in \mathcal{D}'. \tag{5.12}$$

Then by (5.9), (5.10) and (5.12) we have

$$\{b', c', d', b'+c', b'+d', c'+d', b'+c'+d'\} \subset \{0, b'\} + \{0, c'\} + \{0, d'\} \subset \mathcal{B}' + \mathcal{C}' + \mathcal{D}' = \mathcal{A}. \tag{5.13}$$

Now we have to distinguish three cases. Assume first that none of $b', c', d'$ is equal to 1. Then by (5.11) and (5.13) we have

$$b', c', d' \in \mathcal{A} \backslash \{0, 1\}.$$

By (5.2) and (5.3), it follows from this that

$$\frac{p}{4} \leqslant b', c', d' < \frac{p}{2}$$

whence

$$\frac{p}{2} \leqslant b' + c', b' + d', c' + d' < p. \tag{5.14}$$

By (5.13) and (5.14) we have $b'+c', b'+d', c'+d' \in \mathcal{A} \cap \big[\frac{p}{2}, p\big)$ which contradicts the fact that, by (5.2) and (5.3), $\mathcal{A} \cap \big[\frac{p}{2}, p\big)$ is empty.

Now assume that exactly one of $b'$, $c'$ and $d'$ is equal to 1; we may assume that $b' = 1$, $c' \neq 1$, $d' \neq 1$. Then by (5.11) we have

$$c', d' \notin \{0, 1\}$$

so that by (5.2), (5.3) and (5.13) we have

$$c', d' \in \mathcal{A} \backslash \{0, 1\} = \mathcal{A}_0 \subset \left[\frac{p}{4}, \frac{p}{2}\right)$$

whence

$$\frac{p}{4} \leqslant c', d' < \frac{p}{2},$$

$$\frac{p}{2} \leqslant c' + d' < p. \tag{5.15}$$

By (5.13) and (5.15) again we have $c' + d' \in \mathcal{A} \cap \left[\frac{p}{2}, p\right)$ which contradicts $\mathcal{A} \cap \left[\frac{p}{2}, p\right) = \varnothing$.

Finally, assume that at least two of $b', c'$ and $d'$ are equal to 1; we may assume that $b' = c' = 1$. Then by (5.13) we have

$$b' + c' = 2 \in \mathcal{A}.$$

Since $p > 9$ it follows from this that

$$2 \in \mathcal{A} \cap (1, p/4)$$

which contradicts the fact that by (5.2) and (5.3) we have $\mathcal{A} \cap (1, p/4) = \varnothing$.

Thus in each of the three cases (5.8) leads to a contradiction which proves that (5.8) cannot hold so that $\mathcal{A}$ is not 3-reducible.

In order to prove (5.7), consider all the non-empty subsets $\mathcal{E}_0$ of $\mathbb{F}_p$ with

$$\mathcal{E}_0 \subset \left[\frac{p}{4}, \frac{3p}{8}\right), \tag{5.16}$$

and write such a set $\mathcal{E}_0$ as the union of blocks of consecutive integers with gaps between these blocks:

$$\mathcal{E}_0 = \bigcup_{j=1}^{r} \{e_j, e_j + 1, \dots, e_j'\} \tag{5.17}$$

with

$$e_j' \geqslant e_j \quad \text{for} \;\; j = 1, 2, \dots, r \tag{5.18}$$

and

$$e_{j+1} \geqslant e_j' + 2 \quad \text{for} \;\; j = 1, 2, \dots, r-1; \tag{5.19}$$

denote the set of these subsets $\mathcal{E}_0$ by $\mathbb{H}$. To every $\mathcal{E}_0 \in \mathbb{H}$ we assign the set $\mathcal{A}_0 = \mathcal{A}_0(\mathcal{E}_0)$ defined in the following way: first we define the elements $a_j$, $a_j'$ with $j = 1, 2, \dots, r$ by

$$a_j = e_j + (j-1) \quad \text{and} \quad a_j' = e_j' + j \quad \text{for} \;\; j = 1, 2, \dots, r, \tag{5.20}$$

and then define $\mathcal{A}_0 = \mathcal{A}_0(\mathcal{E}_0)$ by (5.4) and the set $\mathcal{A} = \mathcal{A}(\mathcal{E}_0)$ by (5.2). Then by (5.16), (5.17), (5.18), (5.19) and (5.20), each of (5.4), (5.5) and (5.6) holds trivially for every $\mathcal{A}_0 = \mathcal{A}_0(\mathcal{E}_0)$ with $\mathcal{E}_0 \in \mathbb{H}$. In order to prove (5.3), observe that for $a \in \mathcal{A}_0 = \mathcal{A}_0(\mathcal{E}_0)$ we have

$$a \geqslant e_1 \geqslant \frac{p}{4} \quad (\text{for} \;\; a \in \mathcal{A}_0(\mathcal{E}_0)). \tag{5.21}$$

