POWER SUM POLYNOMIALS AS RELAXED EGZ POLYNOMIALS

Tanbir Ahmed
LaCIM, Université du Québec à Montréal, Montréal, Québec, Canada
tanbir@gmail.com

Arie Bialostocki
arie.bialostocki@gmail.com

Thang Pham
Dept. of Mathematics, University of California, San Diego, La Jolla, California
v9pham@ucsd.edu, phamanhthang.vnu@gmail.com

Le Anh Vinh
University of Education, Vietnam National University, Hanoi, Vietnam
vinhla@vnu.edu.vn

Received: 7/12/18, Accepted: 9/4/19, Published: 9/30/19

Abstract

Let p be a prime and let $\varphi \in \mathbb{Z}_p[x_1, x_2, \ldots, x_p]$ be a symmetric polynomial, where $\mathbb{Z}_p$ is the field of p elements. A sequence T in $\mathbb{Z}_p$ of length p is called a φ-zero sequence if $\varphi(T) = 0$; a sequence in $\mathbb{Z}_p$ is called φ-zero free if it does not contain any φ-zero subsequence. Motivated by the EGZ theorem for the prime p, we define a symmetric polynomial $\varphi \in \mathbb{Z}_p[x_1, x_2, \ldots, x_p]$ to be an EGZ polynomial if it satisfies the following two conditions: (i) every sequence in $\mathbb{Z}_p$ of length $2p-1$ contains a φ-zero subsequence and (ii) the φ-zero free sequences of length $2p-2$ are the sequences which contain exactly any two residues where each residue appears $p-1$ times. For a positive integer k and a prime p, a power-sum polynomial over $\mathbb{Z}_p$ is defined as $s_{k,p} = \sum_{j=1}^{p} x_j^k$. In this paper we answer the question of whether there are EGZ polynomials among the power-sum polynomials. Indeed, $s_{k,p}$ is an EGZ polynomial if and only if $\gcd(k, p-1) = 1$ and these polynomials can be derived from $s_{1,p}$ and a permutation polynomial. Next, we introduce a definition of rational number, $r(s_{k,p}, \mathbb{Z}_p) \in (0, 1]$, which measures the deviation of a power-sum polynomial from being an EGZ polynomial. Among some other results we determine $r(s_{k,p}, \mathbb{Z}_p)$ for every prime p and positive integer k.

1. Introduction

This paper is motivated by the following theorem of Erdős, Ginzburg, and Ziv [9], stated below in Theorem 1 (i) for a prime. Part (ii) of the theorem addresses the inverse problem which corresponds to the first part. It was first proved by Yuster and Peterson [15]. Several new proofs of (i) appear in [1], and a proof of (ii) appears in [5] and [15].

Theorem 1. *Let p be a prime and $\mathbb{Z}_p$ be the additive group of residue classes modulo p.*

(i) *Every sequence in $\mathbb{Z}_p$ of length $2p-1$ contains a zero-sum subsequence of length p.*

(ii) *Each sequence of maximal length in $\mathbb{Z}_p$ that does not contain any zero-sum subsequence of length p contains exactly two distinct elements, where each element appears $p-1$ times.*

Numerous generalizations and developments of the EGZ theorem have appeared over the years. It is worthwhile to mention the surveys [2, 3, 8, 10] and their comprehensive references. We follow a recent new direction (see [6, 7]) which considers the field structure of $\mathbb{Z}_p$ rather than of an Abelian group. Furthermore, we consider symmetric polynomials over $\mathbb{Z}_p$. As one can recall, the sum in the EGZ theorem corresponds to the first elementary symmetric polynomial $\mathbb{Z}_p[x_1, x_2, \ldots, x_p]$.

