Journal of Integer Sequences, Vol. 20 (2017),
Article 17.8.6

On Arithmetic Progressions in Lucas Sequences

Lajos Hajdu[1]
Institute of Mathematics
University of Debrecen
P. O. Box 400
H-4002 Debrecen
Hungary
hajdul@science.unideb.hu

Márton Szikszai[2]
Institute of Mathematics, University of Debrecen
and
MTA-DE Research Group Equations Functions and Curves
Hungarian Academy of Sciences and University of Debrecen
P. O. Box 400
H-4002 Debrecen
Hungary
szikszai.marton@science.unideb.hu

Volker Ziegler[3]
Institute of Mathematics
University of Salzburg
Hellbrunnerstrasse 34/I
A-5020 Salzburg
Austria
volker.ziegler@sbg.ac.at

Abstract

In this paper, we consider arithmetic progressions contained in Lucas sequences of the first and second kind. We prove that for almost all Lucas sequences, there

[1] The author was supported by the NKFIH grant 115479.

[2] The author was supported by the Hungarian Academy of Sciences.

[3] The author was supported by the Austrian Research Foundation (FWF), Project P24801-N26.

are only finitely many arithmetic three term progressions and their number can be effectively bounded. We also show that there are only a few Lucas sequences which contain infinitely many arithmetic three term progressions and one can explicitly list both the sequences and the progressions in them. A more precise statement is given for sequences with dominant zero.

1 Introduction

The study of additive structures in certain sets of integers has a long history. In particular, the description of arithmetic progressions has attracted the attention of many researchers and is still an actively studied topic with a vast literature. Without trying to be exhaustive and going into details we only mention a few interesting directions.

Bremner [4] found infinitely many elliptic curves such that among the first coordinates of rational points one can find an eight term arithmetic progression. Campbell [5], modifying ideas of Bremner, gave the first example of a progression of length twelve which was later improved to fourteen by MacLeod [11]. For more details on the various generalizations to other families of curves and recent progress we refer to the paper of Ciss and Moody [6] and the references given there.

The study of arithmetic progressions in solution sets of Pellian equations is another interesting direction. Dujella, Pethő, and Tadić [7] showed that for every four term arithmetic progression $(y_1, y_2, y_3, y_4) \neq (0, 1, 2, 3)$ there exist infinitely many pairs (d, m) such that the equation $x^2 - dy^2 = m$ admits solutions with $y = y_i$ for $i = 1, 2, 3, 4$. On the other hand, Pethő and Ziegler [12] proved that for five term arithmetic progressions only a finite number of such equations are possible. For further progress we refer to the papers of Aguirre, Dujella, and Peral [1] and González-Jiménez [10].

In this paper, we connect to the field by considering arithmetic progressions in Lucas sequences. Let A and B be non-zero integers such that the zeros α and β of the polynomial

$$x^2 - Ax - B \tag{1}$$

satisfy that α/β is not a root of unity. Define the sequences $u = (u_n)_{n=0}^{\infty}$ and $v = (v_n)_{n=0}^{\infty}$ via the binary recurrence relations

$$u_{n+2} = Au_{n+1} + Bu_n \qquad \text{and} \qquad v_{n+2} = Av_{n+1} + Bv_n \qquad (n \geq 0) \tag{2}$$

with initial values $u_0 = 0,\ u_1 = 1$ and $v_0 = 2,\ v_1 = A$. We call u and v the Lucas sequences of the first and second kind corresponding to the pair (A, B), respectively.

Remark 1. The classical definition of u and v requires $\gcd(A, B) = 1$ which is needed for certain arithmetic properties to hold. Hence our definition is more relaxed.

Remark 2. The assumption on the zeros of the companion polynomial (1) coincides with the non-degeneracy property. The study of all linear recurrences can effectively be reduced to such sequences, see [8].

The investigation of arithmetic progressions in linear recurrences is not an entirely new topic. Pintér and Ziegler [13] gave a criterion for linear recurrences of general order to contain infinitely many three term arithmetic progressions. Note that the study of three term arithmetic progressions is the first non-trivial problem and is the most general. Further, they proved that the sequence of Fibonacci and Jacobsthal numbers are the only increasing Lucas sequences having infinitely many three term progressions.

In this paper, we connect to the results of Pintér and Ziegler. On one hand, we give an upper bound for the number of three term arithmetic progressions provided that there are only finitely many. On the other hand, we explicitly list all those sequences which contain infinitely many three term arithmetic progressions. Finally, by restricting ourselves to sequences with companion polynomials having a dominant zero, we find all sequences which contain a three term arithmetic progression and give a complete list of the occurrences.

Our main result is as follows:

Theorem 3. *Let $u = (u_n)_{n=0}^{\infty}$ and $v = (v_n)_{n=0}^{\infty}$ be the Lucas sequences of first and second kind, respectively, corresponding to the pair (A, B). Then u and v admit at most $6.45 \cdot 10^{2340}$ triples (k, l, m) such that $u_k < u_l < u_m$ is a three term arithmetic progression, except when u corresponds to $(A, B) = (\pm 1, 1), (\pm 1, 2), (-1, -2)$ and v corresponds to $(A, B) = (\pm 1, 1), (-1, \pm 2)$, in which cases they admit infinitely many.*

Remark 4. We expect that the upper bound in Theorem 3 is very far from being sharp. It would be an interesting problem to study the average number of three term arithmetic progressions in Lucas sequences of the first and second kind.

By imposing stronger restrictions on the sequences we can state much more. Namely, if the companion polynomial (1) has a dominant zero, then it is possible to explicitly list all three term arithmetic progressions in the corresponding sequence.