Moreover, it also follows from (5.16)–(5.20) that

$$\frac{3p}{8} > e'_r = \sum_{j=1}^{r}(e'_j - e_j) + \sum_{j=1}^{r-1}(e_{j+1} - e'_j) + e_1 \geqslant \sum_{j=1}^{r} 0 + \sum_{j=1}^{r-1} 2 + \left[\frac{p}{4}\right] = 2(r-1) + \left[\frac{p}{4}\right]$$

whence, by $p > 22$,

$$r < \frac{1}{2}\left(\frac{3p}{8} - \left[\frac{p}{4}\right]\right) + 1 \leqslant \frac{1}{2}\left(\frac{3p}{8} - \frac{p-3}{4}\right) + 1 = \frac{p}{16} + \frac{11}{8} < \frac{p}{8}$$

so that, by (5.16) and (5.20), for every $a \in \mathcal{A}_0 = \mathcal{A}_0(\mathcal{E}_0)$ we have

$$a \leqslant a'_r = e'_r + r < \frac{3p}{8} + \frac{p}{8} = \frac{p}{2} \quad (\text{for} \quad a \in \mathcal{A}_0(\mathcal{E}_0)). \tag{5.22}$$

(5.3) follows from (5.21) and (5.22).

Thus all the sets $\mathcal{A} = \mathcal{A}(\mathcal{E}_0)$ assigned to some $\mathcal{E}_0 \in \mathbb{H}$ satisfy the assumptions (5.2)–(5.6) in the theorem so that they belong to $\mathbb{G}$. Clearly, if $\mathcal{E}_0$, $\mathcal{E}'_0$ are distinct subsets of $\mathbb{H}$ then we have $\mathcal{A}(\mathcal{E}_0) \neq \mathcal{A}(\mathcal{E}'_0)$ so that $|\mathbb{H}| = |\mathbb{G}|$. Thus it remains to estimate $|\mathbb{H}|$, i.e., the number of non-empty subsets of $\mathbb{F}_p$ satisfying (5.16). This is clearly

$$(|\mathbb{G}| =)\ |\mathbb{H}| = 2^{|\{n:\ n \in \mathbb{N},\ p/4 \leqslant n < 3p/8\}|} - 1 \geqslant 2^{p/8-1} - 1 > 2^{p/8-2}$$

which completes the proof of Theorem 4. □

# 6 The estimate of the greatest $k$ such that a given subset of $\mathbb{F}_p$ has a $k$-reducible subset

Now we will extend Theorem 2 by showing that large subsets of $\mathbb{F}_p$ also have $k$-reducible subsets for some large $k$:

**Theorem 5.** *If $p$ is a prime number with $p > p_0$, $\mathcal{A} \subset \mathbb{F}_p$,*

$$|\mathcal{A}| \geqslant p^{4/5}, \tag{6.1}$$

*and we write*

$$k = \left[\frac{11}{10} \log \frac{\log 3p}{\log(3p/|\mathcal{A}|)}\right], \tag{6.2}$$

*then $\mathcal{A}$ has a $k$-reducible subset $\mathcal{B}$.*

(Note that if $|\mathcal{A}| = p^{1-o(1)}$ then we have $k \to \infty$ for the number $k$ in (6.2), while for $|\mathcal{A}| \gg p$ we have $k \gg \log\log p$.)