First we introduce some definitions and notation. Let p be a prime and let $\mathbb{Z}_p$ be the prime field of p elements. Let φ be a symmetric polynomial in $\mathbb{Z}_p[x_1, x_2, \ldots, x_p]$. A sequence $a_1, a_2, \ldots, a_p$ of p elements in $\mathbb{Z}_p$ is called a *φ-zero sequence* if $\varphi(a_1, a_2, \ldots, a_p) = 0$; a sequence in $\mathbb{Z}_p$ is called *φ-zero free* if it does not contain any φ-zero subsequence. Define $g(\varphi, \mathbb{Z}_p)$ to be the smallest integer ℓ such that every sequence in $\mathbb{Z}_p$ of length ℓ contains a φ-zero subsequence; if ℓ does not exist, then we set $g(\varphi, \mathbb{Z}_p) = \infty$. Define $M(\varphi, \mathbb{Z}_p)$ to be the set of all φ-zero free sequences of length $g(\varphi, \mathbb{Z}_p) - 1$, whenever $g(\varphi, \mathbb{Z}_p)$ is finite. We consider two sequences in $\mathbb{Z}_p$ identical if they differ only in the order of their elements, thus we deal with multisets. But the language of sequences is more commonly used in the literature. We will use the notation $[a_1]^{\alpha_1}[a_2]^{\alpha_2} \ldots [a_k]^{\alpha_k}$ to denote a sequence in $\mathbb{Z}_p$ where each element a_i appears α_i times. Finally, we will denote by $E(2, \mathbb{Z}_p)$ the set of all sequences of the form $[u]^{p-1}[v]^{p-1}$, where $u, v \in \mathbb{Z}_p$ and $u \neq v$. Clearly $|E(2, \mathbb{Z}_p)| = \binom{p}{2}$.

The EGZ theorem and the definitions above suggest the introduction of the following properties:

$(\mathcal{E}_1)$ a symmetric polynomial $\varphi \in \mathbb{Z}_p[x_1, x_2, \ldots, x_p]$ satisfies $\mathcal{E}_1$ if $g(\varphi, \mathbb{Z}_p) = 2p-1$;

$(\mathcal{E}_2)$ a symmetric polynomial $\varphi \in \mathbb{Z}_p[x_1, x_2, \ldots, x_p]$ satisfies $\mathcal{E}_2$ if $M(\varphi, \mathbb{Z}_p) = E(2, \mathbb{Z}_p)$; and

$(\mathcal{E}_2')$ a symmetric polynomial $\varphi \in \mathbb{Z}_p[x_1, x_2, \ldots, x_p]$ satisfies $\mathcal{E}_2'$ if $M(\varphi, \mathbb{Z}_p) \cap E(2, \mathbb{Z}_p) \neq \emptyset$.

By the EGZ theorem, the first symmetric polynomial satisfies $\mathcal{E}_1$ and $\mathcal{E}_2$ for every prime p. We define a symmetric polynomial $\mathcal{P} \in \mathbb{Z}_p[x_1, x_2, \ldots, x_p]$ to be an EGZ polynomial with respect to a prime p if it satisfies $\mathcal{E}_1$ and $\mathcal{E}_2$. All EGZ polynomials of degree not exceeding three were classified in [7].

In [7], it was shown how to construct new EGZ polynomials from a given EGZ polynomial. Our paper is motivated by a major open problem of the complete classification of EGZ symmetric polynomials. In this paper, we have restricted ourselves to power sum polynomials which provide EGZ symmetric polynomials, however, these polynomials can be deduced from [7]. For a given prime p, we define a polynomial $\varphi \in \mathbb{Z}_p[x_1, x_2, \ldots, x_p]$ to be a *relaxed* EGZ polynomial if it satisfies $\mathcal{E}_1$ and $\mathcal{E}_2'$. Clearly, an EGZ polynomial is a relaxed EGZ polynomial. For relaxed EGZ polynomials, the major interest is to investigate the sets $M(\varphi, \mathbb{Z}_p)$ and $M(\varphi, \mathbb{Z}_p) \cap E(2, \mathbb{Z}_p)$.

