ON THE SUMSET OF BINARY RECURRENCE SEQUENCES

ATTILA BÉRCZES AND ATTILA PETHŐ

Dedicated to the 90th birthday of Professor Lajos Tamássy

1. Introduction

For a subset $\mathcal{A}$ of $\mathbb{Z}$ we define the restricted sumset of $\mathcal{A}$ by

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

Answering a question of I.Z. Ruzsa, A. Bérczes [1] gave a complete description of the restricted sumset of geometric progressions having positive real quotient. In this connection, it is natural to ask whether it is possible to give a similar description of the restricted sumset of binary recurrence sequences? The present paper answers the question for Lucas sequences.

Several results on sumsets of various kind of sets are available in the literature. For such results we refer to [6], [4] 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.

Recall that a Lucas sequence is a binary recurrence sequence given by

$$R_n := A \cdot R_{n-1} + B \cdot R_{n-2}, \quad R_0 := 0, R_1 := 1, \tag{1.1}$$

2000 Mathematics Subject Classification: 11B13,11B37.

Keywords and Phrases: binary recurrence sequence, sumset.

The research was supported in part by the University of Debrecen, and by grants K100339 and NK104208 of the Hungarian National Foundation for Scientific Research. The work is supported by the TÁMOP-4.2.2.C-11/1/KONV-2012-0001 project. The project is implemented through the New Hungary Development Plan, co-financed by the European Social Fund and the European Regional Development Fund.

where $A, B \in \mathbb{Z}$ are non-zero numbers. Further, the two roots of the characteristic polynomial $x^2 - Ax - B$ of the sequence are

$$\alpha := \frac{A + \sqrt{A^2 + 4B}}{2}, \quad \beta := \frac{A - \sqrt{A^2 + 4B}}{2}, \tag{1.2}$$

and the elements of the sequence can be expressed by the so-called Binet formula

$$R_n := \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{1.3}$$

We say that the recurrence has a dominant root if $|\alpha| \neq |\beta|$. Clearly, the sequence given by (1.1) has a dominant root if and only if the discriminant of the characteristic polynomial is positive, i.e. $A^2 + 4B > 0$. For the above definitions and well known facts see [5] and [2].

Throughout these notes we assume $AB \neq 0$ and $\frac{\alpha}{\beta}$ is not a root of unity and call R_n a non-degenerate Lucas sequence. Note that if the discriminant of the characteristic polynomial is non-positive then the second assumption implies that both of α and β are not roots of unity. These are natural assumptions with respect to the investigated problem. Indeed, if $B = 0$ then $R_n = A^n$ for $n \geq 1$, i.e. R_n is a geometric progression with quotient A, which was the topic of the paper of the first author [1]. If $\frac{\alpha}{\beta} = \eta$ is a root of unity of order k, which happens for example if $A = 0$, then there are two subcases: $\eta = 1$ or $k > 1$, actually $k = 2, 3, 4$ or 6. If $\eta = 1$, i.e. $\alpha = \beta$ then $R_n = n, n \geq 0$. Otherwise

$$R_n = \beta^{n-1} \frac{\eta^n - 1}{\eta - 1}.$$

Thus $R_n = 0$ whenever $k|n$. Moreover, if β is a root of unity then R_n assumes only finitely many different values. In all these cases the cardinality of the restricted sumset depends heavily on the choice of the subset.

The situation is completely different under the assumptions above. Concerning the cardinality of the restricted sumset of a Lucas sequence we split our investigation depending on the sign of the discriminant of the characteristic polynomial. For sequences without dominant root we prove the following:

Theorem 1.1. *Let R_n be a non-degenerate Lucas sequence with $A^2+4B<0$, and put $\mathcal{A} := \{R_n | n \in \mathbb{Z}, 0 \leq n \leq N\}$, with $N \geq 3$. Then we have*

$$|\mathcal{A}\widehat{+}\mathcal{A}| = \frac{N(N+1)}{2} - O(1).$$

For Lucas sequences with a dominant root we can prove a more precise result, which completely answers the question of the second author.

