Publ. Math. Debrecen
77/3-4 (2010), 261–276

On the sumset of geometric progressions

By ATTILA BÉRCZES (Debrecen)

This paper is dedicated to Professor P. Dömösi

Abstract. The present paper gives a complete answer to the question of the cardinality of sumsets of finite geometric progressions with positive real quotient. The proof of the main result is based on theorems concerning irreducibility and GCD of trinomials and quadrinomials.

1. Introduction

In a lecture given at the University of Debrecen, I. Z. Ruzsa asked, what can we say about the cardinality of sumsets of finite geometric progressions with positive real quotient. The goal of the present paper is to completely answer this question.

For non-empty sets A and B we define their sumset by

$$A + B := \{a + b : a \in A,\ b \in B\}.$$

If $A = B$ we also define the restricted sumset of A by

$$A \widehat{+} A := \{a + b : a \in A,\ b \in A, a \neq b\}.$$

Mathematics Subject Classification: Primary: 11B75; Secondary: 11P70, 11C08, 12D05.
Key words and phrases: sumset, geometric progression, quadrinomoial, trinomial.
The research was supported in part by grants T75566 and T67580 of the Hungarian National Foundation for Scientific Research, the János Bolyai Research Fellowship of the Hungarian Academy of Sciences, by the National Office for Research and Technology. The work is supported by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, co-financed by the European Social Fund and the European Regional Development Fund.

Our results belong to the family of sum-product estimates, which say that the number of sums and the number of products cannot be both small for a given set. Geometric progressions represent one extremity, when the number of products is as small as possible, namely $2n-1$ for an n-element set. We confirm the natural expectation, that in this case the number of sums is near to its largest possible value $n(n+1)/2$. We mention that there is a similar but weaker phenomenon at the other extreme (arithmetic progressions), see e.g. [1].

Several results on sumsets of various kind of sets are available in the literature. For such results we refer to [5], [2] and the references given there. However, since the results of the present paper are not much connected to those results, and the techniques of the proofs are also quite different, we omit to mention them explicitly in the introduction.

The above mentioned phenomenon is most clearly shown by the following corollary to our main result:

Corollary. *Put $A := \{1, q, q^2, \ldots, q^n\}$ where $q \neq 1$ is a positive real number. For $n \geq 9$, the minimal value of $|A+A|$ is*

$$\frac{n(n+1)}{2} - (4n-22),$$

and it is achieved when q is a root of $x^3 - x + 1$ or $x^3 - x^2 + 1$.

Now we present our main result:

Theorem 1.1 (Main Theorem)**.** *Put $A := \{1, q, q^2, \ldots, q^n\}$ where $q \neq 1$ is a positive real number. Then we have the following propositions.*

(1) *If q is not a zero of any polynomial of the form $x^a - x^b - x^c + 1$ with $a > b > c > 0$ then we have $|A \hat{+} A| = \frac{n(n-1)}{2}$ and $|A+A| = \frac{n(n+1)}{2}$.*

(2) *If q is a zero of a polynomial $F(x) = x^a - x^b - x^c + 1$ with $a > b > c > 0$ but $F(x)$ is not of the form $x^{2u} - x^{2u-v} - x^u + 1$, $x^{3u} - x^{3u-v} - x^{2u-v} + 1$, $x^{2u} - x^u - x^v + 1$ or $x^{3u} - x^{u+v} - x^v + 1$ with $u > v$ then*
   - *if $n \geq a$ then we have $|A \hat{+} A| = \frac{n(n-1)}{2} - (n-a+1)$ and $|A+A| = \frac{n(n+1)}{2} - (n-a+1)$;*
   - *if $n < a$ then we have $|A \hat{+} A| = \frac{n(n-1)}{2}$ and $|A+A| = \frac{n(n+1)}{2}$.*

(3) *If q is a zero of a polynomial $F(x) = x^a - 2x^b + 1$ with $a > b > 0$ but the minimal polynomial of q is not of the form $x^{3r} - x^r - 1$ or $x^{3r} + x^{2r} - 1$ with $r > 0$ then*
   - *if $n \geq a$ then we have $|A \hat{+} A| = \frac{n(n-1)}{2}$ and $|A+A| = \frac{n(n+1)}{2} - (n-a+1)$;*

- *if* $n < a$ *then we have* $|A\hat{+}A| = \frac{n(n-1)}{2}$ *and* $|A + A| =|, \frac{n(n+1)}{2}$.

(4) *If* q *is a zero of one of the polynomials* $x^{2u} - x^{2u-v} - x^u + 1$, $x^{3u} - x^{3u-v} - x^{2u-v} + 1$, $x^{2u} - x^u - x^v + 1$ *or* $x^{3u} - x^{u+v} - x^v + 1$ *with* $u > v$ *but the minimal polynomial of* q *is not of the form* $x^{3r} - x^r - 1$ *or* $x^{3r} + x^{2r} - 1$ *with* $r > 0$ *then*

- *if* $n \geq 3u$ *we have* $|A\hat{+}A| = \frac{n(n-1)}{2} - (2n - 5u + 2)$ *and* $|A + A| = \frac{n(n+1)}{2} - (2n - 5u + 2)$*;*
- *if* $2u \leq n < 3u$ *we have* $|A\hat{+}A| = \frac{n(n-1)}{2} - (n - 2u + 1)$ *and* $|A + A| = \frac{n(n+1)}{2} - (n - 2u + 1)$*;*
- *if* $n < 2u$ *we have* $|A\hat{+}A| = \frac{n(n-1)}{2}$ *and* $|A + A| = \frac{n(n+1)}{2}$.

