On additive complement of a finite set

Sándor Z. Kiss [*], Eszter Rozgonyi [†], Csaba Sándor [‡]

May 7, 2013

Abstract

We say the sets of nonnegative integers $\mathcal{A}$ and $\mathcal{B}$ are additive complements if their sum contains all sufficiently large integers. In this paper we prove a conjecture of Chen and Fang about additive complement of a finite set.

2000 AMS Mathematics subject classification number: primary: 11B13, secondary: 11P99.

Key words and phrases: additive number theory, additive complement, finite sets.

1 Introduction

Let $\mathbb{N}$ denote the set of positive integers and let $\mathcal{A} \subseteq \mathbb{N}$ and $\mathcal{B} \subseteq \mathbb{N}$ be finite or infinite sets. Let $R_{\mathcal{A}+\mathcal{B}}(n)$ denote the number of solutions of the equation

$$a + b = n, \quad a \in \mathcal{A}, \quad b \in \mathcal{B}.$$

[*]Institute of Mathematics, Budapest University of Technology and Economics, H-1529 B.O. Box, Hungary; Computer and Automation Research Institute of the Hungarian Academy of Sciences, Budapest H-1111, Lágymányosi street 11; kisspest@cs.elte.hu. This author was supported by the OTKA Grant No. K77476 and No. NK105645.

[†]Institute of Mathematics, Budapest University of Technology and Economics, H-1529 B.O. Box, Hungary, reszti@math.bme.hu. The work reported in the paper has been developed in the framework of the project "Talent care and cultivation in the scientific workshops of BME" project. This project is supported by the grant TÁMOP - 4.2.2.B-10/1–2010-0009.

[‡]Institute of Mathematics, Budapest University of Technology and Economics, H-1529 B.O. Box, Hungary, csandor@math.bme.hu. This author was supported by the OTKA Grant No. K81658.

We put

$$A(n) = \sum_{\substack{a\le n\\ a\in\mathcal{A}}} 1 \quad and \quad B(n) = \sum_{\substack{b\le n\\ b\in\mathcal{B}}} 1$$

respectively. We say a set $\mathcal{B} \subseteq \mathbb{N}$ is an additive complement of the set $\mathcal{A} \subseteq \mathbb{N}$ if every sufficiently large $n \in \mathbb{N}$ can be represented in the form $a + b = n$, $a \in \mathcal{A}$, $b \in \mathcal{B}$, i.e., $R_{\mathcal{A}+\mathcal{B}}(n) \ge 1$ for $n \ge n_0$. Additive complement is an important concept in additive number theory, in the past few decades it was studied by many authors [4], [6], [8], [9]. In [8] Sárközy and Szemerédi proved a conjecture of Danzer [4], namely they proved that for infinite additive complements $\mathcal{A}$ and $\mathcal{B}$ if

$$\limsup_{x\to+\infty} \frac{A(x)B(x)}{x} \le 1,$$

then

$$\liminf_{x\to+\infty} (A(x)B(x) - x) = +\infty.$$

In [1] Chen and Fang improved this result and they proved that if

$$\limsup_{x\to+\infty} \frac{A(x)B(x)}{x} > 2, \quad or \quad \limsup_{x\to+\infty} \frac{A(x)B(x)}{x} < \frac{5}{4},$$

then

$$\lim_{x\to+\infty} (A(x)B(x) - x) = +\infty.$$

In the other direction they proved in [2] that for any integer $a \ge 2$, there exist two infinite additive complements $\mathcal{A}$ and $\mathcal{B}$ such that

$$\limsup_{x\to+\infty} \frac{A(x)B(x)}{x} = \frac{2a+2}{a+2},$$

but there exist infinitely many positive integers x such that $A(x)B(x) - x = 1$. In [3] they studied the case when $\mathcal{A}$ is a finite set. In this case the situation is different from the infinite case. Chen and Fang proved that for any two additive complements $\mathcal{A}$ and $\mathcal{B}$ with $|\mathcal{A}| < +\infty$ or $|\mathcal{B}| < +\infty$, if

$$\limsup_{x\to+\infty} \frac{A(x)B(x)}{x} > 1,$$

then

$$\lim_{x\to+\infty} (A(x)B(x) - x) = +\infty.$$

They also proved that if

$$\mathcal{A} = \{a + im^s + k_i m^{s+1} : i = 0, ..., m-1\},$$

where $|\mathcal{A}| = m$, a, $s \geq 0$ and k_i are integers, then there exists an additive complement $\mathcal{B}$ of $\mathcal{A}$ such that $A(x)B(x) - x = O(1)$. In the special case $|\mathcal{A}| = 3$ they proved that if $\mathcal{A}$ is not of the form $\{a + i3^s + k_i 3^{s+1} : i = 0, 1, 2\}$, where a, $s \geq 0$ and k_i are integers, then for any additive complement $\mathcal{B}$ of $\mathcal{A}$,

$$\lim_{x \to +\infty} (A(x)B(x) - x) = +\infty$$

holds. Chen and Fang posed the following conjecture (Conjecture 1.5. in [3]):

