On additive complement of a finite set

Sándor Z. Kiss ∗, Eszter Rozgonyi †, Csaba Sándor ‡

May 11, 2014

Abstract

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

$$a + b = n, \quad a \in A, \quad b \in B.$$
We put

\[ A(n) = \sum_{a \leq n \atop a \in A} 1 \quad \text{and} \quad B(n) = \sum_{b \leq n \atop b \in B} 1 \]

respectively. We say a set \( B \subseteq \mathbb{N} \) is an additive complement of the set \( A \subseteq \mathbb{N} \) if every sufficiently large \( n \in \mathbb{N} \) can be represented in the form \( a + b = n \), \( a \in A \), \( b \in B \), i.e., \( R_{A+B}(n) \geq 1 \) for \( n \geq n_0 \). 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 \( A \) and \( B \) if

\[
\limsup_{x \to +\infty} \frac{A(x)B(x)}{x} \leq 1,
\]

then

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

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

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

then

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

In the other direction they proved in [2] that for any integer \( a \geq 2 \), there exist two infinite additive complements \( A \) and \( B \) 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 \( A \) 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 \( A \) and \( B \) with \( |A| < +\infty \) or \( |B| < +\infty \), 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

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

2
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_i3^{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

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

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

$$\mathcal{A} = \{a + ip^s + k_ip^{s+1} : i = 0, \ldots, p - 1\},$$

(1)

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

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

(2)

In the case when the number of elements of $\mathcal{A}$ is a composite number, we disprove the 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

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

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 $\theta$ be an algebraic number. We say the monic polynomial $f$ is the minimal polynomial of $\theta$ if $f$ is the least degree such that $f(\theta) = 0$. It is well-known that if $f$ is the minimal polynomial of $\theta$, and $g$ is a polynomial such that $g(\theta) = 0$, then $f | g$. A complex number is called primitive $n$th root of unity if 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 $\zeta$ runs over all the primitive $n$th 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 $\zeta$ and

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

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 $B$ of $A$, $|A| = p$ such that

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

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

$$
+\infty > C = \liminf_{x \to +\infty} (A(x)B(x) - x) = \liminf_{x \to +\infty} \left( \left( \sum_{a \in A} 1 \right) \left( \sum_{b \in B} 1 \right) - x \right) \geq
$$
\[ \geq \liminf_{x \to +\infty} \left( \sum_{a \in A, b \in B \atop a + b \leq x} 1 - x \right) = \liminf_{x \to +\infty} \left( \sum_{n=0}^{x} R_{A+B}(n) - x \right) \geq \]

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

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

thus we have

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

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

\[ R_{A+B}(n) = 1 \quad \text{for} \quad n \geq n_1. \quad (5) \]

In the next step we prove that \( A \) is the form (1). Let \( z = re^{2i\pi \alpha} = re(\alpha) \), where \( r < 1 \). Let the generating functions of the sets \( A \) and \( B \) be \( f_A(z) = \sum_{a \in A} z^a \) and \( f_B(z) = \sum_{b \in B} z^b \) 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

\[ f_A(z) \cdot f_B(z) = \left( \sum_{a \in A} z^a \right) \left( \sum_{b \in B} z^b \right) = \sum_{n=0}^{+\infty} R_{A+B}(n) z^n = \]

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

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

\[ (1-z)f_A(z) \cdot f_B(z) = (1-z)p_1(z) + z^{n_1}. \quad (6) \]

In next step we prove that \( f_B(z) \) can be written in the form

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

$$(1 - z)f_A(z) \cdot f_B(z) = \sum_{n=0}^{\infty} c_n z^n,$$

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 $f_B(z)$ satisfies 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

$$f_A(z) \cdot \left( F_B(z) + \frac{T(z)}{1 - z^M} \right) = p_1(z) + \frac{z^{n_1}}{1 - z},$$

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

$$(1 - z^M)f_A(z)F_B(z) + f_A(z)T(z) = (1 - z^M)p_1(z) + (1 + z + z^2 + \ldots + z^{M-1})z^{n_1}.$$ (8)

By putting $z = 1$, we obtain that

$$f_A(1)T(1) = M.$$ (9)

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

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

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

$$\Phi_{p^t}(z)|f_A(z)T(z).$$

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

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

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

$$0 \leq r_1 \leq r_2 \leq \ldots \leq r_p < p^{s+1}. \quad (10)$$

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 an integer $j$ with $1 \leq j \leq p$ such that

$$r_{j+1} - r_j \geq p^{s}. \quad (11)$$

In the next step we prove that this implies

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

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

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

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

$$0 \leq t_i \leq p^{s+1} - p^s. \quad (13)$$

As $f_A(\omega) = 0$, and the definition of $\omega$ we obtain that

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

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

Let $n = d_1d_2$, $d_1$, $d_2 > 1$ be integers, and consider the following two sets:

$$A = \{u + v \cdot d_1d_2 : 0 \leq u \leq d_1 - 1, 0 \leq v \leq d_2 - 1\},$$

$$B = \{kd_1d_2^2 + w \cdot d_1 : k \in \mathbb{N}, 0 \leq w \leq d_2 - 1\}.$$ 

It is easy to see that $|A| = d_1d_2$. It is clear that $A(x) = d_1d_2$ if $x$ is large enough and $B(x) = \frac{x}{d_1d_2} + O(1)$, 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

$$m = kd_1d_2^2 + ud_1 + ld_1d_2 + v,$$

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