(5) *If the minimal polynomial of* q *is of the form* $x^{3r} - x^r - 1$ *or* $x^{3r} + x^{2r} - 1$ *with* $r > 0$ *then*

- *if* $n \geq 9r$ *we have* $|A\hat{+}A| = \frac{n(n-1)}{2} - (3n-19r+3)$ *and* $|A+A| = \frac{n(n+1)}{2} - (4n - 26r + 4)$*;*
- *if* $7r \leq n < 9r$ *we have* $|A\hat{+}A| = \frac{n(n-1)}{2} - (2n - 10r + 2)$ *and* $|A + A| = \frac{n(n+1)}{2} - (3n - 17r + 3)$*;*
- *if* $6r \leq n < 7r$ *we have* $|A\hat{+}A| = \frac{n(n-1)}{2} - (2n - 10r + 2)$ *and* $|A + A| = \frac{n(n+1)}{2} - (2n - 10r + 2)$*;*
- *if* $4r \leq n < 6r$ *we have* $|A\hat{+}A| = \frac{n(n-1)}{2} - (n - 4r + 1)$ *and* $|A + A| = \frac{n(n+1)}{2} - (n - 4r + 1)$*;*
- *if* $n < 4r$ *we have* $|A\hat{+}A| = \frac{n(n-1)}{2}$ *and* $|A + A| = \frac{n(n+1)}{2}$*;*

Remark. It is clear, that the sumset of $A := \{1, q, q^2, \dots, q^n\}$ has cardinality at most $\frac{n(n+1)}{2}$, and it can be smaller than that only in the case when

$$q^{n_1} + q^{n_2} = q^{n_3} + q^{n_4}$$

for some integers $n_1, n_2, n_3, n_4 \in \{1, \dots, n\}$. However, this means that q is a zero of a polynomial of the form $x^a - x^b - x^c + 1$. The question is in fact, whether it may happen, that q is a zero of more then one such quadrinomial. So to answer our original question we have to investigate common zeros of some lacunary polynomials. Similar reasoning is true in the case of the restricted sumset of A.

2. Results on common zeros of some lacunary polynomials

According to the above Remark, in order to prove our Main Theorem we need some results concerning common zeros of some quadrinomials and trinomials.

Theorem 2.1. *If the polynomials $F(x) := x^n - x^m - x^k + 1$ and $H(x) := x^\alpha - x^\beta - x^\gamma + 1$ have a common zero which is not a root of unity, then we have one of the following cases*

(1) $F = H$

(2) $F(x) = x^{2u} - x^{2u-v} - x^u + 1$ *and* $H(x) = x^{3u} - x^{3u-v} - x^{2u-v} + 1$, *with* $u > v$

(3) $F(x) = x^{4s} - x^{3s} - x^{2s} + 1$ *and* $H(x) = x^{9s} - x^{8s} - x^{5s} + 1$

(4) $F(x) = x^{9s} - x^{8s} - x^{5s} + 1$ *and* $H(x) = x^{4s} - x^{3s} - x^{2s} + 1$

(5) $F(x) = x^{3u} - x^{3u-v} - x^{2u-v} + 1$ *and* $H(x) = x^{2u} - x^{2u-v} - x^u + 1$, *with* $u > v$

and in the cases (2)–(5) *the polynomials can be interchanged.*

Although the following theorem is due to A. Schinzel (in fact it is Theorem 2 of [4]) we present it here, since its role in the proof of our Main Theorem is similar to the role played by Theorems 2.1 and 2.3.

Theorem 2.2 (A. Schinzel [4])**.** *If the distinct polynomials $F(x) := x^n - 2x^m + 1$ and $H(x) := x^\alpha - 2x^\beta + 1$ have a common zero then it is a root of unity.*

Theorem 2.3. *If the polynomials $F(x) := x^n - 2x^m + 1$ and $H(x) := x^\alpha - x^\beta - x^\gamma + 1$ have a common zero which is not a root of unity, then we have one of the following cases*

(1) $F(x) = x^{7r} - 2x^{5r} + 1$ *and* $H(x) = x^{4r} - x^{3r} - x^{2r} + 1$

(2) $F(x) = x^{7r} - 2x^{5r} + 1$ *and* $H(x) = x^{9r} - x^{8r} - x^{5r} + 1$

(3) $F(x) = x^{7r} - 2x^{5r} + 1$ *and* $H(x) = x^{6r} - x^{5r} - x^{3r} + 1$

(4) $F(x) = x^{7r} - 2x^{2r} + 1$ *and* $H(x) = x^{4r} - x^{2r} - x^r + 1$

(5) $F(x) = x^{7r} - 2x^{2r} + 1$ *and* $H(x) = x^{9r} - x^{4r} - x^r + 1$

(6) $F(x) = x^{7r} - 2x^{2r} + 1$ *and* $H(x) = x^{6r} - x^{3r} - x^r + 1$.

In the first three cases the minimal polynomial of the common zero which is not a root of unity is $x^{3r} - x^r - 1$ and in the last three cases it is $x^{3r} + x^{2r} - 1$, respectively.

3. Auxiliary results

A polynomial $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{R}[x]$ (with $a_n \neq 0$) is called reciprocal if $a_i = a_{n-i}$ for $i = 0, \ldots, n$ and it is called anti-reciprocal if

$a_i = -a_{n-i}$ for $i = 0, \dots, n$, respectively. Clearly, a polynomial $P(x) \in \mathbb{R}[x]$ is reciprocal if and only if $P(x) = x^n P\left(\frac{1}{x}\right)$ and it is anti-reciprocal, if and only if $P(x) = -x^n P\left(\frac{1}{x}\right)$.

For a polynomial $P(x) \in \mathbb{R}[x]$ of degree n put $P^*(x) := x^n P\left(\frac{1}{x}\right)$. Then the polynomial $P(x)P^*(x)$ is clearly reciprocal.

Note also, that a polynomial whose zeros are all roots of unity is either reciprocal or anti-reciprocal, depending on the parity of the multiplicity of 1 as a zero of the polynomial.

Notation. The following notation shall be useful in the proofs of the results below. For a polynomial $P(x)$ of degree d denote by $m_0(P), \dots, m_t(P)$ the monomials of P in decreasing order of their degrees. Further, denote by $e_0(P), \dots, e_t(P)$ the coefficients and by $d_0(P), \dots, d_t(P)$ the degrees of $m_0(P), \dots, m_t(P)$, respectively. Thus P is a reciprocal polynomial if and only if $d_i = d - d_{t-i}$ and $e_i = e_{t-i}$ for every $i = 1, \dots, t$. Similarly, P is an anti-reciprocal polynomial if and only if $d_i = d - d_{t-i}$ and $e_i = -e_{t-i}$ for every $i = 1, \dots, t$. Whenever it is clear which polynomial P is considered we omit the reference to this polynomial in the notation.