Theorem 1.2. *Let R_n be a non-degenerate Lucas sequence with $A^2+4B>0$, and put $\mathcal{A} := \{R_n | n \in \mathbb{Z}, 0 \leq n \leq N\}$, with $N \geq 3$. Then we have the following statements:*

- *If $(A,B) \notin \{(1,1),(-1,1)\}$*
$$|\mathcal{A}\widehat{+}\mathcal{A}| = \frac{N(N+1)}{2}.$$
- *If $(A,B) \in \{(1,1),(-1,1)\}$*
$$|\mathcal{A}\widehat{+}\mathcal{A}| = \frac{N(N+1)}{2} - (N-2).$$

The above Theorem 1.2 is a trivial consequence of the following Proposition.

Proposition 1.1. *Let R_n be a non-degenerate Lucas sequence with $A^2+4B>0$. Let a,b,c,d be distinct non-negative integers. Then*

$$R_a + R_d = R_b + R_c \tag{1.4}$$

can happen only in the following cases:

(i) $A=1, B=1, b=a-1, c=a-2, d=0,$
(ii) $A=-1, B=1, b=a-2, c=0, d=a-1.$

Theorem 1.1 is just a simple consequence of Proposition 1.2 below.

Proposition 1.2. *Let R_n be a non-degenerate Lucas sequence with $A^2+4B<0$. Then the number of 4-tuples (a,b,c,d) with $\max(a,b,c,d)=a$ and $b>c$, for which (1.4) is fulfilled, is bounded by*

$$2 \cdot e^{42^{21} \cdot 15}.$$

2. Auxiliary results

Let us consider the equation

$$a_1x_1 + \cdots + a_nx_n = 1 \quad \text{in } x_1, \ldots, x_n \in \Gamma, \tag{2.5}$$

where Γ is a finitely generated subgroup of rank $r > 0$ of $\overline{\mathbb{Q}}^*$. A solution $(x_1, \ldots, x_n)$ of (2.5) is called non-degenerate, if there is no vanishing subsum of the sum $\sum_{i=1}^n a_ix_i$.

Lemma 2.1. *The number of non-degenerate solutions of equation (2.5) is bounded by*

$$e^{(6n)^{3n}(nr+1)}.$$

Proof. This is the result of Evertse, Schmidt and Schlickewei. See Theorem 1.1 of [3] and the first paragraph on page 810 of [3]. □

Lemma 2.2. *Let a, b, c, d be distinct non-negative integers, such that $a > \max\{b, c, d\}$. Let f be the function defined by*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) := x^a - x^b - x^c + x^d.$$

Then the following statements are true:

(a) *f is strictly monotonic on the interval $]-\infty, -2[$. More precisely, f is strictly monotonically increasing on $]-\infty, -2[$ if a is odd, and strictly monotonically decreasing on $]-\infty, -2[$ if a is even.*

(b) *If $x \leq -4$ then $|f(x)| > 2^{a+1}$.*

(c) *If $-2 \leq x < 0$ then $|f(x)| \leq 2^{a+1}$.*

(d) *If $x \leq -3$ then $|f(x)| > 12$.*

(e) *If $-1 \leq x < 0$ then $|f(x)| \leq 4$.*

(f) *If $x \leq -2$ and $a \geq 6$ then $|f(x)| \geq 8$.*

(g) *If $x \leq -3$ and $a \geq 6$ then $|f(x)| \geq 2^{a+2}$.*

Proof. The derivative of f is $f'(x) = ax^{a-1} - bx^{b-1} - cx^{c-1} + dx^{d-1}$.

First suppose that a is odd, and $x < -2$. Then ax^{a-1} is positive, and we have

$$\begin{aligned} f'(x) &\geq 2a|x|^{a-2} - bx^{b-1} - cx^{c-1} + dx^{d-1} \\ &\geq a|x|^{a-2} + 2a|x|^{a-3} - bx^{b-1} - cx^{c-1} + dx^{d-1} > 0. \end{aligned}$$

Now suppose that a is even, and $x < -2$. Then ax^{a-1} is negative, and we have

$$\begin{aligned} f'(x) &\leq -2a|x|^{a-2} - bx^{b-1} - cx^{c-1} + dx^{d-1} \\ &\leq -a|x|^{a-2} - 2a|x|^{a-3} - bx^{b-1} - cx^{c-1} + dx^{d-1} < 0. \end{aligned}$$

This concludes the proof of statement (a) of Lemma 2.2.