*Proof of Theorem 5.* We will need

**Definition 7.** If $\mathcal{G}$ is an additive group, $d \in \mathbb{N}$ and $y$, $x_1, x_2, \dots, x_d$ are elements of $\mathcal{G}$ with $x_i \neq 0$ for $i = 1, 2, \dots, d$, then the set

$$\mathcal{H} = \left\{ y + \sum_{i=1}^{d} \varepsilon_i x_i : \ \varepsilon_i \in \{0, 1\} \ \text{ for } i = 1, 2, \dots, d \right\} \tag{6.3}$$

is called a *$d$-dimensional Hilbert cube.*

An infinite version of the Hilbert cube occurred first in Hilbert's paper [11]; see also [6], [7], [9], [10], [14], [19]. We will need the following quantitative Hilbert cube theorem proved in [14]:

**Lemma 3.** *If $N > N_0$, $\mathcal{E} \subset \{1, 2, \dots, N\}$ with*

$$|\mathcal{E}| \geqslant N^{4/5} \tag{6.4}$$

*and we write*

$$d = \left[ \frac{11}{10} \log \frac{\log 3N}{\log(3N/|\mathcal{E}|)} \right], \tag{6.5}$$

*then there exists a $d$-dimensional Hilbert cube $\mathcal{H}$ of form* (6.3) *with $x_i \neq x_j$ for $1 \leqslant i < j \leqslant d$ in $\mathcal{E}$:*

$$\mathcal{H} = \left\{ y + \sum_{i=1}^{d} \varepsilon_i x_i : \ \varepsilon_i \in \{0, 1\} \ \textit{ for } i = 1, 2, \dots, d \right\} \subset \mathcal{E}.$$

In order to prove the statement of Theorem 5 we identify $\mathbb{F}_p$ with the field of the modulo $p$ residue classes, and we represent each of the modulo $p$ residue classes belonging to $\mathcal{A}$ by the least positive integer in the given residue class; denote the set of these representant elements by $\mathcal{A}'$. Then by (6.1) and (6.2), we may apply Lemma 3 with $p$, $\mathcal{A}'$ and $k$ in place of $N$, $\mathcal{E}$ and $d$, respectively. We obtain that there is a $k$-dimensional Hilbert cube $\mathcal{H}'$ in $\mathcal{A}'$:

$$\mathcal{H}' = \left\{ y' + \sum_{i=1}^{k} \varepsilon_i x_i' : \ ve_i \in \{0, 1\} \ \text{ for } i = 1, 2, \dots, k \right\} \subset \mathcal{A}'.$$

It follows that if the residue classes represented by $y', x_1', \dots, x_k'$ are denoted by $y, x_1, \dots, x_k$, respectively, then we have

$$\mathcal{H} = \left\{ y + \sum_{i=1}^{k} \varepsilon_i x_i : \ \varepsilon_i \in \{0, 1\} \ \text{ for } i = 1, 2, \dots, k \right\} \subset \mathcal{A}. \tag{6.6}$$

If we write $\mathcal{B}_1 = \{y, y + x_1\}$ and $\mathcal{B}_i = \{0, x_i\}$ for $i = 2, \dots, k$, then (6.6) can be rewritten as

$$\mathcal{H} = \mathcal{B}_1 + \mathcal{B}_2 + \cdots + \mathcal{B}_k \subset \mathcal{A} \tag{6.7}$$

so that $\mathcal{H}$ is a $k$-reducible subset of $\mathcal{A}$ which completes the proof of Theorem 5. □

# 7 Balanced decompositions of large reducible subsets

Now we return to the problem described at the end of Section 3: we will show that if $\mathcal{A}$ is a large subset of $\mathbb{F}_p$ then it has a reducible subset which has a decomposition $\mathcal{B} + \mathcal{C}$ such that *both* $\mathcal{B}$ and $\mathcal{C}$ are large. Observe that such a result follows easily from Theorem 5 and its proof:

**Corollary 2.** *If $p$, $\mathcal{A}$ and $k$ are defined as in Theorem 5, then $\mathcal{A}$ has a reducible subset $\mathcal{R}$ such that it has a decomposition*

$$\mathcal{R} = \mathcal{B} + \mathcal{C} \tag{7.1}$$

*with*

$$\min\{|\mathcal{B}|, |\mathcal{C}|\} \geqslant [k/2] + 1. \tag{7.2}$$

*Proof of Corollary 2.* By using the notations in the proof of Theorem 5, we will show that taking $\mathcal{R}$ as the set $\mathcal{H}$ in (6.6) and (6.7), and $\mathcal{B}, \mathcal{C}$ as

$$\mathcal{B} = \mathcal{B}_1 + \mathcal{B}_2 + \cdots + \mathcal{B}_{[k/2]}, \quad \mathcal{C} = \mathcal{B}_{[k/2]+1} + \cdots + \mathcal{B}_{k-1} + \mathcal{B}_k, \tag{7.3}$$

these sets $\mathcal{R}$, $\mathcal{B}$ and $\mathcal{C}$ satisfy $\mathcal{R} \subset \mathcal{A}$, (7.1) and (7.2). Indeed, $\mathcal{R} \subset \mathcal{A}$ and (7.1) follow from (6.7) and (7.3). In order to prove (7.2) we need