Lemma 3.1 (A. Schinzel [4]). *For the factorization of the lacunary polynomial $F(x) = x^n - 2x^m + 1$ $(n > m)$ we have one of the following possibilities:*

(A) $F(x) = x^{7r} - 2x^{5r} + 1 = (x^r - 1)(x^{3r} - x^r - 1)(x^{3r} + x^{2r} + 1)$, $r \in \mathbb{Z}$,

(B) $F(x) = x^{7r} - 2x^{2r} + 1 = (x^r - 1)(x^{3r} + x^{2r} - 1)(x^{3r} + x^r + 1)$, $r \in \mathbb{Z}$,

(C) *$F(x) = A(x)B(x)$, where $A(x)$ is a polynomial whose zeros are all roots of unity, and $B(x)$ is an irreducible polynomial, which has no zero which is a root of unity.*

Proof. This is Theorem 1 of [4]. □

Note. The factors occurring in cases (A) and (B) of Lemma 3.1 are irreducible (see Lemma 3.8)

Lemma 3.2 (W. H. Mills [3]). *The polynomial $F(x) = x^n - x^m - x^k + 1$ $(n > m > k > 1)$ can be written in the form $F(x) = A(x)B(x)$, where $A(x) \in \mathbb{Q}[x]$ is a polynomial whose zeros are all roots of unity, and $B(x) \in \mathbb{Q}[x]$ is an irreducible polynomial, which has no zero which is a root of unity.*

Proof. This lemma is a part of Theorem 2 of [3]. □

Lemma 3.3. *Let $F(x) := x^n - x^m - x^k + 1$ and $G(x) := x^a - x^b - x^c + 1$ be polynomials such that $F(x)G(x)$ is a reciprocal polynomial. Suppose that 1 is neither a multiple root of F nor of G. Then we have one of the following cases*

(A) $F = G^*$

(B) $F(x) = x^{2u} - x^{2u-v} - x^u + 1$ *and* $G(x) = x^{3u} - x^{u+v} - x^v + 1$, *with* $u > v$

(C) $F(x) = x^{4s} - x^{3s} - x^{2s} + 1$ *and* $G(x) = x^{9s} - x^{4s} - x^s + 1$

(D) $F(x) = x^{9s} - x^{8s} - x^{5s} + 1$ *and* $G(x) = x^{4s} - x^{2s} - x^s + 1$

(E) $F(x) = x^{3u} - x^{3u-v} - x^{2u-v} + 1$ *and* $G(x) = x^{2u} - x^u - x^v + 1$, *with* $u > v$,

and in the cases (B)–(E) *the polynomials* F *and* G *can be interchanged.*

Proof. Put $R := FG$, and suppose that R is reciprocal. Denote by $d := n + a$ the degree of R. Clearly, $m_0 = x^{a+n}$ and $m_t = 1$. In order to verify whether R is reciprocal or not, we have to compare the coefficients and the degrees of the other monomials, too. Without loss of generality suppose that $c \le k$. The other cases follow by interchanging the role of F and G. Now we split the proof of Lemma 3.3 to several cases and subcases.

First suppose that $c = k$. Then $m_{t-1} = -2x^k$ which means that e_1 must be -2, too, and we must have $d_1 = d - k$. This can happen only if $d_1 = n + b = m + a = (n + a) - k$. This means that $n = m + k$ which contradicts the condition that 1 is not a multiple root of F.

Thus we have $c < k$, which means that $m_{t-1} = -x^c$. If R is reciprocal we must have $d_1 = d - d_{t-1}$ and $e_1 = e_{t-1}$. For m_1 we have 3 possible cases.

If $n + b > m + a$ then $m_1 = -x^{n+b}$ and by $d_1 = d - d_{t-1}$ we have $n + b = n + a - c$, i.e. $a = b + c$, which contradicts the fact that $x = 1$ is a simple root of G.

If $n + b = m + a$ then $m_1 = -2x^{n+b}$ and $e_1 = e_{t-1}$ cannot be fulfilled.

If $n + b < m + a$ then $m_1 = -x^{m+a}$ and by $d_1 = d - d_{t-1}$ we have $m + a = n + a - c$, i.e. $n = m + c$. Since both for m_2 and m_{t-2} now there are 3 possibilities, we have to consider several subcases, according to the order of the numbers $n + b, a + k$ and k, b, respectively.

(I) If $n + b = a + k$ then $m_2 = -2x^{n+b}$. In this case we clearly must have $e_{t-2} = -2$, which can happen only if $k = b$. Thus $n = a$, and by $d_2 = d - d_{t-2}$ we also have $a + k = n + b = (n + a) - k = n + a - b$, i.e. $2b = a$ and $2k = n$. Further, we also have $n = m + c$, i.e. $c = 2k - m$. These altogether mean, that $F(x) = x^{2k} - x^m - x^k + 1$ and $G(x) = x^{2k} - x^k - x^{2k-m} + 1$. This means $F = G^*$, which is case A of our lemma.

(II) If $n + b < a + k$ then $m_2 = -x^{a+k}$, and we have the following cases with respect to m_{t-2}:

  (1) If $k = b$ then $m_{t-2} = -2x^k$, thus $e_{t-2} = -2$ which together with $e_2 = -1$ contradicts the fact that R is reciprocal.

(2) If $k < b$ then we have $m_{t-2} = -x^k$, and since $m_2 = -x^{a+k}$ we get $a + k = n + a - k$, which means that $n = 2k$. Now we have to consider m_3 and m_{t-3}. We have the following possibilities

(i) If $n + b > a$ then $m_3 = -x^{n+b}$, and we have six possibilities to consider, according to the possible values of b, m and $k + c$

(a) If $c + k < \min(b, m)$ then $m_{t-3} = x^{c+k}$ and $e_{t-3} = 1$, which together with $e_3 = -1$ contradicts the fact that R is reciprocal.