In this paper, we will look at power sum polynomials defined as $s_{k,p} = \sum_{i=1}^{p} x_i^k$, where k is a positive integer and p is a prime, through the lens of relaxed EGZ polynomials. The notation $s_{k,p}$ will be abbreviated as s_k when p is clear. For $k = 1$ and for every prime p, we get an EGZ polynomial by the EGZ theorem. Furthermore, it follows from the forthcoming Theorem 2 that for $k \geqslant 2$, the power sum polynomials are relaxed EGZ polynomials.

Theorem 2. *The power sum polynomials $s_{k,p} = \sum_{i=1}^{p} x_i^k$, where k is a positive integer and p is a prime, are relaxed EGZ polynomials.*

Proof. Let $f(x) = x^k$. Then $s_{k,p} = f(x_1) + f(x_2) + \cdots + f(x_p)$. If $a_1, a_2, \ldots, a_{2p-1}$ is a sequence in $\mathbb{Z}_p$ of length $2p - 1$, then by the EGZ theorem, the sequence $f(a_1), f(a_2), \ldots, f(a_{2p-1})$ contains a subsequence of length p. It follows that the former sequence contains a $s_{k,p}$-zero subsequence, which implies that $g(s_{k,p}, \mathbb{Z}_p) \leqslant 2p - 1$.

On the other hand, if we consider the sequence $s = [0]^{p-1}[1]^{p-1}$ of length $2p-2$, then it is easy to see that s does not contain any zero-sum subsequence of length p. This completes the proof of the theorem. $\square$

2. On the Structure of $M(s_{k,p}, \mathbb{Z}_p)$ for $k \geqslant 2$

In this section, first we analyze thoroughly the set $M(s_{2,p}, \mathbb{Z}_p)$ and observe that for a given integer k and a prime p, the number of distinct residues in $M(s_{k,p}, \mathbb{Z}_p)$ is pretty small. We prove a theorem about it. Next, we determine the cardinality of $M(s_{k,p}, \mathbb{Z}_p)$ for every integer k and every prime p. We start with a definition which refines the set $M(s_{k,p}, \mathbb{Z}_p)$.

Definition 1. For $t \in \mathbb{N}$, let $M_t(s_{k,p}, \mathbb{Z}_p)$ denote the subset of $M(s_{k,p}, \mathbb{Z}_p)$ that consists of all the multisets in $M(s_{k,p}, \mathbb{Z}_p)$ whose underlying set has cardinality t.

Theorem 3. *Let $p \geq 3$ and let $M_t(s_{2,p}, \mathbb{Z}_p)$ be as defined above. Then*

$$|M_t(s_{2,p}, \mathbb{Z}_p)| = \begin{cases} \frac{(p-1)^2}{2}, & \text{if } t = 2; \\ \frac{(p-1)(p-2)^2}{2}, & \text{if } t = 3; \\ \frac{(p-1)(p-2)^2(p-3)}{8}, & \text{if } t = 4; \\ 0, & \text{if } t \geq 5. \end{cases}$$

$$|M(s_{2,p}, \mathbb{Z}_p)| = \sum_{t=1}^{4} |M_t(s_{2,p}, \mathbb{Z}_p)| = \frac{1}{2}(p-1)\left(p - 1 + \frac{1}{4}(p+1)(p-2)^2\right).$$

Proof. Let $a_1, a_2, \ldots, a_{2p-2}$ be a sequence of length $2p-2$. It is clear that the sequence is $s_{k,p}$-zero free if and only if the sequence $f(a_1), f(a_2), \ldots, f(a_{2p-2})$ does not contain any zero-sum subsequence of length p. It follows from Theorem 2 that the latter sequence is of the form $[x]^{p-1}[y]^{p-1}$, where $x, y \in \mathbb{Z}_p$, $x \neq y$. Since for $a \neq 0$, the equation $x^2 = a^2$ has only two solutions a and $-a$, all elements in $M(s_{2,p}, \mathbb{Z}_p)$ are of the following form:

$$[u]^{\alpha}[-u]^{p-1-\alpha}[v]^{\beta}[-v]^{p-1-\beta}, \; 0 \leq \alpha, \beta \leq p-1. \tag{1}$$