Theorem 5. *Let $u = (u_n)_{n=0}^{\infty}$ and $v = (v_n)_{n=0}^{\infty}$ be the Lucas sequences of first and second kind, respectively, corresponding to the pair (A, B). Assume that $A^2 + 4B > 0$. Then u and v admit no three term arithmetic progression, except the cases listed in Tables 1 and 2, respectively.*

As an immediate consequence of Theorem 5 we have the following:

Corollary 6. *Let $u = (u_n)_{n=0}^{\infty}$ (resp. $v = (v_n)_{n=0}^{\infty}$) be the Lucas sequence of the first (resp. second) kind corresponding to the pair (A, B). Assume that $A^2 + 4B > 0$. If u (resp. v) contains more than two (resp. one) three term arithmetic progressions, then u (resp. v) contains infinitely many three term arithmetic progressions.*

The ineffective methods we use in the proof of Theorem 3 do not give such sharp bounds as in Corollary 6. However, it would be interesting to find optimal bounds also in the general case, i.e., if we drop the condition $A^2 + 4B > 0$ in Corollary 6.

In the next section, we prove Theorem 5. The main idea is to show that under a testable condition, the growth of the sequence would contradict the existence of any three term

(A,B)	(k,l,m)
$(1,1)$	$(0,1,3),\ (2,3,4),\ (t,t+2,t+3),\ t\geq 0$
$(-1,1)$	$(1,0,2),\ (t,t+1,t+3),\ t\geq 0$
$(1,2)$	$(1,2t+1,2t+2),\ (2,2t+1,2t+2),\ t\geq 1$
$(-1,2)$	$(t+2,t,t+1),\ t\geq 0$
$(2,B),\ B\geq 1$	$(0,1,2)$
$(1,B),\ B\geq 3$	$(1,3,4),\ (2,3,4)$
$(-1,B),\ B\geq 3$	$(1,0,2)$

Table 1: Triples (k,l,m) s.t. (u_k,u_l,u_m) is a three term AP.

(A,B)	(k,l,m)
$(1,1)$	$(1,0,2),\ (t,t+2,t+3),\ t\geq 0$
$(-1,1)$	$(t,t+1,t+3),\ t\geq 0$
$(-1,2)$	$(t,t-1,t+1),\ t\geq 1$
$(-2,1)$	$(1,0,2)$
$(1,3)$	$(1,4,5)$
$(-3,-1)$	$(1,0,2)$

Table 2: Triples (k,l,m) s.t. (v_k,v_l,v_m) is a three term AP.

arithmetic progression. Further, this condition leaves only finitely many explicitly given possibilities for (A,B) which we treat one by one, usually in an elementary way. The proof of Theorem 3 in Section 3 is based on the theory of S-unit equations.

2 The dominant zero case

This section is devoted to the case, where $A^2+4B>0$, that is, the zeros of the companion polynomial (1) are real. First, we remark that in any linear recurrence, the terms can be represented as polynomial-exponential sums depending on the zeros of the companion polynomial. In our situation, this leads to the well-known formulas

$$u_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}\qquad\text{and}\qquad v_n=\alpha^n+\beta^n\qquad(n\geq 0).$$

We will regularly use this interpretation of Lucas sequences instead of the recurrence relation (2).

The following lemma concerns equations satisfied by three term arithmetic progressions.

Lemma 7. *Let $u=(u_n)_{n=0}^\infty$ be any sequence. Suppose that for some n_0 we have $|u_n/u_{n'}|>3$ for every $n>n_0$ and every $n'<n$. If $m>n_0$, then neither of the equations*

$$u_k-2u_l+u_m=0,\qquad u_l-2u_k+u_m=0,\qquad u_k-2u_m+u_l=0\tag{3}$$

has a solution (k,l,m) with $k<l<m$. In particular, u does not admit any three term arithmetic progression with terms corresponding to the indices k,l and m with $\max\{k,l,m\}>n_0$.

Proof. Assuming that $n_0<m$ gives us either $3|u_k|<3|u_l|<|u_m|$ or $3|u_l|<3|u_k|<|u_m|$. In the former case, we have

$$|u_k-2u_l+u_m|\geq |u_m|-|u_k-2u_l|\geq |u_m|-(|u_k|+2|u_l|)>3|u_l|-3|u_l|=0.$$

Thus the first equation of (3) has no solution with $k<l<m$. In an analogous way, one can get the same deduction for $3|u_l|<3|u_k|<|u_m|$ and it is easy to see that the second and third equations of (3) are unsolvable as well. □

We are in need of a good criterion for the applicability of Lemma 7.

Lemma 8. *Let $u=(u_n)_{n=0}^{\infty}$ be the Lucas sequence of the first kind corresponding to the pair (A,B) with $A^2+4B>0$. Assume that $n>n'$. Then $|u_n/u_{n'}|>3$ if n is odd or $n\geq 8$, unless*

- *$B<0$ and $|A|\leq 6$ or*
- *$|A|=1$ and $0<B\leq 9$ or*
- *$|A|=2$ and $0<B\leq 3$.*

Proof. Under our conditions the polynomial X^2-AX-B has a dominant zero, say α. Note that if $|A|>6$ or $|B|>9$, then we have $|\alpha|>3$ and may write

$$\left|\frac{u_n}{u_{n-1}}\right|=\left|\frac{\dfrac{\alpha^n-\beta^n}{\alpha-\beta}}{\dfrac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta}}\right|=\left|\frac{\alpha^n}{\alpha^{n-1}}\frac{1-\left(\frac{\beta}{\alpha}\right)^n}{1-\left(\frac{\beta}{\alpha}\right)^{n-1}}\right|=|\alpha|\left|\frac{1-\theta^n}{1-\theta^{n-1}}\right|>3\left|\frac{1-\theta^n}{1-\theta^{n-1}}\right|$$

with $\theta=\beta/\alpha$. It suffices to prove that

$$\left|\frac{1-\theta^n}{1-\theta^{n-1}}\right|>1.$$

Observe that there are trivial cases. These include $\theta>0$ and also $\theta<0$ when n is odd. What remains to consider is the case when $\theta<0$ and n is even.