(b) If $b < \min(c + k, m)$ then $m_{t-3} = -x^b$ and $n + b = n + a - b$, which leads to $a = 2b$. We have $n = m + c$ and since we are in case II2 we also have $n = 2k$. These show that $F(x) = x^{2k} - x^{2k-c} - x^k + 1$ and $G(x) = x^{2b} - x^b - x^c + 1$. Thus $R(x) = (x^{2b+2k} - x^{2b+2k-c} - x^{2b+k} - x^{b+2k}) + x^{2k+b-c} - x^{2k+c} + x^{2b} + x^{k+b} + 2x^{2k} + x^{k+c} - x^{2k-c} + (-x^b - x^k - x^c + 1)$. Further we have $2k-c < 2k < k+b < 2b < 2k+b-c$ (indeed, $b < m = 2k-c$) and $k+c < 2k < k+b < 2b < 2k+c$. Taking in account that $-x^{2k-c}$ has coefficient -1, these show that R can be reciprocal only in the following cases:

- if $2k - c = (2k + 2b) - (2k + c)$ then $k = b$ and we have $F = G^*$ which is case A of our lemma.
- if $2k - c = k + c$ then $k = 2c$ and $F(x) = x^{4c} - x^{3c} - x^{2c} + 1$ and $G = x^{2b} - x^b - x^c + 1$. Thus we have $R(x) = (x^{4c+2b} - x^{3c+2b} - x^{2c+2b} - x^{4c+b}) - x^{5c} + x^{3c+b} + x^{2b} + x^{2c+b} + 2x^{4c} + (-x^b - x^{2c} - x^c + 1)$, and $2c < b < 3c$. However this means that $3c + b > 5c > 4c$ and $3c + b > 2b > 2c + b > 4c$, which contradicts that R is reciprocal.

(c) If $m < \min(b, c+k)$ then $m_{t-3} = -x^m$ and $n+b = n+a-m$, which leads to $a = b + m$. We have $n = m + c$ and since we are in case II2 we also have $n = 2k$. Thus $m = 2k - c$ and $a = 2k + b - c$. Then $F(x) = x^{2k} - x^{2k-c} - x^k + 1$ and $G(x) = x^{2k+b-c} - x^b - x^c + 1$. Thus $R(x) = (x^{4k-c+b} - x^{4k-2c+b} - x^{3k-c+b} - x^{2k+b}) + 2x^{2k} + 2x^{2k-c+b} + x^{k+b} + x^{k+c} - x^{2k+c} - x^b + (-x^{2k-c} - x^k - x^c + 1)$. Now since R is reciprocal, we either have $(4k - c + b) - (k + c) \in \{2k, 2k - c + b, b + k\}$ or we have $c + k \in \{2k + c, b, \frac{4k-c+b}{2}\}$. Since $k > c$ we have $3k + b - 2c > 2k + b - c > 2k$ and $3k + b - 2c > b + k$, thus we can exclude the first possibility. Further, $c + k \neq 2k + c$

and $2(c+k) < 4k - c + b$ (since $c < k$ and $c < b$) leaves us the only possibility that $b = k + c$. Now using this we get $F(x) = x^{2k} - x^{2k-c} - x^k + 1$ and $G(x) = x^{3k} - x^{k+c} - x^c + 1$, which is case B of our lemma.

(d) If $b = m < c+k$ then $m_{t-3} = -2x^b$. Thus we have $e_{t-3} = -2$ which together with $e_3 = -1$ (indeed we are in case II(2)i) contradicts the fact that R is reciprocal.

(e) If $m = c + k < b$ then since $m = 2k - c$ we have $k = 2c$, so it follows $F(x) = x^{4c} - x^{3c} - x^{2c} + 1$ and $G(x) = x^a - x^b - x^c + 1$. Thus $R(x) = (x^{4c+a} - x^{3c+a} - x^{2c+a}) - x^{4c+b} + x^{3c+b} + x^{2c+b} - x^{5c} + 2x^{4c} + x^a - x^b + (-x^{2c} - x^c + 1)$. Now we clearly have $m_3 = -x^{4c+b}$. Since we are in case II(2)ie we have $b > c + k = 3c$ and thus $b + 4c > 7c > 5c > 4c$. These together with $a > b$ and $b + 4c > b + 3c > b + 2c > b$ show that we have three possibilities, namely $m_{t-3} = 2x^{4c}$, $m_{t-3} = -x^b$ or $b = 4c$.

- If $m_{t-3} = 2x^{4c}$ we get contradiction, since $e_3 = -1$ and $e_{t-3} = 2$.
- If $m_{t-3} = -x^b$ then $4c+b = (4c+a)-b$, and we get $a = 2b$. This leads to $R(x) = (x^{4c+2b} - x^{3c+2b} - x^{2c+2b} - x^{4c+b}) + x^{3c+b} + x^{2c+b} - x^{5c} + 2x^{4c} + x^{2b} + (-x^b - x^{2c} - x^c + 1)$. This can be reciprocal only if $5c \in \{3c + b, 2c + b, 4c, 2b, \frac{4c+2b}{2}\}$. Since $b > 3c$ all these possibilities lead to contradiction.
- If $b = 4c$ then we have $F(x) = x^{4c} - x^{3c} - x^{2c} + 1$ and $G(x) = x^a - x^{4c} - x^c + 1$. Then $R(x) = (x^{4c+a} - x^{3c+a} - x^{2c+a}) - x^{8c} + x^{7c} + x^{6c} - x^{5c} + x^{4c} + x^a + (-x^{2c} - x^c + 1)$. Since we are in case II(2)i we have $a < n + b < 8c$, thus $m_3 = -x^{8c}$. Now both the case $m_{t-3} = x^a$ and $m_{t-3} = x^{4c}$ leads to contradiction with the fact that R is reciprocal.

(f) If $b = c + k \leq m$ then we have $F(x) = x^{2k} - x^{2k-c} - x^k + 1$ and $G(x) = x^a - x^{c+k} - x^c + 1$, and we get $R(x) = (x^{2k+a} - x^{2k-c+a} - x^{k+a}) - x^{3k+c} + x^{3k} + 2x^{2k} - x^{2k-c} + x^a + (-x^k - x^c + 1)$. Now $m_3 = -x^{3k+c}$, and either $m_{t-3} = x^a$ or $m_{t-3} = -x^{2k-c}$. The first case contradicts the fact that R is reciprocal, since we would have $e_3 = -1$ and $e_{t-3} = 1$. Thus we must have $m_{t-3} = -x^{2k-c}$, which leads to $2k-c = (2k+a) - (3k+c)$, i.e. $a = 3k$. Thus we have $F(x) = x^{2k} - x^{2k-c} - x^k + 1$

and $G(x) = x^{3k} - x^{c+k} - x^{c} + 1$, and this is again case B of our lemma.

