ON REDUCIBLE AND PRIMITIVE SUBSETS OF $\mathbb{F}_P$, I

Katalin Gyarmati[1]
Department of Algebra and Number Theory, Eötvös Loránd University
and *MTA-ELTE Geometric and Algebraic Combinatorics Research Group,*
Budapest, Hungary
gykati@cs.elte.hu

András Sárközy[1]
Department of Algebra and Number Theory, Eötvös Loránd University,
Budapest, Hungary
sarkozy@cs.elte.hu

Received: 10/18/13, Revised: 2/23/15, Accepted: 3/18/15, Published: 6/15/15

Abstract

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 $\mathcal{B}, \mathcal{C} \subset \mathbb{F}_p$, $|\mathcal{B}|, |\mathcal{C}| \geq 2$. If there are no sets $\mathcal{B}, \mathcal{C}$ with these properties then $\mathcal{A}$ is said to be primitive. First three criteria are presented for primitivity of subsets of $\mathbb{F}_p$. Then the distance between a given set $\mathcal{A} \subset \mathbb{F}_p$ and the closest primitive set is studied.

–Dedicated to the memory of Paul Erdős on the occasion of the 100th anniversary of his birthday.

1. Introduction

We will need

Definition 1. Let $\mathcal{G}$ be an additive semigroup and $\mathcal{A}, \mathcal{B}_1, \ldots, \mathcal{B}_k$ subsets of $\mathcal{G}$ with

$$|\mathcal{B}_i| \geq 2 \quad for\ i = 1, 2, \ldots, k. \tag{1.1}$$

If

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

then this is called an (additive) k-decomposition of $\mathcal{A}$, while if a multiplication is defined in $\mathcal{G}$ and (1.1) and

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

[1]Research partially supported by ERC-AdG.228005, Hungarian National Foundation for Scientific Research, grants no. K100291 and NK104183.
[1]Research partially supported by ERC-AdG.228005, Hungarian National Foundation for Scientific Research, grants no. K100291 and NK104183.

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 [16], [17] 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 $\mathcal{C} = \mathcal{A} + \mathcal{B}$ *with* $|\mathcal{A}| \geq 2,\ |\mathcal{B}| \geq 2$. 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 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.

Ostmann also formulated the following beautiful conjecture:

Conjecture 1. The set $\mathcal{P}$ of the primes is totally primitive.

If $\mathcal{A}$ is an infinite set of non-negative integers, then let $A(n)$ denote its *counting function*:

$$A(n) = |\{a :\ a \leq n,\ a \in \mathcal{A}\}|\,.$$

Inspired by Ostmann's work, Turán asked the following question: is it true that if $\mathcal{A}$ is any infinite set of non-negative integers then one can change at most $o(A(n))$ elements of it up to n so that the new set $\mathcal{A}'$ should be totally primitive? Sárközy [24] gave an affirmative answer to this question (Theorems A, B and C will be presented here in a slightly simplified form):

Theorem A *There is a positive absolute constant c such that if $\mathcal{A}$ is an infinite set of non-negative integers then one can change elements of it so that the number of the elements changed in $[0, n]$ is less than $c\frac{A(n)}{(\log\log A(n))^{1/2}}$ for every $n > n_0$ and the new set $\mathcal{A}'$ is totally primitive.*

Answering a question of Erdős, Sárközy [25] also proved:

Theorem B *There is a positive absolute constant c' such that if $\mathcal{A}$ is an infinite set of non-negative integers, and its complement $\overline{\mathcal{A}} = \{0, 1, 2, \dots\} \setminus \mathcal{A}$ satisfies*

$$\overline{A}(n) = |\{\overline{a} :\ 0 \leq \overline{a} \leq n,\ \overline{a} \notin \mathcal{A}\}| < c'\left(\frac{n\,(\log\log n)^2}{(\log n)^4}\right)^{1/3} \tag{1.3}$$

for $n \geq 3$, then $\mathcal{A}$ is reducible.

Erdős also conjectured that if we change $o(n^{1/2})$ elements of the set of squares up to n, then the new set is always totally primitive. Sárközy and Szemerédi [27] proved this conjecture in the following slightly weaker form:

Theorem C *If $\varepsilon > 0$ and we change $o(n^{1/2-\varepsilon})$ elements of the set of the squares up to n then we get a totally primitive set.*

Volkmann [28], [29] Wirsing [30] and Sárközy [19], [20] estimated the Lebesgue measure, resp. Hausdorff dimension of the point set assigned to reducible sets.

Hornfeck [15], Hofmann and Wolke [14], Elsholtz [5], [6], [7] and Puchta [18] proved partial results toward Ostmann's Conjecture 1 on the totally primitivity of the set $\mathcal{P}$ of the primes. Elsholtz [8] also studied multiplicative decompositions of shifted sets $\mathcal{P}' + \{a\}$ with $\mathcal{P}' \sim \mathcal{P}$.

So far we have surveyed the papers written on decompositions of sets of *integers*. Sárközy [26] proposed to study analogous problems in *finite fields*. Observe that 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.

First (inspired by Erdős's problem and Theorem C on the set of squares) it was conjectured in [26] that for every prime p the set of the modulo p quadratic residues is primitive. (We will identify $\mathbb{F}_p$ with the set of the residue classes modulo p and, as it is customary, we will not distinguish between residue classes and the integers representing them.) This conjecture is still open but partial results have been proved by Sárközy [26], Shkredov [22] and Shparlinski [23].

Dartyge and Sárközy [3] conjectured that the set of modulo p primitive roots is primitive. This conjecture is also still open but partial results have been proved by Dartyge and Sárközy [3] and Shparlinski [23].

Sárközy [21] also studied multiplicative decompositions of the shifted set of the modulo p quadratic residues.

By Theorem B every infinite set $\mathcal{A}$ of non-negative integers satisfying (1.3) is reducible, and by Theorem A, the upper bound in (1.3) for $\overline{A}(n)$ cannot be replaced by $O\left(\frac{n}{(\log\log n)^{1/2}}\right)$. In a recent paper Gyarmati, Konyagin and Sárközy [11] studied the analogue of these results in finite fields: they estimated *the cardinality $f(p)$ of the largest primitive subset* of $\mathbb{F}_p$. Note that earlier Green, Gowers and Green [12], [13], and Alon [1] had studied a closely related problem: they estimated the cardinality $g(p)$ of the largest subset $\mathcal{A}$ of $\mathbb{F}_p$ which cannot be represented in form $\mathcal{B} + \mathcal{B} = \mathcal{A}$. Clearly $f(p) \le g(p)$. Improving on results of Gowers and Green, Alon proved that

$$p - c_1 \frac{p^{2/3}}{(\log p)^{1/3}} < g(p) < p - c_2 \frac{p^{1/2}}{\log p}.$$

In [11] we proved that $f(p)$ is much smaller than this: for $p > p_0$ we have

$$p - c_3 \frac{\log\log p}{(\log p)^{1/2}} p < f(p) < p - c_4 \frac{p}{\log p}. \tag{1.4}$$

Alon, Granville and Ubis [2] estimated the number of distinct sumsets $\mathcal{A}+\mathcal{B}$ in $\mathbb{F}_p$ under various assumptions on the cardinality of $\mathcal{A}$ and $\mathcal{B}$. Among others they proved that there are $2^{p/2+o(p)}$ distinct sumsets $\mathcal{A}+\mathcal{B}$ in $\mathbb{F}_p$ with $|\mathcal{A}|,\ |\mathcal{B}| \to \infty$ as $p \to \infty$. They also proved

Theorem D *There are less than* $(1.9602)^{p+o(p)}$ *reducible subsets of* $\mathbb{F}_p$.