Now we consider the following cases:

(i) If $t = 2$, then each element in $M_2(s_{2,p}, \mathbb{Z}_p)$ is of the form $[u]^{p-1}[v]^{p-1}$. Thus the number of elements in $M_2(s_{2,p}, \mathbb{Z}_p)$ equals the number of pairs $(u, v) \in \mathbb{Z}_p^2$ satisfying $u \neq v, u \neq -v$. This implies that $|M_2(s_{2,p}, \mathbb{Z}_p)| = (p-1)^2/2$.

(ii) If $t = 3$, then each element in $M_3(s_{2,p}, \mathbb{Z}_p)$ is of the form $[u]^{\alpha}[-u]^{p-1-\alpha}[v]^{p-1}$ with $u \neq v$, $u \neq -v$, and $1 \leq \alpha \leq p-2$. Since the number of ordered pairs $(u, v) \in \mathbb{Z}_p^2$ satisfying $u \neq 0, u \neq v, u \neq -v$ equals $(p-1)(p-2)/2$, the number of elements in $M_3(s_{2,p}, \mathbb{Z}_p)$ is $(p-1)(p-2)^2/2$.

(iii) If $t = 4$, then each element in $M_4(s_{2,p}, \mathbb{Z}_p)$ is of the form $[u]^{\alpha}[-u]^{\alpha}[v]^{\beta}[-v]^{p-1-\beta}$ with $u \neq v$, $u \neq -v$, and $1 \leq \alpha, \beta \leq p-2$. Since the number of un-ordered pairs $(u, v) \in \mathbb{Z}_p^2$ satisfying $u, v \neq 0$, $u \neq v$, $u \neq -v$ equals $\binom{(p-1)/2}{2} = (p-1)(p-3)/8$, the number of elements in $M_4(s_{2,p}, \mathbb{Z}_p)$ is $(p-1)(p-2)^2(p-3)/8$.

(iv) If $t \geq 5$, then it follows from (1) that $|M_t(s_{2,p}, \mathbb{Z}_p)| = 0$. Putting these cases together, we obtain

$$|M(s_{2,p}, \mathbb{Z}_p)| = \sum_{t=1}^{4} |M_t(s_{2,p}, \mathbb{Z}_p)| = \frac{1}{2}(p-1)\left(p - 1 + \frac{1}{4}(p+1)(p-2)^2\right),$$

which concludes the proof of the theorem.

□

We proceed with some definitions and examples.

Definition 2. (i) Let $X_{k,p}$ denote the image of the function $x^k \mod p$ with $x \in \mathbb{Z}_p \setminus \{0\}$.

(ii) Let $Y_{k,p}$ denote the family defined as

$$Y_{k,p} = \left\{\left\{x : x^k \equiv a \pmod{p}\right\} : a \in X_{k,p}\right\}$$

Example 1. If $p = 13$, then $X_{3,13} = \{1, 5, 8, 12\}$ with $|X_{3,13}| = 4$ such that

$$Y_{3,13} = \{\{1, 3, 9\}, \{7, 8, 11\}, \{2, 5, 6\}, \{4, 10, 12\}\}.$$

Example 2. If $p = 19$, then $X_{12,13} = \{1, 7, 11\}$ with $|X_{12,19}| = 3$ such that

$$Y_{12,19} = \{\{1, 7, 8, 11, 12, 18\}, \{2, 3, 5, 14, 16, 17\}, \{4, 6, 9, 10, 13, 15\}\}.$$

Note that $|X_{k,p}| = |Y_{k,p}|$. For the sake of simplicity, whenever k and p are fixed, we will use the notation $x = |X_{k,p}| = |Y_{k,p}|$ and we will use y to denote the number of elements in each set in $Y_{k,p}$. It is not difficult to prove that $xy = p - 1$. In order to compute $|M(s_{k,p}, \mathbb{Z}_p)|$, first we need to compute x; and to do this, we will introduce the following definition.