Next, we show that the quotients $|u_{2n+2}/u_{2n+1}|$ increase with n, that is, they satisfy the inequality

$$\left|\frac{u_{2n+2}}{u_{2n+1}}\right|>\left|\frac{u_{2n}}{u_{2n-1}}\right|.$$

Equivalently, we may write

$$|\alpha|\left|\frac{1-\theta^{2n+2}}{1-\theta^{2n+1}}\right| > |\alpha|\left|\frac{1-\theta^{2n}}{1-\theta^{2n-1}}\right|.$$

Since $0<|\theta|<1$, it reduces to

$$\frac{1-\theta^{2n+2}}{1-\theta^{2n+1}} > \frac{1-\theta^{2n}}{1-\theta^{2n-1}}$$

giving us

$$1-\theta^{2n-1}-\theta^{2n+2}+\theta^{4n+1} > 1-\theta^{2n+1}-\theta^{2n}+\theta^{4n+1}.$$

Collecting the terms on the left hand side and dividing both sides of the inequality by $-\theta^{2n-1}>0$ we obtain

$$\theta^3-\theta^2-\theta+1=(\theta-1)^2(\theta+1)>0,$$

which is obviously true for any θ with $0<|\theta|<1$. Since $|u_2/u_1|=|A|\geq 1$, we have, in particular, that $|u_n/u_{n-1}|>1$ for all $n\geq 0$. This proves the lemma for all odd n and all $n>2n_0$ with $|u_{2n_0}/u_{2n_0-1}|>3$. Thus we need to show that $|u_8/u_7|>3$ under our hypotheses.

We distinguish between the cases where $B>0$ and $B<0$. Let us start with $B<0$. We have

$$|\theta|=\left|\frac{\beta}{\alpha}\right|=\frac{|A|-\sqrt{A^2+4B}}{|A|+\sqrt{A^2+4B}}\leq\frac{|A|-1}{|A|+1}=1-\frac{2}{|A|+1}.$$

Note that in this case we also have that $|\alpha|>\frac{|A|+1}{2}$. Write $x=\frac{|A|+1}{2}$. We show that

$$\left|\frac{u_8}{u_7}\right|\geq x\frac{1-\left(1-\frac{1}{x}\right)^8}{1+\left(1-\frac{1}{x}\right)^7}>3.$$

Solving this inequality for x shows that the second inequality holds unless $x<3.55$, i.e., $|A|<6.1$.

When $B>0$, we have

$$|\theta|=\left|\frac{\beta}{\alpha}\right|=\frac{\sqrt{A^2+4B}-|A|}{\sqrt{A^2+4B}+|A|}=1-\frac{2|A|}{\sqrt{A^2+4B}+|A|}$$

and with $|A|\geq 3$ we obtain

$$|\theta|\geq 1+\frac{6}{\sqrt{9+4B}+3}$$

and

$$|\alpha|>\frac{\sqrt{9+4B}+3}{2}=:y.$$

We need to show that

$$\left|\frac{u_8}{u_7}\right| \geq y\frac{1-\left(1-\dfrac{3}{y}\right)^8}{1+\left(1-\dfrac{3}{y}\right)^7} > 3.$$

The inequality holds unless $y \leq 3$. However, $y \leq 3$ is impossible, since it would imply $B \leq 0$ which we excluded.

Similar arguments for the cases $|A| = 2$ and $|A| = 1$ yield that $\left|\dfrac{u_8}{u_7}\right| > 3$ provided that $B > 9$ and $B > 3$, respectively. □

A similar argument for Lucas sequences of the second kind reveals the following.

Lemma 9. *Let $v = (v_n)_{n=0}^{\infty}$ be the Lucas sequence of the second kind corresponding to the pair (A, B), with $A^2 + 4B > 0$. Assume that $n > n'$. Then $|u_n/u_{n'}| > 3$ if n is even or $n \geq 7$, unless*

- *$B < 0$ and $|A| \leq 7$ or*
- *$|A| = 1$ and $0 < B \leq 14$ or*
- *$|A| = 2$ and $0 < B \leq 3$.*

Proof. Since the proof of this Lemma is similar to that of Lemma 8, we omit most of the details. Note that when $|A| = 1$ we have $|v_1/v_0| = 1/2 < 1$ and we can only deduce $|v_n/v_{n-1}| \geq 1$ provided that $n \geq 2$. Thus we shall ensure $|v_7| \geq 6$. Direct computation yields that indeed

$$|v_7| = 7B^3 + 14B^2 + 7B + 1$$

when $|A| = 1$. Since $|A| = 1$ implies that $B \geq 1$, we get $|v_7| > 6$. □

Now we apply Lemma 7 in combination with Lemma 8 and find that if u admits a three term arithmetic progression, then one of the equations in (3) must have a solution with even $m \leq 6$. Writing the terms of u as polynomials in A and B we have to deal with finitely many equations. We only present the main ideas through one example for each different type of possible equations, we treat the rest in a similar manner.

Case $m = 2$. Since $u_0 = 0$, $u_1 = 1$ and $u_2 = A$, we only get trivial equations like $A - 2 = 0$.

Case $m = 4$. The corresponding equations are linear in B. For example, the triple $(k, l, m) = (1, 2, 4)$ substituted into the second equation of (3) gives us

$$A^3 + 2AB + A - 2 = 0$$

implying

$$B = \frac{-A^3 - A + 2}{2A}.$$

Hence $A \mid 2$, i.e., $A = \pm 1, \pm 2$. However, we see that one of the conditions $AB \neq 0$ and $A^2 + 4B > 0$ fails in all cases. One can handle the other equations similarly.

Case $m = 6$**.** The corresponding equations are quadratic in B. Our general strategy is to push the discriminant of each equation between two squares and solve the parametric equation for each square between these lower and upper bounds. For example, the triple $(k, l, m) = (0, 3, 6)$ and the third equation of (3) gives

$$-6AB^2 + (-8A^3 + 1)B - 2A^5 + A^2 = 0.$$

The discriminant is $D = 16A^6 + 8A^3 + 1 = (4A^3 + 1)^2$. However, solving this for B we get the pair $(A, B) = (A, -A^2)$ and $A^2 + 4B > 0$ fails to hold.

Let us consider another example. For instance, take the triple $(k, l, m) = (0, 2, 6)$. Then we obtain $D = A^6 + 6A^2 - 3A$. But

$$A^6 < A^6 + 6A^2 - 3A < (|A|^3 + 1)^2$$

provided that $|A| > 3$ and we deduce that D is never a square if $|A| > 3$. For those with $|A| \leq 3$ and $A \neq 0$ we obtain that D is a square if and only if $A = 1$. In this case, $B = 0$ which contradicts our assumption.