(So that almost all of the 2^p subsets of $\mathbb{F}_p$ are primitive.)

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. First in Section 2 we will present three criteria for primitivity of a subset $\mathcal{A}$ of $\mathbb{F}_p$. Then in Section 3 we will show that these criteria are independent: neither of them follows from any of the others. In Section 4 we will show that any "small" subset of $\mathbb{F}_p$ can be made primitive by adding just one element. Finally, in Section 5 we will discuss a problem on the finite field analogue of Theorem A. (In the sequel of this paper we will extend the notions of reducibility and primitivity, and we will study these extended notions.)

2. Three Criteria for Primitivity in $\mathbb{F}_p$.

Ostmann and others have given several criteria for primitivity of sequences of integers, but no primitivity criteria are known in $\mathbb{F}_p$. Thus we will present three criteria of this type, then we will illustrate their applicability, and we will also study the connection between them.

Theorem 1. *Assume that* $\mathcal{A} = \{a_1, a_2, \dots, a_t\} \subset \mathbb{F}_p$ *and there are* i, j *with* $1 \le i < j \le t$ *such that*

$$a_i + a_j - a_k \notin \mathcal{A} \qquad \text{for every } k \text{ with } 1 \le k \le t,\ k \ne i,\ k \ne j \tag{2.1}$$

and

$$a_i - a_j + a_k \notin \mathcal{A} \qquad \text{for every } k \text{ with } 1 \le k \le t,\ k \ne j. \tag{2.2}$$

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

Corollary 1. *If* p *is a prime of form* $p = 4k+1$ *and* $\mathcal{A} \subset \mathbb{F}_p$ *is defined by*

$$\mathcal{A} = \{0,1\} \cup \{a \in \mathbb{F}_p :\ \left(\frac{a}{p}\right) = 1,\ \left(\frac{a-1}{p}\right) = -1,\ a \ne -1,\ a \ne 2\},$$

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

Corollary 2. *If $\mathcal{A} = \{a_1, a_2, \ldots, a_t\} \subset \mathbb{F}_p$ is a* Sidon set*, then it is primitive.*

(A set $\mathcal{A} = \{a_1, a_2, \ldots, a_t\}$ is called Sidon set if the sums $a_i + a_j$ with $1 \le i < j \le t$ are distinct.)

Proof of Theorem 1. Assume that contrary to the statement of the theorem $\mathcal{A}$ is a set satisfying the assumptions, however, there are $\mathcal{B} \subset \mathbb{F}_p$, $\mathcal{C} \subset \mathbb{F}_p$ with

$$\mathcal{A} = \mathcal{B} + \mathcal{C}, \quad |\mathcal{B}| \ge 2, \ |\mathcal{C}| \ge 2. \tag{2.3}$$

It follows from $a_i \in \mathcal{A}$, $a_j \in \mathcal{A}$ and (2.3) that there are $b_u \in \mathcal{B}$, $b_v \in \mathcal{B}$, $c_x \in \mathcal{C}$ and $c_y \in \mathcal{C}$ with

$$a_i = b_u + c_x \tag{2.4}$$

and

$$a_j = b_v + c_y. \tag{2.5}$$

Now we have to distinguish two cases.

`Case 1.` Assume that $b_u \ne b_v$ and $c_x \ne c_y$. Then by (2.3), (2.4) and (2.5) we have

$$a_i + a_j = (b_u + c_x) + (b_v + c_y) = (b_u + c_y) + (b_v + c_x) = a_r + a_s \tag{2.6}$$

with $a_r = b_u + c_y \in \mathcal{A}$ and $a_s = b_v + c_x \in \mathcal{A}$. Then

$$a_i \ne a_r \tag{2.7}$$

by (2.4) and $c_x \ne c_y$, and

$$a_j \ne a_r \tag{2.8}$$

by (2.5) and $b_u \ne b_v$. (2.6), (2.7) and (2.8) contradict (2.1) (with a_r in place of a_k).

`Case 2.` Assume that

$$b_u = b_v \tag{2.9}$$

or $c_x = c_y$; we may assume that (2.9) holds. Then (2.5) can be rewritten as

$$a_j = b_u + c_y.$$

By $|\mathcal{B}| \ge 2$ there is a $b \in \mathcal{B}$ with

$$b \ne b_u. \tag{2.10}$$

Then by (2.3) we have

$$a_p = b + c_x \in \mathcal{A} \tag{2.11}$$

and

$$a_q = b + c_y \in \mathcal{A}. \tag{2.12}$$

It follows from (2.4), (2.5), (2.9), (2.11) and (2.12) that

$$a_i - a_j = (b_u - b_v) + (c_x - c_y) = c_x - c_y = a_p - a_q$$

whence

$$a_i - a_j + a_q = a_p \in \mathcal{A} \tag{2.13}$$

where by (2.5), (2.9), (2.10) and (2.12)

$$a_q = b + c_y \neq b_u + c_y = b_v + c_y = a_j. \tag{2.14}$$

(2.13) and (2.14) contradict (2.2) which completes the proof of Theorem 1.

Proof of Corollary 1. By the construction of the set $\mathcal{A}$ we have $0 \in \mathcal{A}$ and $1 \in \mathcal{A}$. We will show that (2.1) and (2.2) in Theorem 1 hold with $a_i = 0$, $a_j = 1$; in other words, we have

$$1 - a_k \notin \mathcal{A} \qquad \text{for every } a_k \neq 0, 1 \tag{2.15}$$

and

$$-1 + a_k \notin \mathcal{A} \qquad \text{for every } a_k \neq 1. \tag{2.16}$$

Consider first (2.15). By the construction of $\mathcal{A}$, it follows from $a_k \in \mathcal{A}$, $a_k \neq 0$, $a_k \neq 1$ that $\left(\frac{a_k}{p}\right) = 1$ and $\left(\frac{a_k - 1}{p}\right) = -1$. Then by $p = 4k + 1$ we have

$$\left(\frac{1 - a_k}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{1 - a_k}{p}\right) = \left(\frac{a_k - 1}{p}\right) = -1.$$

This implies by the definition of $\mathcal{A}$ that $1 - a_k \in \mathcal{A}$ may hold only if $1 - a_k = 0$ or $1 - a_k = 1$ whence $a_k = 1$ or $a_k = 0$. But it is assumed in (2.15) that $a_k \neq 0, 1$, thus, indeed, (2.15) holds.

Now consider (2.16). It follows from $a_k \in \mathcal{A}$ and $a_k \neq 1$ that either $\left(\frac{a_k - 1}{p}\right) = -1$ whence $-1 + a_k \notin \mathcal{A}$ or we have $a_k = 0$ whence $-1 + a_k = -1$ which again does not belong to $\mathcal{A}$ so that (2.16) holds.