If $x \leq -4$ then

$$\begin{aligned} |f(x)| &= |x^a - x^b - x^c + x^d| \geq |x|^a - |x|^b - |x|^c - |x|^d \\ &\geq 4|x|^{a-1} - |x|^b - |x|^c - |x|^d > |x|^{a-1} \geq 4^{a-1} = 2^{2a-2} \geq 2^{a+1}, \end{aligned}$$

which concludes the proof of statement (b) of Lemma 2.2.

If $-2 \leq x < 0$ then

$$\begin{aligned} |f(x)| &= |x^a - x^b - x^c + x^d| \leq |x|^a + |x|^b + |x|^c + |x|^d \\ &\leq 2^a + 2^b + 2^c + 2^d < 2^{a+1}, \end{aligned}$$

which concludes the proof of statement (c) of Lemma 2.2.

If $x \leq -3$ then

$$\begin{aligned} |f(x)| &= |x^a - x^b - x^c + x^d| \geq |x|^a - |x|^b - |x|^c - |x|^d \\ &\geq 3|x|^{a-1} - |x|^b - |x|^c - |x|^d \geq |x|^{a-1} + 6|x|^{a-2} - |x|^b - |x|^c - |x|^d \\ &> 4 \cdot |x|^{a-2} \geq 4 \cdot 3^{a-2} \geq 12, \end{aligned}$$

which concludes the proof of statement (d) of Lemma 2.2.

If $-1 \leq x < 0$ then

$$|f(x)| = |x^a - x^b - x^c + x^d| \leq |x|^a + |x|^b + |x|^c + |x|^d \leq 4,$$

which concludes the proof of statement (e) of Lemma 2.2.

If $x \leq -2$ and $a \geq 6$ then

$$\begin{aligned} |f(x)| &= |x^a - x^b - x^c + x^d| \geq |x|^a - |x|^b - |x|^c - |x|^d \\ &\geq 2|x|^{a-1} - |x|^b - |x|^c - |x|^d \geq |x|^{a-1} + 2|x|^{a-2} - |x|^b - |x|^c - |x|^d \\ &\geq |x|^{a-1} + |x|^{a-2} + 2|x|^{a-3} - |x|^b - |x|^c - |x|^d \geq |x|^{a-3} \geq 2^{a-3} \geq 8, \end{aligned}$$

which concludes the proof of statement (f) of Lemma 2.2.

If $x \leq -3$ and $a \geq 6$ then we have $a > \frac{2\log 3}{\log 3 - \log 2}$, thus $3^{a-2} \geq 2^a$, and we get

$$\begin{aligned}|f(x)| &= |x^a - x^b - x^c + x^d| \geq |x|^a - |x|^b - |x|^c - |x|^d \\ &\geq 3|x|^{a-1} - |x|^b - |x|^c - |x|^d \geq |x|^{a-1} + 6|x|^{a-2} - |x|^b - |x|^c - |x|^d \\ &\geq 4|x|^{a-2} \geq 4\cdot 3^{a-2} \geq 4\cdot 2^a \geq 2^{a+2},\end{aligned}$$

which concludes the proof of statement (g) of Lemma 2.2.

□

3. Proof of Proposition 1.1

Recall that a non-degenerate Lucas sequence is given by (1.1) with $AB \neq 0$, and we also have the closed formula (1.3). The assumption $A^2 + 4B > 0$ together with $AB \neq 0$ implies that α/β is not a root of unity.

We split the proof in several subcases:

Case I: $A > 0, B > 0$

In this case by (1.1) we have

$$R_i > 0, \quad R_i > R_{i-1} \quad \text{for every } i \geq 1. \tag{3.6}$$

Without loss of generality, we may suppose that $a > b > c > d$, and thus

$$R_a + R_d = AR_{a-1} + BR_{a-2} + R_d \geq AR_b + BR_c + R_d \geq R_b + R_c, \tag{3.7}$$

and the equality in (3.7) may hold if and only if $A = B = 1$, $R_d = 0$, $R_b = R_{a-1}$ and $R_c = R_{a-2}$, i.e. R_n is the Fibonacci sequence, $b = a-1$, $c = a-2$, and $d = 0$.