Definition 3. Let p and q be distinct primes and let β be a positive integer.

$$Exp(p, q, \lambda) = \begin{cases} 0, \text{if } p \not\equiv 1 \pmod{q^\beta} \text{ for all } \beta \in \{1, 2, \dots, \lambda\}; \\ \text{maximum } \beta \in \{1, 2, \dots, \lambda\} \text{ such that } p \equiv 1 \pmod{q^\beta}, \text{ otherwise.} \end{cases}$$

Example 3. Let $p = 5, q = 3$ and $\lambda = 3$. Then $5 \equiv 2 \mod 3$, $5 \equiv 4 \mod 3^2$ and $5 \equiv 2 \mod 3^3$, and hence $Exp(11, 5, 3) = 0$. Let $p = 11$, $q = 5$ and $\lambda = 3$. Then $11 \equiv 1 \mod 5$, $11 = 11 \mod 5^2$ and $11 \equiv 11 \mod 5^3$, and hence $Exp(51, 5, 3) = 1$.

Lemma 1. *For positive integer k with prime decomposition $k = \prod_{i=1}^t p_i^{\alpha_i}$ and a prime p,*

$$x = \frac{p-1}{\prod_{i=1}^t p_i^{Exp(p, p_i, \alpha_i)}}.$$

Proof. Given $a \in [1, p-1]$, consider the congruence $x^k \equiv a \pmod{p}$. It has been shown [12, p.45] that if $a^{(p-1)/gcd(k,p-1)} \equiv 1 \pmod{p}$, then there is a solution to $x^k \equiv a \pmod{p}$, and the number of solutions to $a^{(p-1)/gcd(k,p-1)} \equiv 1 \pmod{p}$ is $(p-1)/gcd(k, p-1)$. Thus it suffices to prove that

$$\gcd(k, p-1) = \prod_{i=1}^{t} p_i^{Exp(p, p_i, \alpha_i)}. \tag{2}$$

We now prove (2) by induction on the number of primes in the prime factorization of k. For the base case $t = 1$, we consider the following two cases:

1. If $p \pmod{k} \equiv 1 \pmod{p_1^{\beta}}$ with maximum $\beta \in [1, \alpha-1]$, then we have

$$\gcd(p_1^{\alpha_1}, p-1) = p_1^{\beta}.$$

2. If $p \pmod{k} \not\equiv 1 \pmod{p_1^{\beta}}$ for all $\beta \in [1, \alpha-1]$, then we have

$$\gcd(p_1^{\alpha}, p-1) = 1.$$

Thus, the base case follows directly from the definition of $Exp(p, p_1, \alpha)$. Suppose that the statement is true for $k = \prod_{i=1}^{t-1} p_i^{\alpha_i}$. We now show that it also holds for $k = \prod_{i=1}^{t} p_i^{\alpha_i}$. Indeed, let $k_1 = k/p_t^{\alpha_t}$. By the induction hypothesis,

$$\gcd(k_1, p-1) = \prod_{i=1}^{t-1} p_i^{Exp(p,p_i,\alpha_i)}.$$

Clearly, by the definition of $Exp(p, q, \lambda)$, we have

$$\gcd(k, p-1) = p_t^{Exp(p,p_t,\alpha_t)} \gcd(k_1, p-1) = \prod_{i=1}^{t} p_i^{Exp(p,p_i,\alpha_i)},$$

which concludes the proof of the lemma. □

Now we are ready to compute the cardinality of $M(s_{k,p}, \mathbb{Z}_p)$.