**Lemma 4.** *If $\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_t$ are subsets of $\mathbb{F}_p$ with $|\mathcal{D}_1| = |\mathcal{D}_2| = \cdots = |\mathcal{D}_t| = 2$, then we have*

$$\left|\mathcal{D}_1 + \mathcal{D}_2 + \cdots + \mathcal{D}_t\right| \geqslant \min\{t + 1, p\}.$$

*Proof of Lemma 4.* This follows easily from the Cauchy–Davenport inequality by induction.

(7.2) follows from the definition of the sets $\mathcal{B}_i$, (7.3) and Lemma 4, and this completes the proof of Corollary 2. □

Note that in the proof of Corollary 2 we did not use the fact that in Lemma 3 it is also stated that the "generating elements" $x_1, x_2, \dots, x_d$ of the Hilbert cube $\mathcal{H}$ are pairwise distinct. If we also use this fact, then with some work the lower bound in (7.2) could be improved, perhaps, to $\gg k^2$ (but certainly not beyond that); for $|\mathcal{A}| \gg p$ this would give the lower bound

$$\min\{|\mathcal{B}|, |\mathcal{C}|\} \gg (\log\log p)^2 \tag{7.4}$$

for the size of the summands $\mathcal{B}$, $\mathcal{C}$ in (7.1) (while (7.2) gives only the lower bound $\gg \log\log p$). Next we will show that by adding a further idea, one can improve on these estimates significantly.

We will introduce the following definition:

**Definition 8.** If the Hilbert cube $\mathcal{H}$ in (6.3) is such that the sums $\sum\limits_{i=1}^{d} \varepsilon_i x_i$ (with $\varepsilon_i \in \{0,1\}$ for $i = 1, 2, \dots, d$) are pairwise distinct, in other words,

$$|\mathcal{H}| = \left|\left\{y + \sum_{i=1}^{d} \varepsilon_i x_i : \ \varepsilon_i \in \{0,1\} \ \text{ for } i = 1, 2, \dots, d\right\}\right| = 2^d,$$

then $\mathcal{H}$ will be called a *non-degenerate* $d$-dimensional Hilbert cube.

We will need the following sharpening (of independent interest) of the quantitative Hilbert theorem in Lemma 3:

**Lemma 5.** *If $N > N_0$, $\mathcal{E} \subset \{1, 2, \dots, N\}$ and* (6.4) *hold, and d is defined by* (6.5)*, then there exists a* non-degenerate *$d$-dimensional Hilbert cube $\mathcal{H}^*$ in $\mathcal{E}$:*

$$\mathcal{H}^* = \left\{y^* + \sum_{i=1}^{d} \varepsilon_i x_i^* : \ \varepsilon_i \in \{0,1\} \ \textit{ for } i = 1, 2, \dots, d\right\} \subset \mathcal{E} \tag{7.5}$$

*with*

$$|\mathcal{H}^*| = 2^d. \tag{7.6}$$

(Note that (7.6) implies that $x_i^* \neq x_j^*$ for $1 \leqslant i < j \leqslant d$.)

*Proof of Lemma 5.* The proof is similar to the proof of Lemma 3 above given in [14] thus we will leave some details to the reader. □

It suffices to show the existence of sets $\mathcal{E}_0, \mathcal{E}_1, \dots, \mathcal{E}_d$ and positive integers $x_1^*, x_2^*, \dots, x_d^*$ such that

$$\mathcal{E}_0 = \mathcal{E}, \tag{7.7}$$

$$\mathcal{E}_k + \left\{0, x_k^*\right\} \subset \mathcal{E}_{k-1} \quad \text{for} \ \ k = 1, 2, \dots, d, \tag{7.8}$$

$$x_k^* \notin \left\{ \sum_{i=1}^{k-1} \delta_i x_i^* : \ \delta_i \in \{-1,0,+1\} \text{ for } i=1,2,\dots,k-1 \right\} \text{ for } k=2,3,\dots,d, \tag{7.9}$$

$$|\mathcal{E}_k| \geqslant |\mathcal{E}|^{2^k}/(3N)^{2^k-1} \quad \text{for} \quad k=1,2,\dots,d. \tag{7.10}$$

