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

by

Katalin Gyarmati
Eötvös Loránd University
Department of Algebra and Number Theory
and MTA-ELTE Geometric and Algebraic Combinatorics Research Group
H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary
E-mail: gykati@cs.elte.hu

and

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

2010 Mathematics Subject Classification: Primary 11B13.

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

Hungarian National Foundation for Scientific Research, grants no. K100291 and NK104183, the János Bolyai Research Fellowship and the MTA-ELTE Geometric and Algebraic Combinatorics Research Group.

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 *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 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 $\mathcal{A} = \mathcal{B}_1 + \mathcal{B}_2 + \cdots + \mathcal{B}_k$ with $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_k \subset \mathbb{F}_p$, $|\mathcal{B}_1|, |\mathcal{B}_2|, \ldots, |\mathcal{B}_k| \geq 2$.

1 Introduction

In this paper we will use the following notations and definitions: The set of positive integers is denoted by $\mathbb{N}$, the finite field of p elements is denoted by $\mathbb{F}_p$, and we write $\mathbb{F}_p^* \setminus \{0\}$. 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 $\mathcal{A} = \{a_1, a_2, \ldots\}$ is a subset of $\mathcal{G}$ such that the sums $a_i + a_j$ with $1 \leq i < j$ are distinct, then $\mathcal{A}$ is called a Sidon set. In some proofs we will identify $\mathbb{F}_p$ with the field modulo p residue classes, and a residue class and its representant element will be denoted in the same way.

We will also need

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

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

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 the group operation in $\mathcal{G}$ is called and denoted as *multiplication* and (1.1) and

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

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

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

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

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.*

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 [9]. In almost all of these papers written before 2000 *infinite* sequences of non-negative integers are studied. The intensive study of *finite* problems of this type, in particular, of analogues problems in $\mathbb{F}_p$ has started only in the last decade (again, see [9] for details). In [9] 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 this paper we will use these definitions in this extended sense... In this paper our goal is continue the study of the reducible and primitive subsets of $\mathbb{F}_p$ and the connection between them." We recall a couple of results in [9] 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*

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

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

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*, Monathsh. Math. 169 (2013), 317-328.

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

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

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

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

[8] R. Graham, B. Rothochild and J. H. Spencer, *Ramsey theory*, Wiley, 1980.

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

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

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

[12] H.-H. Otmann, *Untersuchungen über den Summenbegriff in der additiven Zahlentheorie*, Math. Ann. 120 (1948), 165-169.

[13] H.-H. Otmann, *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] I. 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.