Conjecture 1 *If the set of nonnegative integers $\mathcal{A}$ is not of the form*

$$\mathcal{A} = \{a + im^s + k_i m^{s+1} : i = 0, ..., m-1\},$$

where $a, m > 0$, $s \geq 0$ and k_i are integers, then, for any additive complement $\mathcal{B}$ of $\mathcal{A}$, we have

$$\lim_{x \to +\infty} (A(x)B(x) - x) = +\infty.$$

In this paper we prove this conjecture, when the number of elements of the set $\mathcal{A}$ is prime:

Theorem 1 *Let p be a positive prime and $\mathcal{A}$ is a set of nonnegative integers with $|\mathcal{A}| = p$. If $\mathcal{A}$ is not of the form*

$$\mathcal{A} = \{a + ip^s + k_i p^{s+1} : i = 0, ..., p-1\}, \tag{1}$$

where $a > 0$, $s \geq 0$ and k_i are integers, then, for any additive complement $\mathcal{B}$ of $\mathcal{A}$, we have

$$\lim_{x \to +\infty} (A(x)B(x) - x) = +\infty. \tag{2}$$

In the case when the number of elements of $\mathcal{A}$ is a composite number, we disprove Conjecture 1.5. in [3]:

Theorem 2 *For any composite number $n > 0$, there exists a set $\mathcal{A}$ and a set $\mathcal{B}$ such that $|\mathcal{A}| = n$, $\mathcal{B}$ is an additive complement of $\mathcal{A}$ and $\mathcal{A}$ is not of the form*

$$\mathcal{A} = \{a + in^s + k_i n^{s+1} : i = 0, ..., n-1\},$$

where $s \geq 0$, $a > 0$, and k_i are integers, and

$$A(x)B(x) - x = O(1).$$

In the next section we give a short survey about the algebraic concepts which play a crucial role in the proof of Theorem 1.

2 Preliminaries

In our proof we are working with cyclotomic polynomials. Both the definition and the most important properties of these polynomials are well-known. Interested reader can find these in [5, p. 63-66]. We denote the degree of a polynomial f by $\deg f$. Let θ be an algebraic number. We say the monic polynomial f is the minimal polynomial of θ if f is the least degree such that $f(\theta) = 0$. It is well-known that if f is the minimal polynomial of θ, and g is a polynomial such that $g(\theta) = 0$, then $f|g$. A μ complex number is called primitive nth root of unity if μ is the root of the polynomial $x^n - 1$ but not of $x^m - 1$ for any $m < n$. The cyclotomic polynomial of order n is defined by

$$\Phi_n(z) = \prod_{\zeta}(z - \zeta),$$

where ζ runs over all the primitive nth root of unity. This is a monic irreducible polynomial with degree $\varphi(n)$, and $\Phi_n(z)$ has integer coefficients. It is well-known that $\Phi_n(z)$ is the minimal polynomial of ζ and

$$1 + z + z^2 + \ldots + z^{n-1} = \prod_{\substack{l|n \\ l>1}} \Phi_l(z). \tag{3}$$

It is easy to see that

$$\Phi_{p^{s+1}}(z) = 1 + z^{p^s} + z^{2p^s} + \ldots + z^{(p-1)p^s} \tag{4}$$

3 Proof of Theorem 1

We will prove that if there exists an additive complement $\mathcal{B}$ of $\mathcal{A}$, $|\mathcal{A}| = p$ such that

$$\liminf_{x\to+\infty}(A(x)B(x) - x) < +\infty,$$

then $\mathcal{A}$ is the form (1). Let us suppose that $R_{\mathcal{A}+\mathcal{B}}(n) \geq 1$ for $n \geq n_0$. First we prove that there exists an integer n_1 such that $R_{\mathcal{A}+\mathcal{B}}(n) = 1$ for $n \geq n_1$. We argue as Sárközy and Szemerédi in [9, p.238]. As $\mathcal{B}$ is an additive complement of $\mathcal{A}$, it follows that