Proof of Corollary 2. If $|\mathcal{A}| = 1$ or 2, then $\mathcal{A}$ is primitive trivially. If $|\mathcal{A}| = t > 2$, then a_i, a_j in the theorem can be chosen as any two distinct elements of $\mathcal{A}$, e.g., we may take $a_i = a_1$ and $a_j = a_2$. Also, (2.1) and (2.2) in Theorem 1 hold trivially by the definition of Sidon sets which proves the primitivity of $\mathcal{A}$.

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

$$\mathcal{A} = \{0\} \cup \mathcal{A}_0 \quad \textit{with } \mathcal{A}_0 \subset (p/3, 2p/3), \tag{2.17}$$

and

$$|\mathcal{A}| > 4, \tag{2.18}$$

then $\mathcal{A}$ is primitive.

Proof of Theorem 2. Assume that contrary to the statement of the theorem (2.17) holds, however there are sets $\mathcal{B} \subset \mathbb{F}_p$, $\mathcal{C} \subset \mathbb{F}_p$ with

$$\mathcal{A} = \mathcal{B} + \mathcal{C}, \ |\mathcal{B}| \geq 2, \ |\mathcal{C}| \geq 2. \tag{2.19}$$

Since $0 \in \mathcal{A}$, thus it follows from (2.18) that there are $b_0 \in \mathcal{B}$, $c_0 \in \mathcal{C}$ with

$$0 = b_0 + c_0.$$

Write $\mathcal{B}' = \mathcal{B} + \{-b_0\}$ and $\mathcal{C}' = \mathcal{C} + \{-c_0\}$ so that $0 \in \mathcal{B}'$ and $0 \in \mathcal{C}'$ and, by (2.19),

$$\mathcal{B}' + \mathcal{C}' = \mathcal{B} + \mathcal{C} = \mathcal{A},\ |\mathcal{B}'| = |\mathcal{B}| \geq 2,\ |\mathcal{C}'| = |\mathcal{C}| \geq 2. \tag{2.20}$$

Represent every non-zero element of $\mathcal{B}'$ and $\mathcal{C}'$ by an integer from the interval $(0, p)$ and let $\mathcal{B}' = \{0, b_1', \ldots, b_r'\}$ and $\mathcal{C}' = \{0, c_1', \ldots, c_s'\}$ with

$$0 < b_1' < \cdots < b_r' < p \text{ and } 0 < c_1' < \cdots < c_s' < p \tag{2.21}$$

where $r \geq 1$ and $s \geq 1$, and by (2.18) and (2.20),

$$(r+1)(s+1) = |\mathcal{B}'|\,|\mathcal{C}'| \geq |\mathcal{A}| > 4.$$

It follows that

$$r \geq 2 \tag{2.22}$$

or $s \geq 2$; we may assume that (2.22) holds. Then by (2.20) and (2.21) we have

$$b_i' = b_i' + 0 \in \mathcal{B}' + \mathcal{C}' = \mathcal{A},\ 0 < b_i' < p \tag{2.23}$$

for $i = 1, 2, \ldots, r$ and

$$c_1' = c_1' + 0 \in \mathcal{B}' + \mathcal{C}' = \mathcal{A},\ 0 < c_1' < p. \tag{2.24}$$

By the construction of $\mathcal{A}$ it follows from (2.23) and (2.24) that

$$2\frac{p}{3} < b_i' + c_1' < \frac{4p}{3}, \tag{2.25}$$

and by (2.20) we have

$$b_i' + c_1' \in \mathcal{B}' + \mathcal{C}' = \mathcal{A}. \tag{2.26}$$

But it follows from the construction of $\mathcal{A}$ that it has only a single element in the interval $\left(\frac{2p}{3}, \frac{4p}{3}\right)$, namely $p\ (= 0)$. Thus by (2.25) and (2.26) we have

$$b_i' + c_1' = 0 \quad \text{for } i = 1, 2, \ldots, r.$$

By (2.22) this holds for both $i = 1$ and $i = 2$ so that

$$b_1' + c_1' = 0 = b_2 + c_1'$$

whence $b_1' = b_2'$ which contradicts (2.21) and this completes the proof of Theorem 2.

Theorem 3. *Let $\mathcal{A} \subset \mathbb{F}_p$ and for $d \in \mathbb{F}_p^*$ denote the number of solutions of*

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

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

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < |\mathcal{A}|^{1/2}, \tag{2.27}$$

then $\mathcal{A}$ is primitive.

Note that Corollary 2 also follows from this criterion trivially. (In the sequel of this paper we will also apply this criterion for proving a stronger result along these lines.)

Proof of Theorem 3. Assume that contrary to the statement of the theorem there are $\mathcal{B} \subseteq \mathbb{F}_p$, $\mathcal{C} \subseteq \mathbb{F}_p$ with

$$\mathcal{A} = \mathcal{B} + \mathcal{C},\ |\mathcal{B}| \geq 2,\ |\mathcal{C}| \geq 2. \tag{2.28}$$

We may assume that

$$|\mathcal{B}| \geq |\mathcal{C}|. \tag{2.29}$$

By (2.28) and (2.29) we have

$$|\mathcal{A}| = |\mathcal{B} + \mathcal{C}| \leq |\{(b, c) :\ b \in \mathcal{B},\ c \in \mathcal{C}\}| = |\mathcal{B}|\,|\mathcal{C}| \leq |\mathcal{B}|^2$$

whence

$$|\mathcal{A}|^{1/2} \leq |\mathcal{B}|. \tag{2.30}$$

It follows from (2.27) and (2.30) that

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) < |\mathcal{B}|. \tag{2.31}$$

On the other hand, let c and c' be two distinct elements of $\mathcal{C}$. Then by (2.28), for every $\mathcal{B}$ we have $a = b + c \in \mathcal{A}$ and $a' = b + c' \in \mathcal{A}$. For this pair (a, a') we have

$$a - a' = (b + c) - (b + c') = c - c',$$

and for different b values we get different solutions of

$$a - a' = c - c',\ a \in \mathcal{A},\ a' \in \mathcal{A}. \tag{2.32}$$

It follows that the number of solutions of (2.32) is at least as large as the number of b's:

$$f(\mathcal{A}, c - c') \geq |\mathcal{B}|. \tag{2.33}$$

Since $c \neq c'$ we have $c - c' \neq 0$ thus (2.32) contradicts (2.31) and this completes the proof of Theorem 3.

Now we will prove that Theorem 3 is sharp in the range $0 < |\mathcal{A}| \ll p^{1/2}$ (and in the next section we will also show that if a set $\mathcal{A} \subset \mathbb{F}_p$ satisfies the assumptions in Theorem 3 then we must have $|\mathcal{A}| \ll p^{1/2}$):

Theorem 4. *If p is large enough and k is a positive integer with*

$$k_0 < k < \frac{1}{2}p^{1/4}, \tag{2.34}$$

then there is a set $\mathcal{A} \subset \mathbb{F}_p$ such that

$$|\mathcal{A}| = k^2, \tag{2.35}$$

$$\max_{d \in \mathbb{F}_p^*} f(\mathcal{A}, d) = |\mathcal{A}|^{1/2} \tag{2.36}$$

and $\mathcal{A}$ is reducible.