Indeed, if $\mathcal{E}_0, \mathcal{E}_1, \dots, \mathcal{E}_d$, $x_1^*, x_2^*, \dots, x_d^*$ satisfy these conditions, then by (7.7) and (7.8), (7.5) holds for any $y^* \in \mathcal{E}_d$, while (7.10) implies that $\mathcal{E}_d$ is not empty. Now we have to show that the Hilbert cube $\mathcal{H}^*$ in (7.5) is non-degenerate, i.e., the assumption that there are distinct $d$-tuples $(\varepsilon_1, \dots, \varepsilon_d)$, $(\varepsilon'_1, \dots, \varepsilon'_d) \in \{0,1\}^d$ with

$$\varepsilon_1 x_1^* + \varepsilon_2 x_2^* + \cdots + \varepsilon_d x_d^* = \varepsilon'_1 x_1^* + \varepsilon'_2 x_2^* + \varepsilon'_d x_d^* \tag{7.11}$$

leads to contradiction. If (7.11) holds, then let $k$ denote the greatest subscript for which $\varepsilon_k \neq \varepsilon'_k$. Then $x_k^*$ can be expressed from (7.11) in the form

$$x_k^* = \sum_{i=1}^{k-1} \delta_i x_i^* \quad \text{with} \quad \delta_i \in \{-1,0,+1\} \quad \text{for} \quad i=1,2,\dots,k-1$$

which, in fact, contradicts (7.9). This then will complete the proof of Lemma 5.

We will construct $\mathcal{E}_0, \mathcal{E}_1, \dots, \mathcal{E}_d$, $x_1^*, x_2^*, \dots, x_d^*$ recursively. Let $\mathcal{E}_0 = \mathcal{E}$. Assume now that $0 \leqslant k \leqslant d-1$ and that $\mathcal{E}_0, \mathcal{E}_1, \dots, \mathcal{E}_k$ and, in the case $k > 0$, $x_1^*, x_2^*, \dots, x_k^*$ have already been defined. For $1 \leqslant h \leqslant N-1$ let $f(\mathcal{E}_k, h)$ denote the number of solutions of

$$e - e' = h, \quad \text{where} \quad e, e' \in \mathcal{E}_k.$$

Then in order to define $\mathcal{E}_{k+1}$ and $x_{k+1}^*$, we need an estimate for

$$F = \max f(\mathcal{E}_k, h) \tag{7.12}$$

where the maximum is taken over all $h$ with $1 \leqslant h \leqslant N-1$,

$$h \notin \left\{ \sum_{i=1}^{k} \delta_i x_i^* : \ \delta_i \in \{-1,0,+1\} \ \text{ for } i=1,2,\dots,k \right\}.$$

Clearly, for all $h$ we have $f(\mathcal{E}_k, h) \leqslant |\mathcal{E}_k|$. Moreover,

$$\sum_{h=1}^{N-1} f(\mathcal{E}_k, h) = \binom{|\mathcal{E}_k|}{2} \tag{7.13}$$

since $e-e' \in \{1,2,\dots,N-1\}$ for any pair $e, e' \in \mathcal{E}_k$ with $e > e'$. If we majorize $f(\mathcal{E}_k, h)$ by $|\mathcal{E}_k|$ for $h \in \left\{\sum_{i=1}^{k} \delta_i x_i^* :\ \delta_i \in \{-1,0,+1\} \text{ for } i = 1,2,\dots,k\right\}$ and by $F$ otherwise, then (7.13) implies

$$\binom{|\mathcal{E}_k|}{2} \leqslant 3^k|\mathcal{E}_k| + (N-1-3^k)F < 3^k|\mathcal{E}_k| + NF$$

so that

$$F > \frac{1}{2N}\left(\left(|\mathcal{E}_k|^2 - |\mathcal{E}_k|\right) - 2\cdot 3^k|\mathcal{E}_k|\right) = \frac{|\mathcal{E}_k|}{2N}\left(|\mathcal{E}_k| - 1 - 2\cdot 3^k\right). \tag{7.14}$$