The same approach for each triple gives the complete list of three term arithmetic progressions.

We are left with the finite number of sequences satisfying

- $B < 0$ and $|A| \leq 6$ or
- $|A| = 1$ and $0 < B \leq 9$ or
- $|A| = 2$ and $0 < B \leq 3$.

In these finitely many cases, we can use a growth argument to find all three term arithmetic progressions.

Let us demonstrate this by an example, say $A = 2$ and $B = 1$ and $(u_n)_{n=0}^{\infty}$ being a Lucas sequence of the first kind. One may handle all the other finitely many equations by a similar reasoning. First, note that in this specific case we have that $\alpha = 1 + \sqrt{2}$ and $\beta = 1 - \sqrt{2}$. Assume that $u_k < u_l < u_m$ is a three term arithmetic progression and consider the first equation of (3) which is equivalent to

$$\alpha^k + \alpha^m - 2\alpha^l = \beta^k + \beta^m - 2\beta^m.$$

Let us assume for the moment that $m > l + 1 > k + 1$. Then

$$|\alpha|^m - 2|\alpha|^{m-2} - |\alpha|^{m-3} < |\alpha^k + \alpha^m - 2\alpha^l| = |\beta^k + \beta^m - 2\beta^m| < 4|\beta|^k.$$

Plugging in the concrete values of α and β we immediately get

$$(1 + \sqrt{2})^{m-3} \left((1 + \sqrt{2})^3 - 2(1 + \sqrt{2}) - 1 \right) = (4 + 3\sqrt{2})(1 + \sqrt{2})^{m-3} < 4$$

which yields a contradiction unless $m < 3$. Now it is easy to find all three term arithmetic progressions in this case. Note that in the case of $l > m$ or $k > m$ we may draw similar conclusions.

Hence we can assume that $m = l + 1 > k + 1$. Then

$$|\alpha|^m - 2|\alpha|^{m-1} < |\alpha|^k + 4|\beta|^k$$

and inserting the concrete values of α and β we get

$$(1+\sqrt{2})^{m-2} < (1+\sqrt{2})^k + 4.$$

Assuming $k \leq m - 3$ yields

$$\sqrt{2}(1+\sqrt{2})^{m-3} < 4,$$

whence $m \leq 4$ and we easily find all three term arithmetic progressions listed in Table 1 for this case. Finally, we have to consider the case when $m = l + 1 = k + 2$. Here we get the inequality

$$\left|\alpha^m - 2\alpha^{m-1} - \alpha^{m-2}\right| < 4|\beta|^k$$

which yields

$$2(1+\sqrt{2})^{m-2} < 4,$$

that is, $m \leq 3$ and we find no additional three term arithmetic progressions. Similar arguments for different orderings of u_k, u_l, u_m reveal no further solutions. Thus the case $A = 2$ and $B = 1$ is completely solved.

3 The case $A^2 + 4B < 0$

Unfortunately, we found no effective method to resolve this case completely. The reason has its roots in the use of the theory of S-unit equations. Indeed, the indices k, l, m corresponding to a non-trivial arithmetic progression $u_k < u_l < u_m$ contained in a Lucas sequence $(u_n)_{n=0}^{\infty}$ of the first kind or a Lucas sequence $(v_n)_{n=0}^{\infty}$ of the second kind satisfy the Diophantine equation

$$\alpha^k + \alpha^m - 2\alpha^l = \pm\left(\beta^k + \beta^m - 2\beta^l\right), \tag{4}$$

where the ± sign depends on whether we consider Lucas sequences of the first or second kind. In view of Theorem 3, it is crucial to discuss the number of solutions to S-unit equation (4). In the real case (cf. Section 2), we resolved this S-unit equation by using the fact that $|\alpha| > |\beta|$ and that $\left|\frac{u_n}{u_{n-1}}\right| \simeq |\alpha|$ as $n \to \infty$. If $A^2 + 4B < 0$, then this is no longer true and we have to apply the deep theory of S-unit equations.

In order to determine an upper bound for the number of solutions we prove a series of Lemmas which culminate in a proof for Theorem 3.

Before we start with the first lemma, let us note that both α and β are algebraic integers. Moreover, due to Theorem 5, which was proved in the previous section, we may assume that

α and β are conjugate imaginary quadratic integers. Hence we can suppose that α and β are not units, otherwise α/β would be a root of unity. Thus we may suppose that $|B| \geq 2$. Write $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ and denote by σ the unique, nontrivial $\mathbb{Q}$-automorphism of K, i.e., $\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$. Since K is an imaginary quadratic field, we also have that $\sigma(\epsilon) = \epsilon^{-1}$, where ϵ is any unit in K.

For fixed α and β we denote by C_1 and C_2 the number of non-trivial three term arithmetic progressions of $(u_n)_{n=0}^{\infty}$ and $(v_n)_{n=0}^{\infty}$, respectively and write $C = \max\{C_1, C_2\}$. Actually, our upper bounds for C_1 and C_2 coincide in each instance and hence we use only the quantity C.

Let $\Gamma = \langle \alpha, \beta \rangle \leq \bar{\mathbb{Q}}^*$ be the multiplicative group generated by α and β. We denote by $A = A(a_0, \ldots, a_r)$ the number of non-degenerate, projective solutions $[x_0 : \cdots : x_r] \in \mathbb{P}^r(\Gamma)$ of the weighted, homogeneous S-unit equation

$$a_0 u_0 + \cdots + a_r u_r = 0. \tag{5}$$

with $a_0, \ldots, a_r \in \mathbb{C}$, in unknowns $u_0, \ldots, u_r \in \Gamma$. By a non-degenerate solution we mean a solution to equation (5) such that no subsum on the left hand side of equation (5) vanishes. Upper bounds $A(a_0, \ldots, a_r) \leq A(r, s)$, where s denotes the rank of Γ, have been found most prominently by Evertse, Schlickewei, and Schmidt [9] and Amoroso and Viada [2] in the most general case. In particular, we use the bounds due to Schlickewei and Schmidt [14] which in our case yield better results, although they depend on $d = [K : \mathbb{Q}]$ as well.