Similarly, in case II(2)ii), i.e. when $n+b < a+k, k < b, n+b < a$ (more precisely in a subcase of it) we get case (C) of our lemma, and subcases of case III (i.e. when $n+b > a+k$) lead to case (D) and case (E) of our lemma. However, since the computation is lengthy, we omit it. The interested reader will find the full version of the proof at the URL http://www.math.klte.hu/∼berczesa/papers/p21full.pdf.

Clearly, in the case $c > k$ we get the same results, just the polynomials F and G are interchanged. □

Lemma 3.4. *Let $F(x) := x^n - 2x^m + 1$ and $G(x) := x^a - 2x^b + 1$ be polynomials such that $F(x)G(x)$ is a reciprocal polynomial. Suppose that 1 is neither a multiple zero of F nor of G. Then we have $F = G^*$.*

Proof. Clearly we have

$$F(x)G(x) = x^{a+n} - 2x^{a+m} - 2x^{n+b} + 4x^{m+b} + x^n + x^a - 2x^m - 2x^b + 1.$$

Put $R := FG$. Then by assumption R is reciprocal. Denote by $d := n + a$ the degree of R. Clearly, $m_0 = x^{a+n}$ and $m_t = 1$.

We may suppose without loss of generality that $b \leq m$.

If $b = m$ then we get

$$R(x) = x^{a+n} - 2x^{a+m} - 2x^{n+m} + 4x^{2m} + x^n + x^a - 4x^m + 1.$$

Since R is reciprocal we must have $a + m = n + m$ and $a + n = (a + m) + m$, which leads to $n = 2m$. This contradicts the fact that 1 is a simple root of F.

Thus we may suppose that $b < m$. This means that $m_{t-1} = -2x^b$. We have to distinguish between three cases

(I) If $a + m = n + b$ then $m_1 = -4x^{a+m}$ which together with $m_{t-1} = -2x^b$ contradicts the fact that R is reciprocal.

(II) If $a + m < n + b$ then $m_1 = -2x^{n+b}$ and since R is reciprocal we get $n + b = (n + a) - b$. This means that $a = 2b$ which contradicts the fact that 1 is a simple root of G.

(III) If $a + m > n + b$ then $m_1 = -2x^{a+m}$ and since R is reciprocal we get $a + m = (n + a) - b$. Thus we get $b = n - m$ and

$$R(x) = x^{a+n} - 2x^{a+m} - 2x^{2n-m} + 5x^n + x^a - 2x^m - 2x^{n-m} + 1.$$

Since R is reciprocal and $2n - m > n > m$ we clearly can have neither $a \geq 2n - m$ nor $a \leq m$. Thus we have $m_2 = -2x^{2n-m}$ and $m_{t-2} = -2x^m$, showing that $a + n = 2n - m + m$, which is $a = n$. Now we have $F(x) = x^n - 2x^m + 1$ and $G(x) = x^n - 2x^{n-m} + 1$, which means that $F = G^*$. □

Lemma 3.5. *Let $F(x) := x^n - 2x^m + 1$ and $G(x) := x^a - x^b - x^c + 1$ be polynomials. Suppose that 1 is neither a multiple zero of F nor of G. Then we have that $F(x)G(x)$ cannot be a reciprocal polynomial.*

Proof. Clearly we have

$$\begin{aligned} F(x)G(x) = x^{a+n} - 2x^{a+m} - x^{n+b} + 2x^{m+b} - x^{n+c} + x^n + x^a \\ + 2x^{m+b} + 2x^{m+c} - x^b - 2x^m - x^c + 1. \end{aligned}$$

Put $R := FG$. Then by assumption R is reciprocal. Denote by $d := n + a$ the degree of R. Clearly, $m_0 = x^{a+n}$ and $m_t = 1$.

Now we have the following possibilities:

(I) if $m < c$ then we have $m_{t-1} = -2x^m$. Since R is reciprocal we must have $a + m > n + b$, and thus $m_1 = -2x^{a+m}$. These together lead to $a + m = (a + n) - m$, which is $n = 2m$. However, this contradicts the fact that 1 is a simple root of F.

(II) if $m = c$ then by the reciprocal property of R we must also have $a+m = n+b$ and this leads again to the relation $n = 2m$, which is a contradiction again.

(III) if $m > c$ then $m_{t-1} = -x^c$ and we clearly must have $a+m < n+b$, in order to guarantee the reciprocal property of R. This means that $n + b = (a + n) - c$, which shows that $a = b + c$ and this contradicts the fact that 1 is a simple root of G. □

Lemma 3.6. *Let $F(x)$ be one of the polynomials $x^{3r} - x^r - 1$, $x^{3r} + x^{2r} - 1$, $x^{3r} + x^r + 1$ and $x^{3r} + x^{2r} + 1$. Let $G(x) := x^a - 2x^b + 1$ and suppose that 1 is not a multiple root of G. Then $F(x)G(x)$ cannot be an anti-reciprocal polynomial.*

Proof. First we consider the case $F(x) = x^{3r} - x^r - 1$. Suppose indirectly that $F(x)G(x)$ is an anti-reciprocal polynomial. Clearly, we have

$$R(x) := F(x)G(x) = x^{a+3r} - x^{a+r} - 2x^{b+3r} + 2x^{b+r} - x^a + x^{3r} + 2x^b - x^r - 1.$$

Now $m_0 = x^{a+3r}$ and $m_t = -1$, and we have the following cases

(I) If $r < b$ then $m_{t-1} = -x^r$. In this case $a + r \geq b + 3r$ is not possible since $(a+r)+r < a+3r$ would be a contradiction to the fact that R is anti-reciprocal. Further, if $a+r < b+3r$ then $e_1 = -2$ also leads to contradiction.

(II) If $r = b$ then we have $m_{t-1} = x^r$, and $a + r \geq b + 3r$ leads again to the contradiction $(a + r) + r < a + 3r$. Further, $b + 3r > a + r$ leads to $m_1 = -2x^{b+3r}$ and this is a contradiction, as well.