$$+\infty > C = \liminf_{x\to+\infty}(A(x)B(x) - x) = \liminf_{x\to+\infty}\left(\Big(\sum_{\substack{a\in\mathcal{A} \\ a\leq x}} 1\Big)\Big(\sum_{\substack{b\in\mathcal{B} \\ b\leq x}} 1\Big) - x\right) \geq$$

$$\geq \liminf_{x\to+\infty}\left(\Big(\sum_{\substack{a\in\mathcal{A},b\in\mathcal{B}\\ a+b\leq x}} 1\Big) - x\right) = \liminf_{x\to+\infty}\Big(\sum_{n=0}^{x} R_{\mathcal{A}+\mathcal{B}}(n) - x\Big) \geq$$

$$\geq \liminf_{x\to+\infty}\Big(\sum_{n=n_0+1}^{x} R_{\mathcal{A}+\mathcal{B}}(n) - x\Big) \geq \liminf_{x\to+\infty}\left([x] - n_0 + \sum_{\substack{n_0<n\leq x\\ R_{\mathcal{A}+\mathcal{B}}(n)>1}} 1 - x\right) \geq$$

$$\geq \liminf_{x\to+\infty}\left(\sum_{\substack{n_0<n\leq x\\ R_{\mathcal{A}+\mathcal{B}}(n)>1}} 1\right) - (n_0+1),$$

thus we have

$$\liminf_{x\to+\infty}\left(\sum_{\substack{n_0<n\leq x\\ R_{\mathcal{A}+\mathcal{B}}(n)>1}} 1\right) < C + n_0 + 1,$$

where C is a positive constant. As $\mathcal{B}$ is an additive complement of $\mathcal{A}$, it follows that there exists an integer n_1 such that

$$R_{\mathcal{A}+\mathcal{B}}(n) = 1 \quad for \quad n \geq n_1. \tag{5}$$

In the next step we prove that $\mathcal{A}$ is of the form (1). Let $z = re^{2i\pi\alpha} = re(\alpha)$, where $r < 1$. Let the generating functions of the sets $\mathcal{A}$ and $\mathcal{B}$ be $f_{\mathcal{A}}(z) = \sum_{a\in\mathcal{A}} z^a$ and $f_{\mathcal{B}}(z) = \sum_{b\in\mathcal{B}} z^b$ respectively. (By $r < 1$ these infinite series and all the other infinite series of the proof are absolutely convergent.) In view of (5) we have

$$f_{\mathcal{A}}(z)\cdot f_{\mathcal{B}}(z) = \Big(\sum_{a\in\mathcal{A}} z^a\Big)\Big(\sum_{b\in\mathcal{B}} z^b\Big) = \sum_{n=0}^{+\infty} R_{\mathcal{A}+\mathcal{B}}(n) z^n =$$

$$= \sum_{n=0}^{n_1-1} R_{\mathcal{A}+\mathcal{B}}(n) z^n + \sum_{n=n_1}^{+\infty} R_{\mathcal{A}+\mathcal{B}}(n) z^n = p_1(z) + \frac{z^{n_1}}{1-z},$$

where $p_1(z)$ is a polynomial of z. Thus we have

$$(1-z) f_{\mathcal{A}}(z)\cdot f_{\mathcal{B}}(z) = (1-z)p_1(z) + z^{n_1}. \tag{6}$$

In next step we prove that $f_{\mathcal{B}}(z)$ can be written in the form

$$f_{\mathcal{B}}(z) = F_{\mathcal{B}}(z) + \frac{T(z)}{1-z^M}, \tag{7}$$

where M is a positive integer, $F_{\mathcal{B}}(z)$ and $T(z)$ are polynomials. We argue as Nathanson in [7, p.18-19]. Let $(1-z)f_{\mathcal{A}}(z) = \sum_{n=K}^{N} a_n z^n$, where $a_N \neq 0$ and $a_K \neq 0$, and let $f_{\mathcal{B}}(z) = \sum_{n=0}^{\infty} e_n z^n$, where $e_n \in \{0,1\}$. Then we have

$$(1-z)f_{\mathcal{A}}(z) \cdot f_{\mathcal{B}}(z) = \sum_{n=0}^{\infty} c_n z^n,$$