Proof of Theorem 4. Write $m = 2k^2$. By theorems of Erdős and Turán [9], [10] and Chowla [4] the cardinality of the maximal Sidon set selected from $\{1, 2, \ldots, N\}$ is $(1 + o(1))N^{1/2}$. Thus for k large enough there is a Sidon set

$$\mathcal{B} = \{b_1, b_2, \ldots, b_k\} \subset \{1, 2, \ldots, m-1\} \quad \text{with } |\mathcal{B}| = k \ \left(= \left(\frac{m}{2}\right)^{1/2}\right). \tag{2.37}$$

Let $\mathcal{C} = \{c_1, c_2, \ldots, c_k\} = (2m) \times \mathcal{B} = \{2mb_1, 2mb_2, \ldots, 2mb_k\}$ and

$$\mathcal{A} = \mathcal{B} + \mathcal{C}. \tag{2.38}$$

Then clearly $\mathcal{A}$ is reducible. Moreover, every $a \in \mathcal{A}$ can be written in the form

$$a = b_i + c_j = b_i + 2mb_j \tag{2.39}$$

with some $i, j \in \{1, 2, \ldots, k\}$, and by (2.34) here we have

$$\begin{aligned} &0 < b_i < m, \ 0 < b_j < m \text{ and} \\ &0 < b_i + 2mb_j < m + 2m(m-1) < 2m^2 = 8k^4 < \frac{p}{2}. \end{aligned} \tag{2.40}$$

(2.39) and (2.40) determine b_i and c_j uniquely, thus we have

$$|\mathcal{A}| = |\mathcal{B} + \mathcal{C}| = |\mathcal{B}|\,|\mathcal{C}| = k^2 \tag{2.41}$$

which proves (2.35).

Finally, consider a $d \in \mathbb{F}_p^*$ with $f(\mathcal{A}, d) > 0$ so that there are a, a' with

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

Let a be of the form (2.39) and

$$a' = b_{i'} + c_{j'} = b_{i'} + 2mb_{j'}.$$

Then we have

$$d = a - a' = (b_i - b_{i'}) + 2m\,(b_j - b_{j'}) = u + 2mv \tag{2.42}$$

with

$$0 \le |b_i - b_{i'}| = |u| < m \tag{2.43}$$

$$0 \le |b_j - b_{j'}| = |v| < m \tag{2.44}$$

and, by (2.34),

$$|d| \le |u| + |2mv| = |b_i - b_{i'}| + 2m\,|b_j - b_{j'}| < m + 2m(m-1) < 2m^2 = 8k^4 < \frac{p}{2}. \tag{2.45}$$

By (2.43), (2.44) and (2.45), d determines u and v in (2.42) uniquely. If $u = b_i - b_{i'} \neq 0$ and $v = b_j - b_{j'} \neq 0$ then by the Sidon property of $\mathcal{B}$ the pair u, v determines $b_i, b_{i'}, b_j$ and $b_{j'}$, and thus also a and a' uniquely so that we have $f(\mathcal{A}, d) = 1$. If $u = b_i - b_{i'} = 0$ and $v = b_j - b_{j'} \neq 0$ then $i = i'$ can be chosen in k ways while v determines j and j' uniquely, thus, by (2.41),

$$f(\mathcal{A}, d) = k = |\mathcal{A}|^{1/2}. \tag{2.46}$$

Similarly, if $u = b_i - b_{i'} \neq 0$ and $v = b_j - b_{j'} = 0$ then $j = j'$ can be chosen in k ways while i, i' are uniquely determined thus again (2.46) holds and this also proves (2.36).

3. Comparison of Three Criteria

Let $\mathcal{F}_1, \mathcal{F}_2$ and $\mathcal{F}_3$ denote the family of the subsets $\mathcal{A}$ of $\mathbb{F}_p$ that satisfy the assumptions in Theorems 1, 2 and 3, respectively, and let L_1, L_2 and L_3 denote the cardinality of the largest subset belonging to $\mathcal{F}_1$, $\mathcal{F}_2$ and $\mathcal{F}_3$, respectively. First we will estimate $|\mathcal{F}_1|$, $|\mathcal{F}_2|$, $|\mathcal{F}_3|$, L_1, L_2 and L_3.

Theorem 5. *We have*
(i)

$$|\mathcal{F}_1| \ge 2^{p/2 - O(1)} \tag{3.1}$$

and

$$L_1 = \frac{p}{2} + O(1). \tag{3.2}$$

(ii)

$$|\mathcal{F}_2| = 2^{p/3 + O(1)} \tag{3.3}$$

and

$$L_2 = \frac{p}{3} + O(1). \tag{3.4}$$

(iii)

$$|\mathcal{F}_3| \le \exp\Big((1 + o(1))\, p^{2/3} \log p\Big) \tag{3.5}$$

and

$$L_3 \le (1 + o(1))\, p^{2/3}. \tag{3.6}$$

Proof of Theorem 5. (i) Write

$$\mathcal{B} = \left\{ b : \ -\frac{p-3}{2} \le b \le \frac{p-3}{2}, \ 2 \mid b, \ b \ne 0, 2 \right\}.$$

We will show that if $\mathcal{A}_0 \subset \mathcal{B}$ then

$$\mathcal{A} = \{0, 1\} \cup \mathcal{A}_0 \in \mathcal{F}_1. \tag{3.7}$$

It suffices to prove that such a set $\mathcal{A}$ satisfies (2.1) and (2.2) in Theorem 1 with $a_i = 1$, $a_j = 0$. For these values of a_i and a_j conditions (2.1) and (2.2) become

$$1 - a \notin \mathcal{A} \quad \text{for } a \in \mathcal{A}, \ a \ne 0, 1 \tag{3.8}$$

and

$$1 + a \notin \mathcal{A} \quad \text{for } a \in \mathcal{A}, \ a \ne 0. \tag{3.9}$$

Indeed, if $a \in \mathcal{A}$, $a \ne 0, 1$ then by $a \in \mathcal{A}_0 \subset \mathcal{B}$ we have

$$-\frac{p-1}{2} \le 1 - a, 1 + a \le \frac{p-1}{2}$$

and $a \in \mathcal{A}_0 \subset \mathcal{B}$ is even so that $1 - a$ and $1 + a$ are odd; thus $1 - a$, $1 + a \notin \mathcal{A}_0$ whence (3.8) and (3.9) follow; if $a = 1$ then $1 + a = 1 + 1 = 2 \notin \mathcal{A}_0$ thus again (3.9) holds.

Since clearly $|\mathcal{B}| = \frac{p}{2} - O(1)$, it follows that $\mathcal{A}_0 \subset \mathcal{B}$ (and also $\mathcal{A}$ in (3.7)) can be chosen in $2^{p/2-O(1)}$ ways, which proves (3.1).