(III) if $r > b$ then $m_{t-1} = 2x^b$ and again $a + r > b + 3r$ leads to $m_1 = -x^{a+r}$ and $a + r = b + 3r$ leads to $m_1 = -3x^{b+3r}$, respectively, and these both contradict the assumption that R is anti-reciprocal. So the only remaining case is $b+3r > a+r$, which leads to $m_1 = -2x^{b+3r}$ and $(b+3r)+b = a+3r$, i.e. $a = 2b$, which is a contradiction to the assumption that 1 is not a multiple root of G.

The cases $F(x) = x^{3r} + x^r + 1$ and $F(x) = x^{3r} + x^{2r} + 1$ are trivial, and the case $F(x) = x^{3r}+x^{2r}-1$ can be easily deduced from the case $F(x) = x^{3r}-x^r-1$, since $-(x^{3r} + x^{2r} - 1)^* = x^{3r} - x^r - 1$. □

Lemma 3.7. *Let $F(x)$ be one of the polynomials $x^{3r} - x^r - 1$, $x^{3r} + x^{2r} - 1$, $x^{3r} + x^r + 1$ and $x^{3r} + x^{2r} + 1$. Let $G(x) := x^a - x^b - x^c + 1$ and suppose that 1 is not a multiple root of G. Then $F(x)G(x)$ can be an anti-reciprocal polynomial only in one of the following cases*

(A) *$F(x) = x^{3r} - x^r - 1$ and $G(x) = x^{4r} - x^{2r} - x^r + 1$*

(B) *$F(x) = x^{3r} - x^r - 1$ and $G(x) = x^{9r} - x^{4r} - x^r + 1$*

(C) *$F(x) = x^{3r} - x^r - 1$ and $G(x) = x^{6r} - x^{3r} - x^r + 1$*

(D) *$F(x) = x^{3r} + x^{2r} - 1$ and $G(x) = x^{4r} - x^{3r} - x^{2r} + 1$*

(E) *$F(x) = x^{3r} + x^{2r} - 1$ and $G(x) = x^{9r} - x^{8r} - x^{5r} + 1$*

(F) *$F(x) = x^{3r} + x^{2r} - 1$ and $G(x) = x^{6r} - x^{5r} - x^{3r} + 1$.*

Proof. First we consider the case $F(x) = x^{3r} - x^r - 1$. Suppose that $F(x)G(x)$ is an anti-reciprocal polynomial. Clearly, we have

$$\begin{aligned} R(x) := F(x)G(x) &= x^{a+3r} - x^{a+r} - x^{b+3r} + x^{b+r} - x^{3r+c} \\ &\quad + x^{r+c} - x^a + x^{3r} + x^b + x^c - x^r - 1. \end{aligned}$$

Now $m_0 = x^{a+3r}$ and $m_t = -1$, and we have the following cases

(I) if $r < c$ then we have $m_{t-1} = -x^r$. Since $r + (a + r) < a + 3r$ in order to guarantee the anti-reciprocal property of R we must have $b + 3r > a + r$, but then $e_1 = -1$ and $e_{t-1} = -1$ contradict the anti-reciprocal property of R.

(II) if $r = c$ then

$$R(x) = x^{a+3r} - x^{a+r} - x^{b+3r} + x^{b+r} - x^a - x^{4r} + x^{3r} + x^{2r} + x^b - 1.$$

We have $3r > 2r = c + r$, which means that we have the following 3 possibilities with respect to m_{t-1}

(1) if $b > 2r$ then $m_{t-1} = x^{2r}$. Thus by the anti-reciprocal property of R we must have $d_1 = a+r$, i.e. $a+r > b+3r$, which means that $m_1 = -x^{a+r}$. Now we have the following possibilities for m_2

(i) if $a > b+3r$ then $m_2 = -x^a$ and this shows that m_{t-2} must be x^{3r}, and since $a > b$ this proves $b > 3r$ and we get

$$R(x) = (x^{a+3r} - x^{a+r} - x^a) - x^{b+3r} + x^{b+r} - x^{4r} \\ + x^b + (x^{3r} + x^{2r} - 1).$$

Now since $b > 3r$ we have $m_3 = -x^{b+3r}$, and since $b+r > \max(b, 4r)$ there are 3 possibilities

- if $b = 4r$, then we must have $(b+3r) + (b+r) = a+3r$, i.e. $a = 9r$. Then FG is indeed reciprocal and we have $G(x) = x^{9r} - x^{4r} - x^r + 1$, which is case (B) of our lemma.
- if $b < 4r$ then we have $m_{t-3} = x^b$ and $b + (b+3r) = a+3r$, i.e. $a = 2b$. Then we either must have $(b+r) + 4r = a+3r$, i.e. $b = 2r$, thus $a = 4r$ which contradicts $a > b+3r$, or we have $b + r = 4r$, i.e. $b = 3r$, which contradicts again $a > b+3r$.
- if $b > 4r$ we get contradiction by $m_{t-3} = -x^{4r}$.

(ii) if $a < b+3r$ then $m_2 = -x^{b+3r}$ and we again have 3 subcases for m_{t-2}

(a) if $b < 3r$ then $m_{t-2} = x^b$, and $b + (b+3r) = a+3r$, i.e. $a = 2b$ and we have

$$R(x) = (x^{a+3r} - x^{a+r} - x^{b+3r}) + x^{b+r} - x^{4r} - x^a \\ + x^{3r} + (x^b + x^{2r} - 1).$$

Since $b < 3r$ we have $b+r < 4r$ and by $b > 2r$ and $a = 2b$ we have $a > 4r$. So $m_3 = -x^a$ and $m_{t-3} = x^{3r}$. Since $4r \neq b+r$ we must have $4r + (b+r) = a+3r$, which leads to $b = 2r$ which is a contradiction to $b > 2r$.

(b) if $b = 3r$ then $m_{t-2} = 2x^{3r}$ which is a contradiction.

(c) if $b > 3r$ then $m_{t-2} = x^{3r}$ and $(b+3r) + 3r = a+3r$, i.e. $a = 3r$, which contradicts the condition $b > 3r$.

(iii) if $a = b+3r$ then $m_2 = -2x^{b+3r}$ and the only way to make possible the anti-reciprocal property of R is to put $b = 3r$, thus we have $m_2 = 2x^{3r}$ and we see that $3r + (b+3r) = a+3r$ is also fulfilled. In this case we have $a = 6r$ and we get $G(x) = x^{6r} - x^{3r} - x^r + 1$, which is case (C) of our lemma.