Theorem 4. *For positive integer k and prime $p \geqslant 3$,*

$$|M(s_{k,p}, \mathbb{Z}_p)| = \binom{x}{2}\binom{p+y-2}{y-1}^2 + (p-1).$$

Proof. The $s_{k,p}$-zero free sequences are of the form

$$[u_1]^{\alpha_1}[u_2]^{\alpha_2}\cdots[u_y]^{\alpha_y}[v_1]^{\beta_1}[v_2]^{\beta_2}\cdots[v_y]^{\beta_y} \tag{3}$$

such that $(u_1, u_2, \ldots, u_y), (v_1, v_2, \ldots, v_y) \in Y_{k,p}$, $u_1^k = u_2^k = \cdots = u_y^k \pmod{p}$, $v_1^k = v_2^k = \cdots = v_y^k \pmod{p}$, where $u_i \neq v_j$ for $1 \leqslant i, j \leqslant y$ and $\alpha_1 + \alpha_2 + \cdots + \alpha_y = \beta_1 + \beta_2 + \cdots + \beta_y = p-1$.

There are $\binom{x}{2}$ ways to choose two sets from $Y_{k,p}$ and there are $\binom{p+y-2}{y-1}$ ordered y-tuples in $\mathbb{Z}_p^y$ with sum of elements equal to $p-1$. Therefore, adding the $(2p-2)$-sequences of the form $[0]^{p-1}[u]^{p-1}$ with $u \neq 0$, we get

$$|M(s_{k,p}, \mathbb{Z}_p)| \quad = \quad \binom{x}{2}\binom{p+y-2}{y-1}^2 + (p-1),$$

which is the desired size of $M(s_{k,p}, \mathbb{Z}_p)$ as stated above. □

We will demonstrate Theorem 4 for $k = 3$.

Corollary 1. *For $p \geq 3$,*

$$|M(s_{3,p}, \mathbb{Z}_p)| = \begin{cases} \binom{p}{2}, & \text{if } p \not\equiv 1 \pmod{3}; \\ \binom{(p-1)/3}{2}\binom{p+1}{2}^2 + (p-1), & \text{if } p \equiv 1 \pmod{3}. \end{cases}$$

Proof. From Definition 3 and Lemma 1, we have

$$x = \begin{cases} p-1, & \text{if } p \not\equiv 1 \pmod{3}; \\ \frac{p-1}{3}, & \text{if } p \equiv 1 \pmod{3}. \end{cases}$$

Thus, the corollary follows directly from Theorem 4. □

Motivated by Theorem 3, we introduce the following definition.

Definition 4. For an integer k and a prime p, let $f(k,p)$ denote the minimal number such that for any $t \geq f(k,p)$ we have $M_t(s_{k,p}, \mathbb{Z}_p) = \emptyset$.

Theorem 5. *For a positive integer k and a prime p,*

$$f(p,k) = 2y + 1.$$

Proof. From the proof of Theorem 4, it follows that the $s_{k,p}$-zero free sequences are of the form

$$[u_1]^{\alpha_1}[u_2]^{\alpha_2}\cdots[u_y]^{\alpha_y}[v_1]^{\beta_1}[v_2]^{\beta_2}\cdots[v_y]^{\beta_y}$$

such that $(u_1, u_2, \ldots, u_y), (v_1, v_2, \ldots, v_y) \in Y_{k,p}$, $u_1^k = u_2^k = \cdots = u_y^k \pmod{p}$, $v_1^k = v_2^k = \cdots = v_y^k \pmod{p}$, where $u_i \neq v_j$ for $1 \leqslant i, j \leqslant r$ and $\alpha_1 + \alpha_2 + \cdots + \alpha_y = \beta_1 + \beta_2 + \cdots + \beta_y = p - 1$.

This implies that there is no $s_{k,p}$-zero free sequence of more than $2y$ elements, thus $f(k,p) \leq 2y+1$. On the other hand, since $y \leq p-1$, it follows that $f(k,p) > 2y$. This concludes the proof of the theorem. □

3. On the Cardinality of $E(2, \mathbb{Z}_p) \cap M(s_k, \mathbb{Z}_p)$

For a given prime p and a positive integer k, our interest is to measure how much is $s_{k,p}$ relaxed. In the following section, we will provide an answer to this question.