As we already noted above, three term arithmetic progressions in the Lucas sequences $(u_n)_{n=0}^{\infty}$ and $(v_n)_{n=0}^{\infty}$ yield solutions to (4). Thus we study the weighted S-unit equation

$$x_1 + x_2 - 2x_3 = \pm(y_1 + y_2 - 2y_3), \tag{6}$$

where $x_1, x_2, x_3, y_1, y_2, y_3 \in \Gamma = \langle \alpha, \beta \rangle$ and, in particular, where $x_1 = \alpha^k, x_2 = \alpha^m, x_3 = \alpha^l, y_1 = \beta^k, y_2 = \beta^m, y_3 = \beta^l$.

Before we start investigating S-unit equations of type (6) we state a theorem due to Beukers [3, Theorem 2] and draw some simple conclusions from it.

Lemma 10 (Beukers [3]). *Let the non-degenerate recurrence sequence of rational integers $(u_n)_{n=0}^{\infty}$ be given by $u_0 \geq 0$, $\gcd(u_0, u_1) = 1$, $u_n = Au_{n-1} - Bu_{n-2}$, with $A, B \in \mathbb{Z}$ and $A \geq 0$. Assume that $A^2 - 4B < 0$. If $u_m = \pm u_0$ has more than three solutions m, then one of the following cases holds:*

$$\begin{array}{lll} A = 1, B = 2, u_0 = u_1 = 1 & \textit{when} & m = 0, 1, 2, 4, 12; \\ A = 1, B = 2, u_0 = 1, u_1 = -1 & \textit{when} & m = 0, 1, 3, 11; \\ A = 3, B = 4, u_0 = u_1 = 1 & \textit{when} & m = 0, 1, 2, 6; \\ A = 2, B = 3, u_0 = u_1 = 1 & \textit{when} & m = 0, 1, 2, 5. \end{array}$$

From this Lemma we can easily conclude the following statement.

Lemma 11. *Let $(u_n)_{n=0}^\infty$ be a Lucas sequence of the first or second kind. Then for a fixed integer λ the equation $\lambda = u_m$ has at most 3 solutions m.*

Proof. Let m_0 be the smallest solution to $\lambda = u_m$. Consider instead of the original sequence the sequence $a_k = u_{m_0+k}/g(-1)^{k\delta}$, where $g = \operatorname{sgn}(u_{m_0}) \gcd(u_{m_0}, u_{m_0+1})$ and $\delta = \frac{1-\operatorname{sgn}(A)}{2}$ (see also the remarks following Theorem 2 in [3]). Therefore we conclude that an equation of the form $\lambda = |u_m|$ has more than three solutions if for the smallest solution m_0, also $m_0 + 1$ is a solution and $(A, B) = (\pm1, -2), (\pm3, -4)$ or $(\pm2, -3)$.

However, the equation $|u_{m_0}| = |u_{m_0+1}|$ is equivalent to the equation

$$\frac{\alpha \pm 1}{\beta \pm 1} = \left(\frac{\beta}{\alpha}\right)^{m_0}$$

in case that $(u_n)_{n=0}^\infty$ is a Lucas sequence of first kind and

$$\frac{\alpha \pm 1}{\beta \pm 1} = -\left(\frac{\beta}{\alpha}\right)^{m_0}$$

in case that $(u_n)_{n=0}^\infty$ is a Lucas sequence of second kind. For all pairs of (α, β) we solve these equations and find for instance, that $m_0 \leq 2$ (if a solution exists at all). By computing the values of all possible further solutions we find that indeed no equation of the form $\lambda = u_m$ has more than three solutions. □

Remark 12. Beukers [3, Corollary on page 267] already showed this result in case of Lucas sequences of the first kind. In fact, he proved more and listed all the cases when there can be three solutions. To the authors knowledge the case of Lucas sequences of the second kind has not been treated since then.

Let us start by investigating the number of non-degenerate solutions to the S-unit equation (4):

Lemma 13. *There are at most $A(5, 2)$ three term arithmetic progressions contained in a Lucas sequence $(u_n)_{n=0}^\infty$ of the first kind that yield non-degenerate solutions to (4).*

The same statement also holds for Lucas sequence $(v_n)_{n=0}^\infty$ of the second kind.

Proof. Consider the weighted S-unit equation

$$x_1 + x_2 - 2x_3 = y_1 + y_2 - 2y_3 \tag{7}$$

with unknowns $x_1, x_2, x_3, y_1, y_2, y_3 \in \Gamma$. This has at most $A(5, 2)$ non-degenerate, projective solutions. Thus there exists a set $\mathcal{C}$, with $|\mathcal{C}| \leq A(5, 2)$, of sextuples $(1, c_2, c_3, c_4, c_5, c_6)$ such that for any solution we have $x_2/x_1 = c_2$, $x_3/x_1 = c_3$, $y_1/x_1 = c_4$, $y_2/x_1 = c_5$ and $y_3/x_1 = c_6$. Assume now that a solution comes from an arithmetic progression $u_k < u_l < u_m$ in a Lucas sequence $(u_n)_{n=0}^\infty$ of the first kind. Then we have

$$\frac{\alpha^k}{\beta^k} = \frac{1}{c_4}, \quad \frac{\alpha^m}{\beta^m} = \frac{c_2}{c_5}, \quad \frac{\alpha^l}{\beta^l} = \frac{c_3}{c_6} \quad \text{or} \quad \frac{\beta^k}{\alpha^k} = \frac{1}{c_4}, \quad \frac{\beta^m}{\alpha^m} = \frac{c_2}{c_5}, \quad \frac{\beta^l}{\alpha^l} = \frac{c_3}{c_6} \tag{8}$$

for some $(1, c_2, c_3, c_4, c_5, c_6) \in \mathcal{C}$. Since by assumption α/β is not a root of unity, for every sextuple $(1, c_2, c_3, c_4, c_5, c_6) \in \mathcal{C}$, there exists at most one triple (k, l, m) such that any set of identities of (8) is satisfied, i.e., $u_k < u_l < u_m$ is an arithmetic progression. Hence there exist at most $A(5, 2)$ three term arithmetic progressions in a Lucas sequence of the first kind $(u_n)_{n=0}^{\infty}$, yielding a non-degenerate solution to (4).