(2) if $b = 2r$, then we have $m_{t-1} = 2x^b$, so we must have $a+r = b+3r$, i.e. $a = 4r$. Thus we have

$$R(x) = x^{7r} - 2x^{5r} - 2x^{4r} + 2x^{3r} + 2x^{2r} - 1.$$

In this case we have $F(x) = x^{3r} - x^r - 1$ and $G(x) = x^{4r} - x^{2r} - x^r + 1$, which is case (A) of our lemma.

(3) if $b < 2r$ then $m_{t-1} = x^b$ and we have 3 possibilities for m_1

(i) if $a + r > 3r + b$ then $m_1 = -x^{a+r}$, and by $(a+r) + b = a + 3r$ we get the contradiction $b = 2r$

(ii) if $a + r = 3r + b$ then $m_1 = -2x^{a+r}$ which is a contradiction

(iii) if $a + r < 3r + b$ then $m_1 = -x^{3r+b}$, and $(3r+b) + b = 3r + a$, i.e. $a = 2b$. In this case have

$$\begin{aligned} R(x) = {} & (x^{2b+3r} - x^{b+3r}) - x^{2b+r} + x^{b+r} - x^{4r} - x^{2b} \\ & + x^{3r} + x^{2r} + (x^b - 1). \end{aligned}$$

Now since $b < 2r$ and $b > c = r$ we have $b + r > 2r$, and $4r > 3r > 2r$, so we have $m_{t-2} = x^{2r}$ and

(a) if $2b + r > 4r$, then $m_2 = -x^{2b+r}$. Now $4r > 2b > 3r > b + r$ shows that $m_3 = -x^{4r}$ and $m_{t-3} = x^{b+r}$. Thus $(b+r)+4r = 2b + 3r$ leads to $b = 2r$, which is a contradiction to $b < 2r$.

(b) if $4r > 2b + r$ then $m_2 = -x^{4r}$ and $4r + 2r = 2b + 3r$ leads to $2b = 3r$, which contradicts $4r > 2b + r$.

(c) if $4r = 2b + r$ then $m_2 = -2x^4r$ is a contradiction to $m_{t-2} = x^{2r}$, since R is supposed to be anti-reciprocal.

(III) if $c < r$ then $m_{t-1} = x^c$ and we have 3 possibilities for m_1

(1) if $a + r < b + 3r$ then $m_1 = -x^{b+3r}$ and $c + (b + 3r) = a + 3r$, i.e. $a = b + c$, which is a contradiction to the fact that 1 is a simple root of G.

(2) if $a + r = b + 3r$ then $m_1 = -2x^{b+3r}$ is a contradiction

(3) if $a+r > b+3r$ then $m_1 = -x^{a+r}$, and $(a+r)+c = a+3r$, i.e. $c = 2r$, which is a contradiction to $c < r$.

Clearly, if $F = x^{3r} + x^{2r} - 1 = -(x^{3r} - x^r - 1)^*$, then we get cases (D), (E) and (F), and if F is one of the polynomials $x^{3r} + x^r + 1$ and $x^{3r} + x^{2r} + 1$ then $F(x)G(x)$ cannot be anti-reciprocal. □

Lemma 3.8. *The polynomials $x^{3r} - x^r - 1$, $x^{3r} + x^{2r} - 1$, $x^{3r} + x^r + 1$ and $x^{3r} + x^{2r} + 1$ are irreducible for each natural number r.*

Proof. Tverberg in [6] proves that any polynomial $x^n \pm x^m \pm 1$ is irreducible (over the field of rational numbers) whenever none of its zeros is a root of unity. Since no zero of the polynomials $x^3 - x - 1$, $x^3 + x^2 - 1$, $x^3 + x + 1$ and $x^3 + x^2 + 1$ is a root of unity, this proves our lemma. □

4. Proof of the theorems

Proof of Theorem 2.1. Clearly, $x = 1$ is a simple root of F, since otherwise we would get $F'(1) = 0$, thus $n = m + k$ and $F = (x^m - 1)(x^k - 1)$ and each root of F would be a root of unity, which cannot happen by the assumption of our Theorem. Similarly, $x = 1$ is a simple root of H.

By Lemma 3.2 both F and H may have at most one irreducible factor which has a zero being not a root of unity. Further, by our assumption such a factor exists, and it is the same factor in the case of F and H. So we have $F(x) = A_1(x)B(x)$ and $H(x) = A_2(x)B(x)$, where A_1 and A_2 are polynomials with all their zeros being roots of unity, and B is an irreducible polynomial such that none of its zeros is a root of unity. Now, since 1 is exactly double zero of $F(x)H^*(x)$, clearly $F(x)H^*(x) = A_1(x)A_2^*(x)B(x)B^*(x)$ is a reciprocal polynomial. Since all the assumption of Lemma 3.3 are fulfilled we get all the possibilities for F and H^* and the Theorem follows easily. □

Proof of Theorem 2.2. Suppose that F and H have a common zero which is not a root of unity. Denote it by α. Then clearly, $x = 1$ is a simple root of F, since otherwise we would get $F'(1) = 0$, thus $n = 2m$ and $F = (x^m - 1)^2$, so each zero of F would be a root of unity, which cannot happen by the assumption of our theorem. Similarly, $x = 1$ is a simple zero of H.

Now if F and H are not of the type $x^{7r} - 2x^{5r} + 1$ ($r \in \mathbb{Z}$) or $x^{7r} - 2x^{2r} + 1$ ($r \in \mathbb{Z}$), then by Lemma 3.1 we have $F(x) = A_1(x)B(x)$ and $H(x) = A_2(x)B(x)$, where A_1 and A_2 are polynomials with all their zeros being roots of unity, and B is an irreducible polynomial such that none of its zeros is a root of unity. Now, since 1 is exactly double zero of $F(x)H^*(x)$, clearly $F(x)H^*(x) = A_1(x)A_2^*(x)B(x)B^*(x)$ is a reciprocal polynomial, which cannot happen by Lemma 3.4.