Case II: $A < 0$, $B > 0$

In this case we define the sequence $Q_0 = 0, Q_1 = 1$ and

$$Q_n := |A| \cdot Q_{n-1} + B \cdot Q_{n-2} \quad \text{for } n \geq 2, \tag{3.8}$$

and we have $Q_n := |R_n|$. More precisely it is easily shown by induction that

$$R_i = (-1)^{i+1} Q_i, \quad Q_i > 0, \quad Q_i > Q_{i-1} \quad \text{for every } i \geq 1. \tag{3.9}$$

These show that

$$\operatorname{sgn}(AR_{a-1}) = \operatorname{sgn}(BR_{a-2}) \quad \text{for every } a \geq 2. \tag{3.10}$$

Without loss of generality, we may suppose that $a > \max\{b, c, d\}$ and $b > c$. Thus using (1.1), (3.9) and (3.10) we have

$$\begin{aligned}|R_a + R_d| &\geq |R_a| - |R_d| = |AR_{a-1} + BR_{a-2}| - |R_d| \\ &= |A| \cdot |R_{a-1}| + |B| \cdot |R_{a-2}| - |R_d| \\ &\geq |A| \cdot |R_b| + |B| \cdot |R_c| - |R_d| > |R_b| + |R_c| \geq |R_b + R_c|,\end{aligned}$$

whenever $|AB| \neq 1$.

So we have to check the case $A = -1, B = 1$. If $d = a - 2$ then

$$|R_a + R_d| = |R_a + R_{a-2}| = |R_a| + |R_{a-2}| > |R_b| + |R_c| \geq |R_b + R_c|,$$

which is impossible. First suppose that $d = a - 1$ and $b \neq a - 2$. Then we have

$$\begin{aligned}|R_a + R_d| &= | - R_{a-1} + R_{a-2} + R_{a-1}| = |R_{a-2}| = | - R_{a-3} + R_{a-4}| \\ &= |R_{a-3}| + |R_{a-4}| \geq |R_b| + |R_c| \geq |R_b + R_c|,\end{aligned}$$

and we have equality if and only if $b = a-3$, $c = a-4$ and $\mathrm{sgn}(R_b) = \mathrm{sgn}(R_c)$, however, these assumptions are contradictory, so we have

$$|R_a + R_d| > |R_b + R_c|.$$

Now suppose that $d = a - 1$ and $b = a - 2$. In this case

$$R_a + R_d = R_a + R_{a-1} = -R_{a-1} + R_{a-2} + R_{a-1} = R_{a-2} = R_b$$

shows that

$$R_a + R_d = R_b + R_c$$

may be fulfilled if and only if $R_c = 0$, so we get the case $A = -1, B = 1$ and the identity $R_a + R_{a-1} = R_{a-2} + R_0$.

Let us also consider the case $b = a - 1$. Then we have

$$|R_a - R_b| = |R_a - R_{a-1}| = |R_a| + |R_{a-1}| > |R_c| + |R_d| \geq |R_c - R_d|,$$

so $R_a - R_b = R_c - R_d$ cannot be fulfilled.

Finally, suppose that $d \neq a-1$, $d \neq a-2$ and $b \neq a-1$. Now using that $\operatorname{sgn}(R_{a-2}) = \operatorname{sgn}(-R_{a-3})$ we have

$$\begin{aligned}|R_a + R_d| &= |-R_{a-1} + R_{a-2} + R_d| \geq |-R_{a-1} + R_{a-2}| - |R_d| \\ &\geq |2R_{a-2} - R_{a-3}| - |R_d| \geq 2|R_{a-2}| + |R_{a-3}| - |R_d| \\ &> |R_{a-2}| + |R_{a-3}| \geq |R_b| + |R_c| \geq |R_b + R_c|.\end{aligned}$$

Case III: $A < 0$, $B < 0$

In this case by (1.2) we have $\beta < \alpha < 0$. Further, by (1.3) equation (1.4) may be written in the form

$$\alpha^a - \alpha^b - \alpha^c + \alpha^d = \beta^a - \beta^b - \beta^c + \beta^d. \tag{3.11}$$

If $\alpha \leq -2$ then clearly $\beta < -2$ and by statement (a) of Lemma 2.2 the equation (3.11) cannot be fulfilled. If $\alpha > -2$ and $\beta \leq -4$ then statements (b) and (c) of Lemma 2.2 imply that (3.11) cannot be fulfilled.