where $c_n = 0$ from a certain point on. It is clear that if n is large enough, then $c_n = e_{n-K}a_K + e_{n-K-1}a_{K+1} + \ldots + e_{n-N}a_N = 0$. This shows that the coefficients of the power series $f_{\mathcal{B}}(z)$ satisfy a linear recurrence relation from a certain point on. These coefficients are either 0 or 1 from a certain point on. It is easy to see that a sequence defined by a linear recurrence relation on a finite set must be eventually periodic, which proves (7).
It follows from (6) and (7) that

$$f_{\mathcal{A}}(z) \cdot \left(F_{\mathcal{B}}(z) + \frac{T(z)}{1-z^M} \right) = p_1(z) + \frac{z^{n_1}}{1-z},$$

hence for every $z \in \mathbb{C}$

$$(1-z^M)f_{\mathcal{A}}(z)F_{\mathcal{B}}(z) + f_{\mathcal{A}}(z)T(z) = (1-z^M)p_1(z) + (1+z+z^2+\ldots+z^{M-1})z^{n_1}. \tag{8}$$

By putting $z=1$, we obtain that

$$f_{\mathcal{A}}(1)T(1) = M. \tag{9}$$

As $f_{\mathcal{A}}(1) = |\mathcal{A}| = p$, it follows from (9) that $p|M$. Define k by $p^k|M$ but $p^{k+1} \nmid M$. It follows from (8) that

$$(1+z+z^2+\ldots+z^{M-1}) | f_{\mathcal{A}}(z)T(z).$$

It follows from (3) that for any $1 \leq t \leq k$ we have

$$\Phi_{p^t}(z) | f_{\mathcal{A}}(z)T(z).$$

Assume that for any $1 \leq t \leq k$ we have $\Phi_{p^t}(z)|T(z)$. Then

$$T(z) = \left(\prod_{t=1}^{k} \Phi_{p^t}(z) \right) \cdot q(z),$$

where $q(z)$ is a polynomial with integer coefficients. By putting $z=1$ we obtain that $T(1) = p^k q(1)$, hence $M = f_{\mathcal{A}}(1)T(1) = p^{k+1}q(1)$ which contradicts the definition of k. It follows that there exists an integer $0 \leq s \leq k-1$ such that $\Phi_{p^{s+1}}(z)|f_{\mathcal{A}}(z)$, thus $f_{\mathcal{A}}(z) = \Phi_{p^{s+1}}(z) \cdot a(z)$, where $a(z)$ is a polynomial. As $\mathcal{A} = \{a_1, \ldots, a_p\}$, we have $f_{\mathcal{A}}(z) = \sum_{i=1}^{p} z^{a_i}$. Let ω be the following p^{s+1}th root of unity,

$$\omega = exp\left(\frac{2\pi}{p^{s+1}} i\right).$$

It follows that $f_{\mathcal{A}}(\omega) = 0$, thus we have $\sum_{i=1}^{p} \omega^{a_i} = 0$. Let $a_i = l_i p^{s+1} + r_i$, where $0 \le r_i < p^{s+1}$. Without loss of generality we may assume that

$$0 \le r_1 \le r_2 \le \ldots \le r_p < p^{s+1}. \tag{10}$$

Define $r_{p+1} = p^{s+1} + r_1$. Since $\sum_{i=1}^{p}(r_{i+1} - r_i) = r_{p+1} - r_1 = p^{s+1}$ then it follows that there exists a j with $1 \le j \le p$ such that

$$r_{j+1} - r_j \ge p^s. \tag{11}$$

In the next step we prove that this implies

$$a_i - r_{j+1} = n_i p^{s+1} + t_i, \tag{12}$$

where $1 \le i \le p$ and $0 \le t_i \le p^{s+1} - p^s$ holds. Assume that $i \le j$. By the definition of a_i we have $a_i - r_{j+1} = l_i p^{s+1} + r_i - r_{j+1}$. It follows from (10) and (11) that $r_{j+1} - r_i \le r_{j+1} < p^{s+1}$ and $-p^{s+1} < r_i - r_{j+1} \le r_j - r_{j+1} \le -p^s$. Thus we have $0 \le r_i - r_{j+1} + p^{s+1} \le p^{s+1} - p^s$, which implies (12). In the second case assume that $i \ge j + 2$. It is clear from (10) that $r_i - r_{j+1} > 0$. By the definition of a_i and (10), (11) we have

$$a_i - r_{j+1} = l_i p^{s+1} + r_i - r_{j+1} < l_i p^{s+1} + p^{s+1} - r_{j+1} \le l_i p^{s+1} + p^{s+1} - p^s,$$

which implies (12). It follows that there exists an integer a such that $a_i = a + n_i p^{s+1} + t_i$, where n_i is an integer and

$$0 \le t_i \le p^{s+1} - p^s. \tag{13}$$

As $f_{\mathcal{A}}(\omega) = 0$, and the definition of ω we obtain that

$$\sum_{i=1}^{p} \omega^{a_i} = \sum_{i=1}^{p} \omega^{a + n_i p^{s+1} + t_i} = \sum_{i=1}^{p} \omega^{a + t_i} = 0.$$