Taking $\mathcal{A}_0 = \mathcal{B}$ in (3.7) we get that $\mathcal{A} = \{0, 1\} \cup \mathcal{B} \in \mathcal{F}_1$. Thus, clearly we have

$$L_1 \ge |\{0, 1\} \cup \mathcal{B}| \ge |\mathcal{B}| = \frac{p}{2} - O(1). \tag{3.10}$$

In order to give an upper bound for L_1 consider a set $\mathcal{A}$ which satisfies the assumptions in Theorem 1 with some fixed a_i, a_j. Then by (2.1), for any pair $a, a' \in \mathbb{F}_p$ with

$$a_i + a_j - a = a'$$

only at most one of a and a' may belong to $\mathcal{A}$. There are at most $\frac{p+1}{2}$ such pairs (including the pair (a, a') with $a = a'$), and every element of $\mathbb{F}_p$ belongs to one of these pairs. Thus $|\mathcal{A}|$ is at most $\frac{p+1}{2}$ (=the number of pairs) + 2 (to also count a_i and a_j) $= \frac{p}{2} + O(1)$, so that

$$L_2 \le \frac{p}{2} + O(1)$$

which, together with (3.10), proves (3.2).

(ii) The number of the sets $\mathcal{A}$ of form (2.17) is equal to the number of the sets $\mathcal{A}_0 \subset \mathbb{F}_p$ with $\mathcal{A}_0 \subset (p/3, 2p/3)$ which is clearly

$$2^{2p/3-p/3+O(1)} = 2^{p/3+O(1)}$$

which proves (3.3).

The maximal cardinality of a set $\mathcal{A}$ of form (2.17) is at most

$$|\mathcal{A}| \le |\{0\}| + |\mathcal{A}_0| \le 1 + |\{a:\ p/3 \le a < 2p/3\}| = \frac{p}{3} + O(1)$$

which proves (3.4).

(iii) If $\mathcal{A} \in \mathcal{F}_3$ then (2.27) holds so that

$$\sum_{d\in\mathbb{F}_p^*} f(\mathcal{A},d) < \sum_{d\in\mathbb{F}_p^*} |\mathcal{A}|^{1/2} = (p-1)\,|\mathcal{A}|^{1/2}. \tag{3.11}$$

On the other hand, clearly we have

$$\begin{aligned}\sum_{d\in\mathbb{F}_p^*} f(\mathcal{A},d) &= \sum_{d\in\mathbb{F}_p^*} |\{(a,a'):\ a,a'\in\mathcal{A},\ a-a'=d\}| \\ &= |\{(a,a'):\ a,a'\in\mathcal{A},\ a\ne a'| = |\mathcal{A}|\,(|\mathcal{A}|-1)\,. \end{aligned}\tag{3.12}$$

It follows from (3.11) and (3.12) that

$$|\mathcal{A}|^{1/2}\,(|\mathcal{A}|-1) < p-1. \tag{3.13}$$

Now assume that contrary to (3.6) there is an $\varepsilon > 0$ such that for infinitely many primes p there is an $\mathcal{A}\in\mathcal{F}_3$ with

$$|\mathcal{A}| > (1+\varepsilon)p^{2/3}. \tag{3.14}$$

It follows from (3.13) and (3.14) that

$$(1+\varepsilon)^{1/2}\,p^{1/3}\left((1+\varepsilon)p^{2/3}-1\right) < p-1$$

whence

$$(1+\varepsilon)^{3/2} - \frac{(1+\varepsilon)^{1/2}}{p^{2/3}} < 1 - \frac{1}{p}.$$

But for $p\to\infty$ the limit of the left hand side is $(1+\varepsilon)^{3/2}$ (>1) while the limit of the right hand side is 1, thus for p large enough this inequality cannot hold, and this contradiction proves (3.6).

It follows from (3.6) that

$$\begin{aligned}|\mathcal{F}_3| &\le |\{\mathcal{A}:\ \mathcal{A}\subset\mathbb{F}_p,\ |\mathcal{A}|\le L_3\}| = \sum_{k=1}^{L_3}\binom{p}{L_3} \le p\binom{p}{L_3} = p^{L_3+1} \\ &= \exp\left((1+o(1))p^{2/3}\log p\right)\end{aligned}$$

which proves (3.5) and this completes the proof of Theorem 5. (We remark that with a little work it could be also shown that (3.5) and (3.6) hold with equality sign but we do not need this here.)

Note that comparing (3.1), (3.3) and (3.5) we can see that Theorem 1 covers more primitive sets than Theorem 2 and Theorem 3, and both Theorem 1 and Theorem 2 cover much more primitive sets than Theorem 3. Moreover, by (3.2), (3.4) and (3.6) there are much larger primitive sets covered by Theorems 1 and 2 than by Theorem 3. In spite of this Theorem 3 seems to be at least as useful and applicable as the other two theorems since it covers almost all the thin subsets $\mathcal{A}$ of $\mathbb{F}_p$ (almost all the subsets $\mathcal{A}$ with $|\mathcal{A}| \ll p^{2/3}$); on the other hand, e.g. a set $\mathcal{A}$ satisfying Theorem 2 must have a very special structure: apart from $0 \in \mathcal{A}$, it must lie completely in the interval $(p/3, 2p/3)$.

Now we will show that Theorems 1, 2 and 3 are independent.

Proposition 1. *For p large enough Theorems 1, 2 and 3 are independent: for either of the three criteria there is an $\mathcal{A} \in \mathbb{F}_p$ which satisfies the conditions in it but which does not satisfy the conditions in the other two theorems.*

Proof of Proposition 1. By (3.1), (3.3) and (3.5) in Theorem 1 for p large enough there are much more subsets $\mathcal{A} \subset \mathbb{F}_p$ satisfying the assumptions in Theorem 1 than the ones in Theorems 2 and 3, and there are much more subsets satisfying the assumptions in Theorem 2 than the ones in Theorem 3.

There are (many) Sidon sets $\mathcal{A}$ with $\mathcal{A} \subset (0, p/3)$ and $|\mathcal{A}| > 1$; these sets $\mathcal{A}$ satisfies the assumptions in Theorem 3 but not (2.17) in Theorem 2.

With a little work it could be shown that almost all the subsets $\mathcal{A} \subset \mathbb{F}_p$ with $|\mathcal{A}| = \left[\frac{1}{2}n^{2/3}\right]$ satisfy the inequality

$$2 \le f(\mathcal{A}, d) < |\mathcal{A}|^{1/2} \quad \text{for every } d \in \mathbb{F}_p^*;$$

such a subset $\mathcal{A}$ satisfies the assumptions in Theorem 3 but not (2.2) in Theorem 1.

Finally, consider the set

$$\mathcal{A} = \{0\} \cup \{a : \ p/3 < a < 2p/3\}.$$

For p large enough this set satisfies the assumptions in Theorem 2. On the other hand, for any $a_i, a_j \in \mathcal{A}$ we also have $-a_i \in \mathcal{A}$ since $\mathcal{A}$ also contains the negative of every element of it; take $a_k = -a_i$ in (2.2). Then

$$a_i - a_j + a_k = a_i - a_j - a_i = -a_j \in \mathcal{A}$$

(since the negative of a_j also belongs to $\mathcal{A}$) so that (2.2) in Theorem 1 does not hold.

4. Making Primitive Set From a "Small" Subset of $\mathbb{F}_p$ by Adding a Single Element

By Theorem D almost all the subsets of $\mathbb{F}_p$ are primitive. But how are the "few" reducible subsets distributed in the space formed by the subsets of $\mathbb{F}_p$? Are there

"balls" of "not very small radius" in this space such that every subset belonging to them is reducible or the opposite of this is true: for any fixed subset $\mathcal{A} \subset \mathbb{F}_p$ there is a primitive subset "very close" to it? First we will show that for "*small*" subsets of $\mathbb{F}_p$ this is so in a very strong sense (while for *any* subset $\mathcal{A}$ the problem will be studied in Section 5).