Now we will show that here we have

$$1 + 2\cdot 3^k < \frac{1}{3}|\mathcal{E}_k| \tag{7.15}$$

which will follow from

$$3^{k+2} < |\mathcal{E}|.$$

By our induction assumption (7.10), it suffices to prove that

$$3^{k+2} < |\mathcal{E}|^{2^k}/(3N)^{2^k-1}$$

or, in equivalent form,

$$N > \left(\frac{3N}{|\mathcal{E}|}\right)^{2^k} \cdot 3^{k+1},$$

$$\log N > 2^k \log\frac{3N}{|\mathcal{E}|} + k\log 3 + \log 3.$$

The right-hand side is increasing in $k$, thus by $k \leqslant d-1$ we may replace the last inequality by

$$\log N > 2^d \log\frac{3N}{|\mathcal{E}|} + d\log 3 + \log 3. \tag{7.16}$$

By (6.4) and (6.5), the right-hand side can be estimated in the following way for $N$ large enough:

$$\begin{aligned}
&2^d \log\frac{3N}{|\mathcal{E}|} + d\log 3 + \log 3\\
&\quad< \exp\left((\log 2)\cdot\frac{11}{10}(\log\log 3N - \log\log 3N/|\mathcal{E}|) + \log\log 3N/|\mathcal{E}|\right)\\
&\qquad\qquad + O(\log\log N)
\end{aligned}$$

$$\begin{aligned}
&= \exp\left((\log 2)\cdot\frac{11}{10}\log\log 3N + \left(1-(\log 2)\frac{11}{10}\right)\log\log 3N/|\mathcal{E}|\right)\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad + O(\log\log N)\\
&= \exp\left((\log 2)\cdot\frac{11}{10}\log\log N + \left(1-(\log 2)\frac{11}{10}\right)\log\log N^{1/5} + o(1)\right)\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad + O(\log\log N)\\
&= \exp\left(\log\log N - \left(1-(\log 2)\frac{11}{10}\right)\log 5 + o(1)\right) + O(\log\log N)\\
&< \exp(\log\log N - 0.3825) + O(\log\log N) < 0.6821\log N. \qquad (7.17)
\end{aligned}$$

(7.16) and thus also (7.15) follow from (7.17). By (7.15), it follows from (7.14) that

$$F > \frac{|\mathcal{E}_k|}{2N}\cdot\frac{2}{3}|\mathcal{E}_k| = \frac{|\mathcal{E}_k|^2}{3N} \tag{7.18}$$

so that by the assumption (7.10) we have

$$F > \left(|\mathcal{E}|^{2^k}/(3N)^{2^k-1}\right)^2/3N = |\mathcal{E}|^{2^{k+1}}/(3N)^{2^{k+1}-1}. \tag{7.19}$$

Now let $x^*_{k+1} \in \{1,2,\dots,N-1\}\backslash\left\{\sum\limits_{i=1}^{k}\delta_i x^*_i \ :\ \delta_i \in \{-1,0,+1\} \text{ for } i = 1,2,\dots,k\right\}$ denote an integer $h$ for which the maximum in (7.12) is attained and let

$$\mathcal{E}_{k+1} = \left\{e \in \mathcal{E}_k : \ e + x^*_{k+1} \in \mathcal{E}_k\right\}.$$

Then (7.8) and (7.9) also hold with $k+1$ in place of $k$ and since $|\mathcal{E}_{k+1}| = F$, (7.19) implies (7.10) with $k+1$ in place of $k$. This completes the proof of the existence of $\mathcal{E}_0, \mathcal{E}_1, \dots, \mathcal{E}_d$, $x^*_1, x^*_2, \dots, x^*_d$ with the desired properties, so that Lemma 5 is proved. □

Now we are ready to prove the following sharpening of Corollary 2:

**Theorem 6.** *If $p$, $\mathcal{A}$ and $k$ are defined as in Theorem 5, then $\mathcal{A}$ has a reducible subset $\mathcal{R}^*$ such that it has a decomposition*

$$\mathcal{R}^* = \mathcal{B}^* + \mathcal{C}^* \tag{7.20}$$

*with*

$$\min\left\{|\mathcal{B}^*|, |\mathcal{C}^*|\right\} \geqslant 2^{[k/2]}. \tag{7.21}$$

(Observe that for $|\mathcal{A}| \gg p$ this gives the lower bound

$$\min\left\{|\mathcal{B}^*|, |\mathcal{C}^*|\right\} \gg (\log p)^c$$

with $c = \frac{11}{20}\log 2$; compare this with the lower bound in (7.4).)