So we have to check the cases when $\alpha > -2$ and $\beta > -4$. However, $\beta > -4$ may happen only if $A \geq -7$. More precisely, combining these with $A^2 + 4B > 0$ we see that we must have

$$(A, B) \in \{(-5,-5), (-5,-6), (-4,-1), (-4,-2), (-4,-3), (-3,-1), (-3,-2)\}.$$

In the cases $(A, B) \in \{(-4,-1), (-4,-2), (-4,-3)\}$ we have $-1 \leq \alpha < 0$ and $\beta \leq -3$, so by statements (d) and (e) of Lemma 2.2 we have $R_a + R_d \neq R_b + R_c$.

If $(A, B) = (-5,-5)$ and $(A, B) = (-5,-6)$ then $-2 \leq \alpha < 0$ and $\beta \leq -3$ yield by statements (c) and (g) of Lemma 2.2 that $R_a + R_d \neq R_b + R_c$, provided that $a \geq 6$.

If $(A, B) = (-3,-1)$ and $(A, B) = (-3,-2)$ then $-1 \leq \alpha < 0$ and $\beta \leq -2$ yield by statements (e) and (f) of Lemma 2.2 that $R_a + R_d \neq R_b + R_c$, provided that $a \geq 6$.

So we have to check the identity $R_a + R_d = R_b + R_c$ for $a < 6$ if $(A, B) \in \{(-5,-5), (-5,-6), (-3,-1), (-3,-2)\}$. Using MAGMA we checked all these possibilities and we saw that also in these cases we have $R_a + R_d \neq R_b + R_c$. This concludes the prof of Case III.

Case IV: $A > 0$, $B < 0$

In this case we obviously have $A \geq 3$ and we prove that

$$\frac{R_{i+1}}{R_i} > \frac{A}{2}, \quad \text{for } i \geq 1. \tag{3.12}$$

Clearly, this is true for $i = 1$, and we proceed by induction. Suppose that for a fixed value of i (3.12) is true. Then we prove that

$$\frac{R_{i+2}}{R_{i+1}} > \frac{A}{2},$$

also holds. Indeed, using also $A^2 + 4B > 0$ we get

$$\begin{aligned} R_{i+2} = AR_{i+1} + BR_i &= \frac{A}{2}R_{i+1} + \frac{A}{2}R_{i+1} + BR_i \\ &> \frac{A}{2}R_{i+1} + \frac{A^2}{4}R_i + BR_i > \frac{A}{2}R_{i+1}. \end{aligned} \tag{3.13}$$

This proves (3.12), which means in addition, that the sequence R_n is strictly monotonically increasing, with non-negative terms.

Without loss of generality, we may suppose that $a > \max\{b, c, d\}$ and $b > c$.

Now suppose that $A \geq 4$. Then

$$R_a + R_d > \frac{A}{2}R_{a-1} + R_d > 2R_{a-1} + R_d > R_b + R_c.$$

So we have to consider the remaining cases $(A, B) = (3, -1)$ and $(A, B) = (3, -2)$. If $b \neq a - 1$ then by (3.12) we have

$$R_a + R_d > \frac{3}{2}R_{a-1} + R_d > \frac{9}{4}R_{a-2} + R_d > R_b + R_c.$$

If $b = a - 1$ then

$$\begin{aligned} R_a + R_d = 3R_{a-1} + BR_{a-2} + R_d &\geq R_b + 2R_{a-1} - 2R_{a-2} + R_d \\ &\geq R_b + 6R_{a-2} - 4R_{a-3} - 2R_{a-2} + R_d \geq R_b + 4R_{a-2} - 4R_{a-3} \\ &\geq R_b + R_c + 3R_{a-2} - 4R_{a-3} \\ &\geq R_b + R_c + \left(\frac{9}{2} - 4\right) R_{a-3} > R_b + R_c. \end{aligned}$$

This concludes the proof of Proposition 1.1.