In the case of a Lucas sequence of the second kind $(v_n)_{n=0}^{\infty}$, we consider instead of (7) the Diophantine equation

$$x_1 + x_2 - 2x_3 = -(y_1 + y_2 - 2y_3)$$

and derive the same conclusion as before. □

Before we start dealing with vanishing subsums in equation (4) we note that α and β are always multiplicatively independent. Otherwise, we would have $\alpha^t = \beta^s$ for some integers t, s. Taking the conjugates we get $\alpha^s = \beta^t$ and hence $(\alpha/\beta)^{t+s} = 1$ which we did not allow in the definition.

To deal with vanishing two-term subsums we use the following lemma.

Lemma 14. *For fixed non-zero complex numbers a, b and c either there exists at most one solution $x, y \in \mathbb{Z}$ to $a^x = cb^y$ or a and b are multiplicatively dependent.*

Proof. Assume that two distinct solutions x, y and x', y' exist. Then we have

$$\frac{a^x}{b^y} = c = \frac{a^{x'}}{b^{y'}},$$

hence

$$a^{x-x'} = b^{y-y'}.$$

Thus a and b are multiplicatively dependent, since by assumption at least one exponent does not vanish. □

In view of Lemma 13, we are left to deal with vanishing subsums, which may occur in equation (4). Of course, no one-term vanishing subsum exists. First, consider two term vanishing subsums.

Lemma 15. *There are at most $3A(3, 2) + 30$ three term arithmetic progressions in a Lucas sequence $(u_n)_{n=0}^{\infty}$ of the first kind or a Lucas sequence $(v_n)_{n=0}^{\infty}$ of the second kind that yield a solution to (4) such that a two term subsum vanishes.*

Proof. First, we consider the Lucas sequences $(u_n)_{n=0}^{\infty}$ of the first kind. In this case, there exist exactly 15 possible vanishing two-term subsums in equation (4). We can divide these 15 subsums into five classes, namely

Case I $x_1 = -x_2$, $y_1 = -y_2$,

Case II $x_1 = y_2$, $x_2 = y_1$,

Case III $x_1 = 2x_3$, $x_2 = 2x_3$, $y_1 = 2y_3$, $y_2 = 2y_3$,

Case IV $x_1 = -2y_3$, $x_2 = -2y_3$, $y_1 = -2x_3$, $y_2 = -2x_3$.

Case V $x_1 = y_1$, $x_2 = y_2$, $x_3 = y_3$,

For each one we pick an equation and discuss it in detail. Since one can treat the other equations in the same class by exactly the same arguments, we do not discuss them.

Case I: The equation $x_1 = -x_2$ implies that $\alpha^k = -\alpha^m$ and we get $\alpha^{k-m} = -1$. Thus α and hence β are roots of unity, which is excluded.

Case II: The equation $x_1 = y_2$ implies that $\alpha^k = \beta^m$, i.e., α and β are multiplicatively dependent, which cannot be the case.

Case III: The equation $x_1 = 2x_3$ implies that $\alpha^k = 2\alpha^l$, i.e., $\alpha^{k-l} = 2$. Thus $\alpha = \pm\sqrt{2}$ or $\alpha = 2$, both a contradiction to our assumption that α is imaginary quadratic.

Case IV: If $x_1 = -2y_3$ we get the equation $\alpha^k = -2\beta^l$ and an by an application of Lemma 14 there exists at most one pair (k,l) satisfying $\alpha^k = -2\beta^l$ or α and β are multiplicatively dependent. The latter is not possible. However, if the pair (k,l) is fixed then u_l and u_k and therefore also u_m is fixed. Due to Lemma 11 there are at most three possiblities for m, i.e., there are at most three ways to extend the pair (k,l) to a triple (k,l,m) such that $u_k < u_l < u_m$ is an arithmetic progression.

Case V: If $x_1 = y_1$, then we have $\alpha^k = \beta^k$ and therefore $(\alpha/\beta)^k = 1$. Hence α/β is a root of unity unless $k = 0$.

So far we have proved that one of the following statements holds:

- we obtain at most 12 additional solutions coming from Case IV,
- $klm = 0$.

Concerning the last case we assume that $k = 0$ first. We get the S-unit equation

$$x_2 - 2x_3 = y_2 - 2y_3. \tag{9}$$

By the same arguments as in the proof of Lemma 13 we obtain that there are at most $A(3,2)$ three term arithmetic progressions which come from non-degenerate solutions of (9). Further, we have two vanishing two term subsums falling into Case III, two falling into Case IV and two into Case V. Case III yields no additional solution. Case IV yields at most 3 additional solutions, hence in total at most six additional solutions. Finally, note that in Case V we can now exclude that l or m vanishes, otherwise we would obtain $k = l$ or $k = m$ and we get no additional solution. Thus $k = 0$ yields at most $A(3,2)+6$ additional solutions.

By the same arguments it is possible to treat the cases of $l = 0$ and $m = 0$. We omit the details. However, the case that $klm = 0$ yields at most $3A(3,2) + 18$ additional solutions. Therefore we have at most $3A(3,2) + 30$ solutions. □

Let us note that the proof of Lemma 15, in particular its last part, shows the following.

Lemma 16. *There are at most $A(3,2)+6$ three term arithmetic progressions $u_k < u_l < u_m$ in a Lucas sequence of the first or second kind such that $k=0$. The same statements hold, if we replace $k=0$ by $m=0$ or $l=0$, respectively.*

Since a vanishing four term or five term subsum implies a two term or one term vanishing subsum, respectively, we are left to consider vanishing three term subsums.