If F is of the form $x^{7r}-2x^{5r}+1$ $(r \in \mathbb{Z})$ or $x^{7r}-2x^{2r}+1$ $(r \in \mathbb{Z})$, and H is not of this form, then α is a zero of one of the polynomials $x^{3r}+x^{2r}+1$, $x^{3r}+x^r+1$, $x^{3r}+x^{2r}-1$ or $x^{3r}-x^r-1$, call it F_0. Since by Lemma 3.8 $F_0(x)$ is irreducible, and α is a zero of both F_0 and H we get by Lemma 3.1 that H can be written in the form $H(x) = A_2(x)F_0(x)$, where A_2 is a polynomial with all its zeros being roots of unity. Now 1 is a simple root of $F_0(x)H^*(x) = A_2^*(x)F_0(x)F_0^*(x)$, thus $F_0(x)H^*(x)$ is an anti-reciprocal polynomial. But this is not possible by Lemma 3.6.

If both F and H are of the form $x^{3r}+x^{2r}+1$, $x^{3r}+x^r+1$, $x^{3r}+x^{2r}-1$ or $x^{3r}-x^r-1$, then since all these polynomials are irreducible, they can have a common root only if they coincide. □

Proof of Theorem 2.3. Suppose that F and H have a common zero which is not a root of unity. Denote it by α. Then clearly, $x=1$ is a simple zero of F, since otherwise we would get $F'(1)=0$, thus $n=2m$ and $F=(x^m-1)^2$ and each zero of F would be a root of unity, which cannot happen by the assumption of our Theorem. Similarly, $x=1$ is a simple root of H.

Now if F is not of the type $x^{7r}-2x^{5r}+1$ $(r \in \mathbb{Z})$ or $x^{7r}-2x^{2r}+1$ $(r \in \mathbb{Z})$, then by Lemmas 3.1 and 3.2 we have $F(x) = A_1(x)B(x)$ and $H(x) = A_2(x)B(x)$, where A_1 and A_2 are polynomials with all their zeros being roots of unity, and B is an irreducible polynomial such that none of its zeros is a root of unity. Now, since 1 is exactly double zero of $F(x)H^*(x)$, clearly $F(x)H^*(x) = A_1(x)A_2^*(x)B(x)B^*(x)$ is a reciprocal polynomial, which cannot happen by Lemma 3.4.

If F is of the form $x^{7r}-2x^{5r}+1$ $(r \in \mathbb{Z})$ or $x^{7r}-2x^{2r}+1$ $(r \in \mathbb{Z})$, then α is a zero of one of the polynomials $x^{3r}+x^{2r}+1$, $x^{3r}+x^r+1$, $x^{3r}+x^{2r}-1$ or $x^{3r}-x^r-1$, call it F_0. Since by Lemma 3.8 $F_0(x)$ is irreducible, and α is a zero of both F_0 and H we get by Lemma 3.2 that H can be written in the form $H(x) = A_2(x)F_0(x)$, where A_2 is a polynomial with all its zeros being roots of unity. Now 1 is a simple zero of $F_0(x)H^*(x) = A_2^*(x)F_0(x)F_0^*(x)$, thus $F_0(x)H^*(x)$ is an anti-reciprocal polynomial. But this leads by Lemma 3.7 to the cases listed in our theorem. □

Proof of the Main Theorem. Put $I := \{(i,j) \mid i,j \in Z,\ 0 \le i \le j \le n\}$ and $\widehat{I} := \{(i,j) \mid i,j \in Z,\ 0 \le i < j \le n\}$. Clearly, we have

$$A+A = \{q^i+q^j \mid (i,j) \in I\}$$

and

$$A\widehat{+}A = \{q^i+q^j \mid (i,j) \in \widehat{I}\}$$

If none of the sums q^i+q^j and q^k+q^l coincide for $(i,j)\neq(k,l)$, $(i,j),(k,l)\in I$ ($(i,j),(k,l)\in\widehat{I}$, respectively) then we clearly have $|A+A|=\frac{n(n+1)}{2}$ ($|A\widehat{+}A|=\frac{n(n-1)}{2}$).

If we have $q^i+q^j=q^k+q^l$ for some pairs $(i,j)\neq(k,l)$, $(i,j),(k,l)\in I$ ($(i,j),(k,l)\in\widehat{I}$, respectively), then if we suppose without loss of generality that $i=\max\{i,j,k,l\}$ then we have $j=\min\{i,j,k,l\}$, since $q\neq 1$ is a positive real number. Suppose again without loss of generality that $k\geq l$ and put $a:=i-j$, $b:=k-j$, $c:=l-j$. We see that q is a zero of the polynomial $x^a-x^b-x^c+1$ (x^a-2x^b+1, respectively). However, if q is a zero of such a polynomial, then along with the coincidence $q^a+1=q^b+q^c$ ($q^a+1=2q^b$, respectively) we also have the equalities $q^{a+h}+q^h=q^{b+h}+q^{c+h}$ ($q^{a+h}+q^h=2q^{b+h}$, respectively) for $0\leq h\leq n-a$. Now Theorems 2.1, 2.2 and 2.3 cover all cases when q is a common root of more than one such polynomial, and the proof of our Main Theorem is concluded by counting the coincidences $q^i+q^j=q^k+q^l$ in these cases. □

References

[1] G. Elekes and I. Z. Ruzsa, Few sums, many products, *Studia Sci. Math. Hungar.* **40** (2003), 301–308.

[2] A. Geroldinger and I. Z. Ruzsa, Combinatorial Number Theory and Additive Group Theory, *Birkhäuser*, 2009.

[3] W. H. Mills, The factorization of certain quadrinomials, *Math. Scand.* **57** (1985), 44–50.

[4] A. Schinzel, Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives de nombres irrationnels, *Colloq. Math.* **9** (1962), 291–296.

[5] T. Tao and V. Vu, Additive Combinatorics, Vol. 105, Cambridge Studies in Advanced Mathematics, *Cambridge*, 2006.

[6] H. Tverberg, On the irreducibility of the trinomials $x^n\pm x^m\pm 1$, *Math. Scand.* **8** (1960), 121–126.

ATTILA BÉRCZES
INSTITUTE OF MATHEMATICS
UNIVERSITY OF DEBRECEN
NUMBER THEORY RESEARCH GROUP
HUNGARIAN ACADEMY OF SCIENCES AND
UNIVERSITY OF DEBRECEN
H-4010 DEBRECEN, P.O. BOX 12
HUNGARY

E-mail: berczesa@math.klte.hu

(Received July 30, 2009; revised February 11, 2010)