4. Proof of Proposition 1.2

Recall that a Lucas sequence is given by (1.1), and we also have the closed formula (1.3). Since in Proposition 1.2 we assume that $A^2 + 4B < 0$, and since a Lucas sequence is supposed to be non-degenerate in the sequel we may suppose that α and β are non-real complex numbers such that α/β is not a root of unity, especially α is not a root of unity. Using (1.3) equation (1.4) can be transformed to the equation

$$\alpha^a - \beta^a + \alpha^d - \beta^d = \alpha^b - \beta^b + \alpha^c - \beta^c \quad \text{in } a, b, c, d \in \mathbb{Z}_{\geq 0}. \tag{4.14}$$

However, dividing (4.14) by β^c, we reduce it to an equation of the form

$$x_1 - x_2 + x_3 - x_4 - x_5 + x_6 - x_7 = 1 \quad \text{in } x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in \Gamma, \tag{4.15}$$

where Γ is the multiplicative subgroup of $\overline{\mathbb{Q}}^*$ generated by α and β. If there are no vanishing subsums in (4.14), then the same holds for (4.15) and then by Lemma 2.1 $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ comes from a set of cardinality at most

$$e^{42^{21} \cdot 15}. \tag{4.16}$$

Further as α/β is not a root of unity, for any fixed tuple $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ there exists at most one tuple (a, b, c, d), so equation (1.4) has also at most $e^{42^{21} \cdot 15}$ solutions.

In the sequel we give an upper bound for the number of those solutions of (4.14) in which there is a vanishing subsum. We split the argument into parts, depending on the number of terms in a vanishing subsum.

First we deal with the case when in (4.14) there is a vanishing subsum of two terms. This subsum may be classified in the following types:

- The base of the two terms is the same. Without loss of generality we may suppose that this base is alpha, and we have

  $$\alpha^u = \pm\alpha^v,$$

  which (since $u \neq v$) is impossible because α is not a root of unity.
- The base of the two terms is different, i.e.

  $$\alpha^u = \pm\beta^v$$

with $u, v \in \{a, b, c, d\}$. (Here we may have $u = v$ or $u \neq v$.) Taking conjugates we get

$$\beta^u = \pm\alpha^v$$

and multiplying these two latter equations we get

$$\left(\frac{\alpha}{\beta}\right)^{u+v} = 1,$$

which contradicts the fact that $\frac{\alpha}{\beta}$ is not a root of unity.

Next we suppose that in (4.14) there is no vanishing subsum consisting of two terms, but there is a vanishing subsum consisting of three terms, and consequently another vanishing subsum of 5 terms. This subcase can be split in the following subcases

- There are two terms in the vanishing subsum with the same exponent, i.e.

  $$\alpha^u - \beta^u \pm \gamma^w = 0, \quad u, w \in \{a, b, c, d\},\ \gamma \in \{\alpha, \beta\}.$$

  Taking conjugates this gives

  $$\beta^u - \alpha^u \pm \overline{\gamma}^w = 0,$$

  and adding these two equations we get

  $$\gamma^w + \overline{\gamma}^w = 0$$

  and thus

  $$\alpha^w + \beta^w = 0$$

  which is again impossible, because α/β is not a root of unity.
- There are three different exponents in the vanishing subsum, i.e.

  $$\gamma^u \pm \delta^v \pm \mu^w = 0, \quad u, v, w \in \{a, b, c, d\},\ \gamma, \delta, \mu \in \{\alpha, \beta\},$$

  where u, v, w are pairwise distinct. Taking conjugates and subtracting the two equations we get a vanishing subsum of (4.14) of six terms, which gives a vanishing subsum of two terms, which is impossible, as shown above.

The last case to be treated is when (4.14) has a solution with a vanishing subsum of four terms, but no vanishing subsums of two or three terms. We shall give an upper bound on the number of such solutions.

If all bases in the vanishing subsum are the same (e.g. α) then we have

$$\alpha^a + \alpha^d - \alpha^b - \alpha^c = 0,$$

and we know that α and β are roots of the polynomial $x^a + x^d - x^b - x^c$, which means that $x^2 + Ax + B$ divides $x^a + x^d - x^b - x^c$, however, this means $B = \pm 1$ and by $\Delta = A^2 + 4B < 0$ we must have $B = -1$ and $A = \pm 1$ which is impossible since in these cases α is a root of unity.