Theorem 6. *Let p be a prime with*

$$p > 3 \tag{4.1}$$

and let $\mathcal{A} \subset \mathbb{F}_p$,

$$0 < |\mathcal{A}| < \left(\frac{2}{3}p\right)^{1/2} - 1. \tag{4.2}$$

Then there is an $x \in \mathbb{F}_p \setminus \mathcal{A}$ such that the set $\mathcal{A} \cup \{x\}$ is primitive.

Proof of Theorem 6. Fix some $a \in \mathcal{A}$. If there is an

$$x \in \mathbb{F}_p \setminus \mathcal{A} \tag{4.3}$$

such that the assumptions (2.1) and (2.2) in Theorem 1 hold with the set $\mathcal{A}_x = \mathcal{A} \cup \{x\}$ in place of $\mathcal{A}$ and with a and x in place of a_i and a_j, respectively, then by Theorem 1 this set $\mathcal{A}_x$ is primitive, which proves our claim. Thus, if contrary to the statement of the theorem there is no x satisfying (4.3) for which $\mathcal{A}_x$ is primitive, then for all these x values either (2.1) and (2.2) fails with $a = a_i$, $a_j = x$, i.e., there is either an a_k with

$$a + x - a_k \in \mathcal{A}$$

or an a'_k with

$$a - x + a'_k \in \mathcal{A}$$

so that either

$$x \in \mathcal{A} + \mathcal{A} + \{-a\} \tag{4.4}$$

or

$$x \in \mathcal{A} - \mathcal{A} + \{a\} \tag{4.5}$$

must hold. But by (4.1) and (4.2) the total number of x values satisfying (4.4) and (4.5) is at most

$$\begin{aligned} |\mathcal{A} + \mathcal{A}| + |\mathcal{A} - \mathcal{A}| &\le \frac{1}{2}|\mathcal{A}|(|\mathcal{A}| + 1) + |\mathcal{A}|(|\mathcal{A}| - 1) + 1 \\ &= \frac{1}{2}|\mathcal{A}|(3|\mathcal{A}| - 1) + 1 = \frac{1}{2}|\mathcal{A}|(3|\mathcal{A}| + 1) + 1 - |\mathcal{A}| \\ &< \frac{1}{2}|\mathcal{A}|\left(\sqrt{6p} - 2\right) + 1 - |\mathcal{A}| \le \frac{1}{2}|\mathcal{A}|\sqrt{6p} - |\mathcal{A}| \\ &< p - |\mathcal{A}| = |\mathbb{F}_p \setminus \mathcal{A}| \end{aligned}$$

which contradicts the fact that *every* x satisfying (4.3) must also satisfy one of (4.4) and (4.5), and this completes the proof of Theorem 6.

It is a natural question to ask: what can one say from the opposite side? More precisely, let $h(p)$ denote the greatest integer h such that for every $\mathcal{A} \subset \mathbb{F}_p$ with $|\mathcal{A}| \le h$ one can find an $x \in \mathbb{F}_p \setminus \mathcal{A}$ for which the set $\mathcal{A} \cup \{x\}$ is primitive. Then by Theorem 6 for $p > 3$ we have

$$\left[\left(\frac{2}{3}p\right)^{1/2}\right] - 1 \le h(p). \tag{4.6}$$

On the other hand, it follows trivially from our result [11] in (1.4) that

$$h(p) < \left[p - c_4 \frac{p}{\log p}\right].$$

This upper bound can be improved easily to

$$h(p) < \frac{1}{2}p + O(1). \tag{4.7}$$

Proposition 2. *Let $p \ge 5$ and define $\mathcal{A} \subset \mathbb{F}_p$ by*

$$\mathcal{A} = \bigcup_{k=0}^{\left[\frac{p-1}{4}\right]} \{4k, 4k+1\}.$$

Then any set $\mathcal{B} \subset \mathbb{F}_p$ with $\mathcal{A} \subseteq \mathcal{B}$ is reducible.

Proof of Proposition 2. Clearly, if $p \ge 5$, $\mathcal{B} \subset \mathbb{F}_p$ and $\mathcal{A} \subseteq \mathcal{B}$ then $\mathcal{B}$ has a representation

$$\mathcal{B} = \{0, 1\} + \mathcal{C} \quad \text{with } |\mathcal{C}| \ge 2$$

so that, indeed, $\mathcal{B}$ is reducible.

It follows from this proposition that for this set $\mathcal{A}$ we have

$$h(p) < |\mathcal{A}| \le 2\left[\frac{p-1}{4}\right]$$

which proves (4.7).

There is a large gap between the lower bound (4.6) and the upper bound (4.7); it is not clear which one is closer to $h(p)$. Of course, the set $\mathcal{A}$ constructed in Proposition 2 possesses a much stronger property than the one needed for $h(p) < |\mathcal{A}|$ so that probably the upper bound (4.7) obtained in this way is far from the value of $h(p)$, but the lower bound (4.6) also seems to be far from $h(p)$.

5. Making Primitive Set From Any Subset of $\mathbb{F}_p$ by Changing Relatively Few Elements

By Theorem D above (the result of Alon, Granville and Ubis [2]) there are only a "few" reducible subsets in $\mathbb{F}_p$. Moreover, our results and methods point to direction that the reducible sets are not well-distributed in the sense that there are less reducible sets among the small subsets of $\mathbb{F}_p$ than the large ones. This explains that we have been able to show that from any *small* subset of $\mathbb{F}_p$ one can make a primitive set by adding a single element but, on the other hand, we have not been able to prove such a result for larger subsets. Now we will prove that if instead of adding just one element we may change more (but still relatively few) elements of the given subset then we may make a primitive set also from larger subsets.

Theorem 7. *Let $p \geq 3$ be a prime and $\mathcal{A}$ a subset of $\mathbb{F}_p$. Then by removing at most $\left[\frac{3+\sqrt{5}}{2} \cdot \frac{|\mathcal{A}|^2}{p}\right]$ elements of $\mathcal{A}$ and adding at most* two *elements of $\mathbb{F}_p \setminus \mathcal{A}$ one can form a set $\mathcal{B}$ which is primitive.*

Corollary 3. *If $p \geq 3$ is a prime and $\mathcal{A}$ is a subset of $\mathbb{F}_p$ with*

$$|\mathcal{A}| < \frac{\sqrt{5}-1}{2} p^{1/2},$$

then by adding at most two *elements of $\mathbb{F}_p \setminus \mathcal{A}$ one can form a set $\mathcal{B}$ which is primitive.*

(We remark that it follows already from Theorem 6 with a constant factor c slightly smaller than the one in the upper bound here that if $|\mathcal{A}| < cp^{1/2}$ then by adding just one element of $\mathbb{F}_p \setminus \mathcal{A}$ to $\mathcal{A}$ we can get a primitive set $\mathcal{B}$.)

In order to formulate another consequence of Theorem 7 we need one more definition:

Definition 5. If $\mathcal{A}, \mathcal{B}$ are subsets of $\mathbb{F}_p$ 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 $\mathcal{B}$).