Lemma 17. *At least one of the following statements holds:*

- *There are at most $18A(2,2)+9$ three term arithmetic progressions in a Lucas sequence of the first or second kind that yield a solution to (4) such that a three term subsum vanishes,*
- *or α and β are quadratic irrational numbers and if $u_k < u_l < u_m$ is an arithmetic progression, then the companion polynomial of the Lucas sequence $(u_n)_{n=0}^{\infty}$ of the first kind divides $X^k - 2X^l + X^m$,*
- *or α and β are quadratic irrational numbers and if $v_k < v_l < v_m$ is an arithmetic progression, then the companion polynomial of the Lucas sequence $(v_n)_{n=0}^{\infty}$ of the second kind divides $X^k - 2X^l + X^m$.*

Proof. Let us consider the case of Lucas sequences of the first kind. Lucas sequences of the second kind can be treated by the same means.

There are 20 possible, different vanishing three term subsums of (4). These appear in pairs and we can differentiate three different types:

$$
\begin{array}{rrr}
I: & x_1+x_2-2x_3=0, & 0=y_1+y_2-2y_3,\\
II: & x_1+x_2=y_1, & -2x_3=y_2-2y_3,\\
II: & x_1+x_2=y_2, & -2x_3=y_1-2y_3,\\
III: & x_1+x_2=-2y_3, & -2x_3=y_1+y_2,\\
II: & x_1-2x_3=y_1, & x_2=y_2-2y_3,\\
III: & x_1-2x_3=y_2, & x_2=y_1-2y_3,\\
II: & x_1-2x_3=-2y_3, & x_2=y_1+y_2,\\
II: & x_1=y_1+y_2, & x_2-2x_3=-2y_3,\\
II: & x_1=y_1-2y_3, & x_2-2x_3=y_2,\\
III: & x_1=y_2-2y_3, & x_2-2x_3=y_1.
\end{array}
$$

Let us take the equations of type II first. Pick the first pair of equations in the list above (the other cases run completely analogously). Consider the left hand side equation

$$x_1+x_2=y_1. \tag{10}$$

By the theory of S-unit equations there are at most $A(2,2)$ pairs (c_1, c_2) such that $x_1/y_1 = (\alpha/\beta)^k = c_1$ and $x_2/y_1 = \alpha^m/\beta^k = c_2$. These two relations determine the pair (k,m) uniquely. Hence there are at most $A(2,2)$ pairs (k,m) that fulfill the equation. With the pair (k,m) fixed, the value of u_l is fixed as well and by Lemma 11 there are at most three ways to extend the pair (k,l) to a triple (k,l,m) such that $u_k < u_l < u_m$ is an arithmetic progression. We deduce that there exist at most $3A(2,2)$ triples (k,l,m) satisfying a pair of equations of type II.

Consider now equations of type I. Rewriting the two equations we get $\alpha^k + \alpha^m - 2\alpha^l = 0 = \beta^k + \beta^m - 2\beta^l$. Thus in this case, the minimal polynomial of α and β, which is also the companion polynomial of the sequence, divides $X^k - 2X^l + X^m$.

Finally, we turn to equations of type III and consider the first equation of this type in detail. We can handle the others similarly. Assume for the moment that there exists a prime ideal $\mathfrak{p}$ with $\mathfrak{p} \nmid (2)$ and $v_{\mathfrak{p}}(\alpha) > 0$. Let $\mathfrak{p}_2$ be a prime ideal lying above (2) and suppose that $m > k$. We consider the equation $x_1 + x_2 = -2y_3$ from a $\mathfrak{p}$-adic point of view. Write $v_{\mathfrak{p}}(\alpha) = \xi_{\mathfrak{p}}$ and $v_{\mathfrak{p}}(\beta) = \eta_{\mathfrak{p}}$. Since the two smallest $\mathfrak{p}$-adic valuations of the summands have to coincide, we have $v_{\mathfrak{p}}(x_2) = k\xi_{\mathfrak{p}} = l\eta_{\mathfrak{p}} = v_{\mathfrak{p}}(2y_3)$. Considering $\mathfrak{p}_2$-adic valuations we obtain $k\xi_{\mathfrak{p}_2} = l\eta_{\mathfrak{p}_2} + \delta$, where $\delta = 1, 2$ depending on whether (2) is ramified or not. We get the following system of linear equations

$$\begin{aligned} k\xi_{\mathfrak{p}_2} - l\eta_{\mathfrak{p}_2} &= \delta \\ k\xi_{\mathfrak{p}} - l\eta_{\mathfrak{p}} &= 0 \end{aligned}$$

which has either no solution or at most one solution. Note that by assumption $\xi_{\mathfrak{p}} > 0$. Thus in this case, equations of type III yield at most one pair (k,l) that extends to a triple (k,l,m) such that $u_k < u_l < u_m$ is an arithmetic progressions. Hence by Lemma 11 we have at most three additional three term arithmetic progression.

If $v_{\mathfrak{p}}(\alpha) = 0$, but $v_{\mathfrak{p}}(\beta) > 0$, then we take the equation $-2x_3 = y_1 + y_2$ instead and draw the same conclusions.

In view of the paragraph above, we may assume that the only prime ideals dividing (α) and (β) are lying above (2). We distinguish now whether (2) splits, ramifies or is inert above K.

We start with the case when (2) is inert, i.e., (2) is a prime in K. Then $(\alpha) = (2)^x$ and $(\beta) = (2)^y$ with some non-negative integers x, y. Since α and β are conjugate, we get $x = y$. Hence α/β is a unit. However, recalling that α, β are from a quadratic imaginary field, this yields that α/β is a root of unity, which is a contradiction.

One may prove the case where (2) ramifies by similar means as the inert case. In this case,we have $(2) = \mathfrak{p}^2$ with some prime ideal $\mathfrak{p}$. Note that $\mathfrak{p}$ need not be principal although $\mathfrak{p}^2$ is principal. Thus $(\alpha) = \mathfrak{p}^x$ and $(\beta) = \mathfrak{p}^y$ with some non-negative integers x, y. Taking norm, we get $x = y$, and similarly as above we obtain that α/β is a root of unity, which is impossible.