Let $h(z) = \sum_{i=1}^{p} z^{t_i}$. Thus we obtain that $h(\omega) = 0$. As $\Phi_{p^{s+1}}(z)$ is a minimal polynomial of ω we have $\Phi_{p^{s+1}}(z)|h(z)$. It follows from (13) that $deg\Big(\sum_{i=1}^{p} z^{t_i}\Big) \le p^{s+1} - p^s = \varphi(p^{s+1}) = deg\Big(\Phi_{p^{s+1}}(z)\Big)$. Therefore, by using (4) we have $\sum_{i=1}^{p} z^{t_i} = \Phi_{p^{s+1}}(z) = 1 + z^{p^s} + z^{2p^s} + \ldots + z^{(p-1)p^s}$ and then we have $\{t_1, \ldots, t_p\} = \{0, p^s, 2p^s, \ldots, (p-1)p^s\}$. It follows that there exist integers $a > 0$ and k_i, such that $\mathcal{A} = \{a + ip^s + k_i p^{s+1}\}$, as desired.

4 Proof of Theorem 2

Let $n = d_1 d_2$, d_1, $d_2 > 1$ be integers, and consider the following two sets:

$$\mathcal{A} = \{u + v \cdot d_1 d_2 : 0 \le u \le d_1 - 1, 0 \le v \le d_2 - 1\},$$

$$\mathcal{B} = \{k d_1 d_2^2 + w \cdot d_1 : k \in \mathbb{N}, 0 \le w \le d_2 - 1\}.$$

It is easy to see that $|\mathcal{A}| = d_1 d_2$. It is clear that $A(x) = d_1 d_2$ if x is large enough and $B(x) = \frac{x}{d_1 d_2} + O(1)$, which implies $A(x)B(x) - x = O(1)$. Let m be a fixed positive integer. It is clear that any positive integer m can be written uniquely in the form

$$m = k d_1 d_2^2 + u d_1 + l d_1 d_2 + v,$$

where k is a nonnegative integer, $0 \le u, l \le d_2$, $0 \le v \le d_1$. Hence $\mathcal{B}$ is an additive complement of $\mathcal{A}$. In the next step we prove that the set $\mathcal{A}$ is not of the form (1). Assume that $\mathcal{A}$ is the form (1). It is clear that the difference of any two elements from $\mathcal{A}$ divisible by n^s. As $\mathcal{A}$ also contains consecutive integers we have $n^s | 1$, which implies $s = 0$. Thus $\mathcal{A} = \{a + i + k_i n : i = 0, \ldots, n-1\}$, that is $\mathcal{A}$ is a complete residue system modulo n, which is a contradiction.

Acknowledgement: The authors would like to thank András Bíró for the valuable discussions.

References

[1] Y.-G. Chen, J.-H. Fang, *On additive complements I.*, Proc. Amer. Math. Soc, **138**, (2010) 1923-1927.

[2] Y.-G. Chen, J.-H. Fang, *On additive complements II.*, Proc. Amer. Math. Soc, **139**, (2011) 881-883.

[3] Y.-G. Chen, J.-H. Fang, *On finite additive complements*, Discrete Math., **313**, (2013) 595-598.

[4] L. Danzer, *Über eine Frage von G. Hanani aus der additiven Zahlentheorie*, J. Reine Angew. Math., **214-215**, (1964) 392-394.

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

[6] Narkiewicz, *Remarks on a conjecture of Hanani in additive number theory*, Colloq. Math., **7**, (1959/60) 161-165.

[7] M. B. Nathanson, *Representation functions of sequences in additive number theory*, Proc. Amer. Math. Soc., **72**, (1978) 16-20.

[8] I. Z. Ruzsa, *Additive completion of lacunary sequences*, In: Paul Erdős and his mathematics, Budapest, 1999.

[9] A. Sárközy, E. Szemerédi, *On a problem in additive number theory*, Acta Math. Hungar., **64**, (1994) 237-245.