It follows trivially from Theorem 7 that

Corollary 4. *If $p \geq 3$ is a prime and $\mathcal{A}$ is a subset of $\mathbb{F}_p$ then there is a primitive set $\mathcal{B} \subset \mathbb{F}_p$ such that*

$$d(\mathcal{A}, \mathcal{B}) \leq \left[\frac{3+\sqrt{5}}{2} \cdot \frac{|\mathcal{A}|^2}{p}\right] + 2.$$

Proof of Theorem 7. We will use the following lemma.

Lemma 1. *Let $p \geq 3$ be a prime, $\mathcal{A} \subset \mathbb{F}_p$. Suppose that there are $u, v \in \mathbb{F}_p$ for which*

$$u \notin \mathcal{A}+\mathcal{A},\ v \notin \mathcal{A}-\mathcal{A},\ \frac{3v+u}{2} \notin \mathcal{A}. \tag{5.1}$$

Then adding at most two *elements of $\mathbb{F}_p \setminus \mathcal{A}$ to $\mathcal{A}$ one can form a set $\mathcal{B}$ which is primitive.*

Proof of Lemma 1. Let $\mathcal{A} = \{a_1, a_2, \ldots, a_s\}$. For some fixed u, v satisfying (5.1) define a_{s+1} and a_{s+2} by

$$a_{s+1} = \frac{u+v}{2},\ a_{s+2} = \frac{u-v}{2}.$$

Then by (5.1)

$$\begin{aligned} a_{s+1}+a_{s+2} &= u \notin \mathcal{A}+\mathcal{A}, \\ a_{s+1}-a_{s+2} &= v \notin \mathcal{A}-\mathcal{A}, \\ a_{s+1}-a_{s+2}+a_{s+1} &= \frac{u+3v}{2} \notin \mathcal{A}. \end{aligned}$$

In other words

$$\begin{aligned} &a_{s+1}+a_{s+2}-a_k \notin \mathcal{A} \quad \text{for } 1 \leq k \leq s, \\ &a_{s+1}-a_{s+2}+a_k \notin \mathcal{A} \quad \text{for } 1 \leq k \leq s+1. \end{aligned}$$

Using Theorem 1 with $i = s+1$, $j = s+2$ we get that $\mathcal{A} \cup \{a_{s+1}, a_{s+2}\}$ is primitive, and this completes the proof of the lemma.

Now we return to the proof of the theorem. Clearly Theorem 7 is trivial for $|\mathcal{A}| \geq \frac{3-\sqrt{5}}{2}p$ (in this case $\left[\frac{3+\sqrt{5}}{2} \cdot \frac{|\mathcal{A}|^2}{p}\right] \geq |\mathcal{A}|$, and then removing $|\mathcal{A}|-1$ elements from $\mathcal{A}$ we get a set which contains only one element, and thus it is reducible), thus we may assume

$$|\mathcal{A}| < \frac{3-\sqrt{5}}{2}p. \tag{5.2}$$

First we prove that there exist a set $\mathcal{A}' \subset \mathcal{A}$ and an element $u \in \mathbb{F}_p$ such that

$$u \notin \mathcal{A}'+\mathcal{A}' \quad \text{and } |\mathcal{A}'| \geq |\mathcal{A}| - \frac{|\mathcal{A}|^2}{p}. \tag{5.3}$$

Indeed, for $d \in \mathbb{F}_p$ let

$$h(\mathcal{A}, d) \stackrel{\text{def}}{=} |\{(a, a') :\ a+a' = d,\ a, a' \in \mathcal{A}\}|.$$

Clearly,

$$\sum_{d \in \mathbb{F}_p} h(\mathcal{A}, d) = \sum_{d \in \mathbb{F}_p} \sum_{\substack{a, a' \in \mathcal{A} \\ a+a'=d}} 1 = \sum_{a, a' \in \mathcal{A}} 1 = |\mathcal{A}|^2.$$

On the other hand, we have

$$p \min_{d\in\mathbb{F}_p} h(\mathcal{A},d) \le \sum_{d\in\mathbb{F}_p} h(\mathcal{A},d) = |\mathcal{A}|^2$$

whence

$$\min_{d\in\mathbb{F}_p} h(\mathcal{A},d) \le \frac{|\mathcal{A}|^2}{p}. \tag{5.4}$$

Let $u \in \mathbb{F}_p$ be an element with

$$h(\mathcal{A},u) = \min_{d\in\mathbb{F}_p} h(\mathcal{A},d) \stackrel{\text{def}}{=} t, \tag{5.5}$$

and $(a_1,a_1'),\ (a_2,a_2'),\dots,(a_t,a_t')$ the solutions of the equation

$$a+a'=u \quad \text{with } a,a'\in\mathcal{A}.$$

By (5.4) and (5.5) we have

$$t = h(\mathcal{A},u) \le \frac{|\mathcal{A}|^2}{p}.$$

For $\mathcal{A}' = \mathcal{A}\setminus\{a_1,a_2,\dots,a_t\}$ the equation

$$a+a'=u, \quad a,a'\in\mathcal{A}'\ (\subset\mathcal{A})$$

cannot be solved; thus

$$u \notin \mathcal{A}'+\mathcal{A}'.$$

This proves (5.3).

Consider a set $\mathcal{A}'$ and an element $u\in\mathbb{F}_p$ for which (5.3) holds. We will prove that there exists a set $\mathcal{A}''\subset\mathcal{A}'$ and an element $v\in\mathbb{F}_p$ with

$$\begin{aligned} v &\notin \mathcal{A}''-\mathcal{A}'', \\ \frac{u+3v}{2} &\notin \mathcal{A}'' \end{aligned} \tag{5.6}$$

and

$$\begin{aligned} |\mathcal{A}''| &\ge |\mathcal{A}'| - \frac{1+\sqrt{5}}{2}\cdot\frac{|\mathcal{A}|^2}{p} \\ &\ge |\mathcal{A}| - \frac{3+\sqrt{5}}{2}\cdot\frac{|\mathcal{A}|^2}{p}. \end{aligned} \tag{5.7}$$

Since $\mathcal{A}''\subset\mathcal{A}'$ by (5.3)

$$u \notin \mathcal{A}''+\mathcal{A}'' \tag{5.8}$$

trivially holds.