Theorem 6. *Let the decomposition of k into power of primes be $k = \prod_{i=1}^{t} p_i^{\alpha_i}$, where p_i are distinct primes and α_i are positive integers for $i = 1, 2, \ldots, t$. Then*

$$|E(2, \mathbb{Z}_p) \cap M(s_k, \mathbb{Z}_p)| = \binom{p}{2} \cdot \left(1 - \frac{\prod_{i=1}^{t} p_i^{Exp(p,p_i,\alpha_i)} - 1}{p}\right).$$

Proof. Let $m(p,k)$ denote the number of sequences $[u]^{p-1}[v]^{p-1} \in E(2,\mathbb{Z}_p)$ such that $u^k \mod p = v^k \mod p$ for some $u, v \in [1, p-1]$ where $u \neq v$. Such a sequence contains an s_k-zero subsequence of length p. Thus, in order to prove Theorem 6, it is sufficient to prove that

$$m(p,k) = \binom{p}{2} \cdot \frac{\prod_{i=1}^{t} p_i^{Exp(p,p_i,\alpha_i)} - 1}{p}. \tag{4}$$

Indeed, given $a \in [1, p-1]$, let $N(p,k,a)$ be defined as the number of solutions y satisfying the congruence $y^k \equiv a \pmod{p}$. Consider the congruence $x^k \equiv a \pmod{p}$. If $a^{(p-1)/gcd(k,p-1)} \equiv 1 \pmod{p}$, then $N(p,k,a) = gcd(k, p-1)$, or else $N(p,k,a) = 0$. Therefore,

$$m(p,k) = \sum_{a=1}^{p-1} \binom{N(p,k,a)}{2} = (gcd(k,p-1) - 1) \cdot \frac{p-1}{2}.$$

This implies that the equation (4) is equivalent to

$$\gcd(k, p-1) = \prod_{i=1}^{t} p_i^{Exp(p,p_i,\alpha_i)}, \tag{5}$$

which has been proved in Lemma 1. Therefore the theorem follows. □

Next, as promised, we will introduce a measurement to indicate how much is $s_{k,p}$ relaxed. It is a number $r \in (0,1]$. The closer $r = r(s_k, \mathbb{Z}_p)$ is to 1, the closer $s_{k,p}$ is to being an EGZ polynomial. Furthermore, $r = 1$ if and only if $s_{k,p}$ is an EGZ polynomial.

Definition 5. Given a positive integer k and a prime p, we define

$$r(s_k, \mathbb{Z}_p) = \frac{|E(2,\mathbb{Z}_p) \cap M(s_k,\mathbb{Z}_p)|}{|E(2,\mathbb{Z}_p)|} = \frac{|E(2,\mathbb{Z}_p) \cap M(s_k,\mathbb{Z}_p)|}{\binom{p}{2}}.$$

With this definition, Theorem 4 can be presented in the following form.

Theorem 7. *Let the decomposition of k into power of primes be $k = \prod_{i=1}^{t} p_i^{\alpha_i}$, where p_i are distinct primes and α_i are positive integers for $i = 1, 2, \ldots, t$. Then*

$$r(s_k, \mathbb{Z}_p) = 1 - \frac{\prod_{i=1}^{t} p_i^{Exp(p,p_i,\alpha_i)} - 1}{p}.$$

Theorem 8. *Let p be a prime and let k be a positive integer. Then the power sum polynomial $s_{k,p}$ is an EGZ polynomial if and only if* $\gcd(k, p-1) = 1$.

Proof. The power sum polynomial $s_{k,p}$ is an EGZ polynomial if and only if $r(s_k, \mathbb{Z}_p) = 1$. And, by Theorem 7 and (5), $r(s_k, \mathbb{Z}_p) = 1$ if and only if $\gcd(k, p-1) = 1$. □

Remark 1. Since by [13, p. 351] the monomial x^k is a permutation of polynomial of $\mathbb{Z}_p$ if and only if $\gcd(k, p-1) = 1$, it follows from [7] that the EGZ power sum polynomials in Theorem 8 are already known EGZ polynomials.