*Proof of Theorem 6.* We argue in the same way as in the proofs of Theorem 5 and Corollary 2, but we use Lemma 5 instead of Lemma 3. Then we obtain that $\mathcal{A}$ contains a *non-degenerate* $k$-dimensional Hilbert cube $\mathcal{H}^*$:

$$\mathcal{H}^* = \left\{ y^* + \sum_{i=1}^{k} \varepsilon_i x_i^* : \ \varepsilon_i \in \{0,1\} \ \text{ for } i = 1,2,\dots,k \right\} \subset \mathcal{A}. \tag{7.22}$$

Then writing $\mathcal{B}_1^* = \{y^*, y^* + x_1^*\}$ and $\mathcal{B}_i^* = \{0, x_i^*\}$ for $i = 1,2,\dots,k$, and taking $\mathcal{R}^* = \mathcal{H}^*$, $\mathcal{B}^* = \mathcal{B}_1^* + \mathcal{B}_2^* + \dots + \mathcal{B}_{[k/2]}^*$ and $\mathcal{C}^* = \mathcal{B}_{[k/2]+1}^* + \dots + \mathcal{B}_{k-1}^* + \mathcal{B}_k^*$, (7.20) follows from (7.21), and $\mathcal{B}^*$, $\mathcal{C}^*$ are also *non-degenerate* Hilbert cubes of dimension $[k/2]$ and $k - [k/2] \geqslant [k/2]$, respectively, thus their cardinalities satisfy (7.21). □

# References

[1] N. Alon, A. Granville and A. Ubis, The number of sumsets in a finite field, *Bull. London Math. Soc.* **42** (2010), 784–794.

[2] S. Chowla, Solution of a problem of Erdős and Turán in additive number theory, *Proc. Nat. Acad. Sci. India* **14** (1944), 1–2.

[3] C. Dartyge and A. Sárközy, On additive decompositions of the set of primitive roots modulo $p$, *Monatsh. Math.* **169** (2013), 317–328.

[4] P. Erdős, Addendum, On a problem of Sidon in additive number theory and on some related problems, *J. London Math. Soc.* **19** (1944), 208.

[5] P. Erdős and P. Turán, On a problem of Sidon in additive number theory, and some related problems, *J. London Math. Soc.* **16** (1941), 212–215.

[6] P. Erdős, A. Sárközy and V. T. Sós, On a conjecture of Roth and some related problems, I, in: *Irregularities of Partitions*, eds. G. Halász et al., Springer, Berlin, 1989; pp. 47–59.

[7] H. Fürstenberg and B. Weiss, Topological dynamics and combinatorial number theory, *J. Analyse Math.* **34** (1978), 61–85.

[8] K. Gyarmati and A. Sárközy, On reducible and primitive subsets of $\mathbb{F}_p$, I, *Integers (EJCNT)*, to appear.

[9] R. Graham, B. Rothschild and J. H. Spencer, *Ramsey Theory*, Wiley, 1980.

[10] N. Hegyvári and A. Sárközy, On Hilbert cubes in certain sets, *Ramanujan J.* **3** (1999), 303–314.

[11] D. Hilbert, Über die Irreduzibilität ganzer rationaler Functionen mit ganzzahligen Koeffizienten, *J. Reine Angew. Math.* **110** (1892), 104–129.

[12] H.-H. Ostmann, Untersuchungen über den Summenbegriff in der additiven Zahlentheorie, *Math. Ann.* **120** (1948), 165–196.

[13] H.-H. Ostmann, *Additive Zahlentheorie*, Springer, Berlin, 1956.

[14] C. Pomerance, A. Sárközy and C. L. Stewart, On divisors of sums of integers, III, *Pacific J. Math.* **133** (1988), 363–379.

[15] A. Sárközy, Some metric problems in the additive number theory, II, *Annales Univ. Sci. Budapest. Eötvös* **20** (1977), 111–129.

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

[17] J. D. Shkredov, Sumsets in quadratic residues, *Acta Arith.*, to appear.

[18] J. E. Shparlinski, Additive decompositions of subgroups of finite fields, arXiv: 1301.2872v1 [math.NT]

[19] E. Szemerédi, On sets of integers containing no four elements in arithmetic progression, *Acta Math. Acad. Sci. Hungar.* **20** (1969), 89–104.