If there are different bases, we shall prove that for each such vanishing subsum there are at most $e^{18^9 \cdot 7}$ solutions. Since we may choose the possible vanishing subsum (where not all the bases are equal) in at most $\binom{8}{4} - 2$ ways, the number of possible solution tuples (a, b, c, d) of (1.4) which correspond to a solution of (4.14) with a four term vanishing subsum is

$$68 \cdot e^{18^9 \cdot 7}.$$

So it remains to prove that if in the four-term vanishing subsum there are different bases, then there are at most $e^{18^9 \cdot 7}$ solutions.

The easier case is when there are two coinciding exponents, i.e. the vanishing subsum looks like

$$\alpha^u - \beta^u \pm \gamma^v \pm \delta^w = 0. \tag{4.17}$$

Dividing the above equation by β^u and using Lemma 2.1 we get that the tuple (u, v, w) comes from a set of cardinality at most $e^{18^9 \cdot 7}$. Then taking the other four term vanishing subsum, if (u, v, w) is fixed, then the fourth exponent is also fixed.

Now we consider the harder case, when all four exponents in the vanishing subsum are distinct. In this case the vanishing subsum takes the form

$$\gamma^a \pm \delta^b \pm \eta^c \pm \mu^d = 0, \tag{4.18}$$

where $\gamma, \delta, \eta, \mu \in \{\alpha, \beta\}$, and $a > \max\{b, c, d\}$.

If $|\alpha| = |\beta| \geq 2$ then

$$\begin{aligned}|\gamma|^a &\geq 2|\gamma|^{a-1} \geq |\gamma|^{a-1} + 2|\gamma|^{a-2}\\ &> |\delta|^b + |\eta|^c + |\mu|^d \geq | \pm \delta^b \pm \eta^c \pm \mu^d|,\end{aligned}$$

thus (4.18) cannot hold.

So we have to handle the cases $|\alpha| < 2$, which leads to $N(\alpha) < 4$, i.e. $|B| \leq 3$, which together with $A^2 + 4B < 0$ leads to

$$(A, B) \in \{(\pm 1, -1), (\pm 1, -2), (\pm 2, -2), (\pm 1, -3), (\pm 2, -3), (\pm 3, -3)\}.$$

However, $(A, B) = (\pm 1, -1), (\pm 2, -2), (\pm 3, -3)$ is excluded since the corresponding sequence is degenerate. In the remaining cases $(A, B) = (\pm 1, -2)$, $(\pm 1, -3), (\pm 2, -3)$ it is easy to check that the principal ideals generated by α and by β, respectively, are prime ideals. The vanishing subsum of four terms (which exists by assumption in the presently treated case) has the form

$$\gamma^a \pm \delta^b \pm \eta^c \pm \mu^d = 0,$$

and since $\{\gamma, \delta, \eta, \mu\} \subset \{\alpha, \beta\}$ has cardinality 2, we may suppose without loss of generality that $\gamma \neq \delta$. Dividing by δ^b we get the equation

$$\frac{\gamma^a}{\delta^b} \pm 1 \pm \frac{\eta^c}{\delta^b} \pm \frac{\mu^d}{\delta^b} = 0,$$

which has at most $e^{18^9 \cdot 3}$ solutions. For a fixed solution of this equation $\frac{\gamma^a}{\delta^b}$ is fixed, so using that α and β both generate a prime ideal, and $\gamma \neq \delta$, $\gamma, \delta \in \{\alpha, \beta\}$ we get that a, b are fixed, and using that $\frac{\eta^c}{\delta^b}$ and $\frac{\mu^d}{\delta^b}$ are also fixed, we see that c, d are fixed. This concludes the proof of Proposition 1.2.

References

[1] A. Bérczes, On the sumset of geometric progressions, *Publ. Math. Debrecen*, **77** (2010), 261–276.

[2] Y. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.*, **539** (2001), 75–122.

[3] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, Linear equations in variables which lie in a multiplicative group, *Ann. of Math. (2)*, **155** (2002), 807–836.

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

[5] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Univ. Press, Cambridge–New York, 1986.

[6] T. Tao and V. Vu, *Additive combinatorics*, vol. 105 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 2006.

A. Bérczes
Institute of Mathematics, University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: berczesa@science.unideb.hu

A. Pethő
Department of Computer Science
Faculty of Informatics, University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: petho.attila@inf.unideb.hu