Corollary 2. *If k is prime and p is also a prime, then*

$$r(s_k, \mathbb{Z}_p) = \begin{cases} 1 - (k-1)/p, & \text{if } p \equiv 1 \pmod{k}; \\ 1, & \text{if } p \not\equiv 1 \pmod{k}. \end{cases}$$

Corollary 3. *If k is a positive integer such that $k = 2q$ where $q \not\equiv 1, 2 \pmod{k}$ and q is a prime, then*

$$r(s_k, \mathbb{Z}_p) = 1 - (1/p).$$

Hence

$$\liminf r(s_{k,p}, \mathbb{Z}_p) = 0, \quad \limsup(s_{k,p}, \mathbb{Z}_p) = 1$$

where k is a positive integer and p is a prime.

Corollary 4. *The only k for which the power sum polynomials $s_{k,p}$ is an EGZ polynomial for every prime p is $k = 1$.*

We conclude with a problem.

Problem 1. Is the set $\{s_{k,p} : k$ a positive integer and p a prime$\}$ dense in $[0, 1]$?

Acknowledgements. The authors would like to thank the anonymous referee for his suggestion to include references [11] and [14].

References

[1] N. Alon and M. Dubiner, Zero-sum sets of prescribed size, in *Combinatorics, Paul Erdős is Eighty, Vol. 1 Boyai Soc. Math. Stud., János Bolyai Math. Soc., Budapest*, (1993), 33–50.

[2] A. Bialostocki, Zero-sum trees: a survey of results and open problems, in Finite and Infinite Combinatorics in Sets and Logic (Banff, AB, 1991), *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.* **411** (1993), 19–29.

[3] A. Bialostocki, Some problems in view of recent developments of the Erdős-Ginzburg-Ziv theorem, *Integers* **7(2)** (2007), #A7.

[4] A. Bialostocki and P. Dierker, Zero-sum Ramsey theorems, in Proceedings of the Twentieth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1989), *Congr. Numer.* **70** (1990), 119–130.

[5] A. Bialostocki and P. Dierker, On the Erdős-Ginzburg-Ziv Theorem and the Ramsey numbers for stars and matchings, *Discrete Math.* **110(1–3)** (1992), 1–8.

[6] A. Bialostocki and T. D. Luong, An analogue of the Erdős-Ginzburg-Ziv theorem for quadratic symmetric polynomials, *Integers* **9** (2009), 459–465.

[7] A. Bialostocki and T. D. Luong, Cubic symmetric polynomials yielding variations of the Erdős-Ginzburg-Ziv theorem, *Acta Math. Hungar* **142(1)** (2014), 152–166.

[8] Y. Caro, Zero-sum problems - a survey, *Discrete Math.* **152** (1996), 93–113.

[9] P. Erdős, A. Ginzburg, and A. Ziv, Theorem in additive number theory, *Bull. Res. Council Israel* **10F** (1961), 41–43.

[10] W. Gao and A. Geroldinger, Zero-sum problems in finite abelian groups: a survey, *Expo. Math.* **24** (2006), 337–369.

[11] W. Gao, Y. Li, P. Yuan and J. Zhuang, On the structure of long zero-sum free sequences and n-zero-sum free sequences over finite cyclic groups, *Arch. Math. (Basel)* **105** (2015), 361–370.

[12] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Second edition, Graduate Texts in Mathematics, **84**, Springer-Verlag, New York, 1990.

[13] R. Lidl and H. Niederreiter, *Finite Fields*, Second edition, Encyclopedia of Mathematics and its Applications, **20**, Cambridge University Press, Cambridge, 1997.

[14] S. Savchev and F. Chen, Long n-zero-free sequences in finite cyclic groups, *Discrete Math.* **308** (2008), 1–8.

[15] T. Yuster and B. Peterson, On a generalization of an addition theorem for solvable groups, *Canad. J. Math.* **36(3)** (1984), 529–536.