Again, for $d \in \mathbb{F}_p$ we define

$$f(\mathcal{A}', d) \stackrel{\text{def}}{=} |\{(a, a') : \ a - a' = d, \ a, a' \in \mathcal{A}'\}| \, .$$

Let $\mathcal{G} = \{v \in \mathbb{F}_p : \ \frac{u+3v}{2} \in \mathcal{A}'\}$. Since u is fixed (see (5.3)), we have

$$|\mathcal{G}| \leq |\mathcal{A}'| \leq |\mathcal{A}| \, . \tag{5.9}$$

Clearly,

$$\sum_{d \in \mathbb{F}_p \setminus \mathcal{G}} f(\mathcal{A}', d) = \sum_{d \in \mathbb{F}_p \setminus \mathcal{G}} \sum_{\substack{a, a' \in \mathcal{A} \\ a - a' = d}} 1 \leq \sum_{d \in \mathbb{F}_p} \sum_{\substack{a, a' \in \mathcal{A} \\ a - a' = d}} 1 = \sum_{a, a' \in \mathcal{A}} 1 = |\mathcal{A}'|^2 \leq |\mathcal{A}|^2 \, . \tag{5.10}$$

On the other hand, by (5.9) and (5.10) we have

$$(p - |\mathcal{A}|) \min_{d \in \mathbb{F}_p \setminus \mathcal{G}} f(\mathcal{A}', d) \leq (p - |\mathcal{G}|) \min_{d \in \mathbb{F}_p \setminus \mathcal{G}} f(\mathcal{A}', d) \leq \sum_{d \in \mathbb{F}_p \setminus \mathcal{G}} f(\mathcal{A}', d) \leq |\mathcal{A}|^2 \, . \tag{5.11}$$

It follows from this and (5.2) that

$$\min_{d \in \mathbb{F}_p \setminus \mathcal{G}} f(\mathcal{A}', d) \leq \frac{|\mathcal{A}|^2}{p - |\mathcal{A}|} \leq \frac{|\mathcal{A}|^2}{p - \frac{3-\sqrt{5}}{2} p} \leq \frac{1 + \sqrt{5}}{2} \cdot \frac{|\mathcal{A}|^2}{p}. \tag{5.12}$$

Let $v \in \mathbb{F}_p \setminus \mathcal{G}$ be an element with

$$f(\mathcal{A}', v) = \min_{d \in \mathbb{F}_p \setminus \mathcal{G}} f(\mathcal{A}', d) \stackrel{\text{def}}{=} s, \tag{5.13}$$

and $(b_1, b_1'), \ (b_2, b_2'), \ldots, (b_s, b_s')$ the solutions of the equation

$$b - b' = v \quad \text{with } b, b' \in \mathcal{A}'.$$

By (5.12) and (5.13) we have

$$s = f(\mathcal{A}', v) \leq \frac{1 + \sqrt{5}}{2} \cdot \frac{|\mathcal{A}|^2}{p}. \tag{5.14}$$

For

$$\mathcal{A}'' = \mathcal{A}' \setminus \{b_1, b_2, \ldots, b_s\}, \tag{5.15}$$

the equation

$$b - b' = v, \quad b, b' \in \mathcal{A}'' \ (\subset \mathcal{A})$$

cannot be solved, thus

$$v \notin \mathcal{A}'' - \mathcal{A}''. \tag{5.16}$$

By $v \in \mathbb{F}_p \setminus \mathcal{G}$ and the definition of $\mathcal{G}$ we have $\frac{u+3v}{2} \notin \mathcal{A}'$. Since $\mathcal{A}'' \subseteq \mathcal{A}'$ we have

$$\frac{u+3v}{2} \notin \mathcal{A}''. \tag{5.17}$$

(5.6) and (5.7) follow from (5.14), (5.15), (5.16) and (5.17). Thus we have constructed a set $\mathcal{A}'' \subset \mathcal{A}$ and $u, v \in \mathbb{F}_p$ for which

$$u \notin \mathcal{A}'' + \mathcal{A}'',\ v \notin \mathcal{A}'' - \mathcal{A}'',\ \frac{u+3v}{2} \notin \mathcal{A}'',\ |\mathcal{A}''| \geq |\mathcal{A}| - \frac{3+\sqrt{5}}{2} \cdot \frac{|\mathcal{A}|^2}{p}.$$

Using Lemma 1 wee see that it is possible to add at most two elements of $\mathbb{F}_p \setminus \mathcal{A}''$ to $\mathcal{A}''$ so that we get a primitive set $\mathcal{B}$. This completes the proof of Theorem 7.

6. Generalizations

In order to keep our presentation more transparent and the discussions simpler, we have decided to stick to $\mathbb{F}_p$ in this paper. However, we remark that all but one of our results can be generalized easily: Theorems 1, 3, 6, 7 and Corollaries 2, 3, 4 can be extended to any Abelian groups, Theorems 2, 4, 5 and Propositions 1, 2 to cyclic groups (and Corollary 1 is the only result whose proof goes through only in $\mathbb{F}_p$).

Acknowledgement. We would like to thank tha anonymous referee for suggesting us an idea to sharpen Theorem 6 and also to shorten its proof.

References

[1] N. Alon, *Large sets in finite sets are sumsets*, J. Number Theory 126 (2007), 110-118.

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

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

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

[5] C. Elsholtz, *A remark on Hofmann and Wolke's additive decompositions of the set of primes*, Arch. Math. (Basel) 76 (2001), 30-33.

[6] C. Elsholtz, *The inverse Goldbach problem*, Mathematika 48 (2001), 151-158.

[7] C. Elsholtz, *Additive decomposability of multiplicatively defined sets*, Funct. Approx. Comment. Math. 35 (2006), 61-77.

[8] C. Elsholtz, *Multiplicative decomposability of shifted sets*, Bull. Lond. Math. Soc. 40 (2008), 97-107.

[9] 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.

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

[11] K. Gyarmati, S. Konyagin and A. Sárközy, *On the reducibility of large sets of residues modulo p*, J. Number Theory 133 (2013), 2374-2397.

[12] B. Green, *Counting sets with small sumset, and the clique number of random Cayley graphs*, Combinatorica 25 (2005), 307-326.

[13] B. Green, *Essey submitted for the Smith's Prize*, Cambridge University, 2001.

[14] A. Hofmann and D. Wolke, *On additive decompositions of the set of primes*, Arch. Math. (Basel) 67 (1996), 379-382.

[15] B. Hornfeck, *Ein Satz über die Primzahlmenge*, Math. Z. 60 (1954), 271–273 and **62** (1955), 502.

[16] H.-H. Ostmann, *Additive Zahlentheorie*, 2 Vols., Springer, Berlin, 1956.

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

[18] J.-P. Puchta, *On additive decompositions of the set of primes*, Arch. Math. (Basel) 78 (2002), 24-25.

[19] A. Sárközy, *Some metric problems in the additive number theory, I*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 19 (1976), 107-127.

[20] A. Sárközy, *Some metric problems in the additive number theory, II*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 20 (1977), 111-129.

[21] A. Sárközy, *On multiplicative decompositions of the set of shifted quadratic residues modulo p*, in: Number Theory, Analysis and Combinatorics, W. De Gruyter, to appear.

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

[23] I. E. Shparlinski, *Additive decompositions of subgroups of finite fields*, arXiv: 1301.2872v1 [math.NT].

[24] A. Sárközy, *Über totalprimitive Folgen*, Acta Arith. 8 (1962), 21-31.

[25] A. Sárközy, *Über reduzible Folgen*, Acta Arith. 10 (1965), 399-408.

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

[27] A. Sárközy and E. Szemerédi, *On the sequence of squares*, Mat. Lapok 16 (1965), 76-85 (in Hungarian).

[28] B. Volkmann, *Über die Klasse der Summenmergen*, Arch. Math. 6 (1955), 200-207.

[29] B. Volkmann, *Über Klassen von Mengen natürlicker Zahlen*, J. Reine Angew. Math. 190 (1952), 199-230.

[30] E. Wirsing, *Ein metrischer Satz über Mengen ganzer Zahlen*, Arch Math. 4 (1953), 392-398.