Finally, let us consider the case when (2) splits, that is, we can write $(2) = \mathfrak{p}_1\mathfrak{p}_2$. Assume that $(\alpha) = \mathfrak{p}_1^{\xi}\mathfrak{p}_2^{\eta}$, then $(\beta) = \mathfrak{p}_1^{\eta}\mathfrak{p}_2^{\xi}$. Considering the equation $x_1 + x_2 = -2y_3$ from a $\mathfrak{p}_1$-adic and a $\mathfrak{p}_2$-adic viewpoint, respectively we get the following system of linear equations under the assumption that $m > k$:

$$\begin{aligned} v_{\mathfrak{p}_1}(x_2) &= k\xi = l\eta + 1 = v_{\mathfrak{p}_1}(2y_3), \\ v_{\mathfrak{p}_2}(x_2) &= k\eta = l\xi + 1 = v_{\mathfrak{p}_2}(2y_3). \end{aligned} \tag{11}$$

Note that we obtained this system due to the fact that the smallest $\mathfrak{p}$-adic valuations must coincide. Solving the linear system (11) yields $k(\xi^2 - \eta^2) = (\xi - \eta)$. Therefore either $\xi = \eta$ or $k(\xi + \eta) = 1$. The first case yields $\alpha = 2^{\xi}\epsilon$ and $\beta = 2^{\xi}\epsilon^{-1}$ for some unit ϵ which yields that $\alpha/\beta = \epsilon^2$ is a root of unity, a contradiction. When $k(\xi + \eta) = 1$ we have $k = 1$ and $(\xi, \eta) = (0, 1), (1, 0)$. In any case, we obtain from the linear system (11) that $l = -1$, a contradiction to our assumption that k, l, m are nonnegative integers. □

So we are left with the problem which quadratic polynomials divide $X^k - 2X^l + X^m$. In particular, we may assume that the companion polynomial is irreducible, otherwise α and β would be rational integers which case is covered by Theorem 5. We need to find all quadratic factors of polynomials of the type:

- $X^a - 2X^b + 1$ or
- $X^a + X^b - 2$ or
- $2X^a - X^b - 1$.

Since all zeros of the first polynomial are units, and all the zeros of the third polynomial are either non-integral algebraic numbers or units, it is enough to study polynomials of the form $X^a + X^b - 2$ only.

We state the following result due to Pintér and Ziegler [13, Lemma 3].

Lemma 18. *Let $a > b > 0 \in \mathbb{Z}$ and let $f(X) = X^a + X^b - 2$ be a polynomial. Then $f(X) = h(X)g(X)$ factors into the monic polynomials $h(X)$ and $g(X)$ over $\mathbb{Z}$, where the only zeros of $h(X)$ are roots of unity and $g(X)$ is irreducible. Further, $h(X) | X^{\gcd(a,b)} \pm 1$.*

We are interested in finding the quadratic factors of $X^a + X^b - 2$. By Lemma 18 we only have to consider the cases $(a, b) = (3, 2), (3, 1), (2, 1)$ or $(4, 2)$. Thus the companion polynomial is either $X^2 + 2X + 2$ or $X^2 + X + 2$ or $X^2 + 2$.

Since $X^2 + X + 2$ is the only polynomial with negative discriminant which is also a companion polynomial of a non-degenerate binary recurrence, we obtain that either $(A, B) = (-1, -2)$ or there are at most $A(5, 2)$ three term arithmetic progressions coming from non-degenerate solutions to (4) (cf. Lemma 13), $3A(3, 2) + 30$ three term arithmetic progressions coming form two term vanishing subsums of (4) (cf. Lemma 15) and $18A(2, 2) + 9$ three term arithmetic progressions coming form three term vanishing subsums of (4) (cf. Lemma 17). We summarize these results.

Proposition 19. *Let $u = (u_n)_{n=0}^{\infty}$ and $v = (v_n)_{n=0}^{\infty}$ be Lucas sequences of the first and second kind corresponding to the pair (A, B) with $A^2 + 4B < 0$. Then u and v admit at most*

$$C = A(5,2) + 3A(3,2) + 18A(2,2) + 39$$

three term arithmetic progressions unless u or v correspond to $(A, B) = (-1, -2)$ respectively. In case of $(A, B) = (-1, -2)$, the recurrences u and v admit infinitely many three term arithmetic progressions.

Remark 20. Since $X^2 + X + 2 | X^3 + X - 2$, we get that $u_k < u_l < u_m$ and $v_k < v_l < v_m$ with $(k, l, m) = (t + 1, t, t + 3)$ yield infinite families of three term arithmetic progressions in u and v, respectively.

Theorem 3 is now an easy Corollary of Proposition 19. Indeed, due to a result of Schlickewei and Schmidt [14], we know that $A(k, s) \leq 2^{35B^3} d^{6B^2}$, where $B = \max\{k + 1, s\}$ and $d = [K : \mathbb{Q}]$, hence

$$C \leq A(5,2) + 3A(3,2) + 18A(2,2) + 39 < 6.45 \cdot 10^{2340}.$$

4 Acknowledgment

The authors are grateful to the referee for her/his useful comments and suggestions.

References

[1] J. Aguirre, A. Dujella, and J. C. Peral, Arithmetic progressions and Pellian equations, *Publ. Math. Debrecen* **83** (2013), 683–695.

[2] F. Amoroso and E. Viada, Small points on subvarieties of a torus, *Duke Math. J.* **150** (2009), 407–442.

[3] F. Beukers, The multiplicity of binary recurrences, *Compos. Math.* **40** (1980), 251–267.

[4] A. Bremner, On arithmetic progressions on elliptic curves, *Exp. Math.* **8** (1999), 409–413.

[5] G. Campbell, A note on arithmetic progressions on elliptic curves, *J. Integer Seq.* **6** (2003), Article 03.1.3.

[6] A. A. Ciss and D. Moody, Arithmetic progressions on conics, *J. Integer Seq.* **20** (2017), Article 17.2.8.

[7] A. Dujella, A. Pethő, and P. Tadić, On arithmetic progressions on Pellian equations, *Acta Math. Hungar.* **120** (2008), 29–38.

[8] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence Sequences*, Vol. 104 of *Mathematical Surveys and Monographs*, American Mathematical Society, 2003.

[9] 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.

[10] E. González-Jiménez, Covering techniques and rational points on some genus 5 curves, in *Trends in Number Theory*, Vol. 649 of *Contemp. Math.*, Amer. Math. Soc., 2015, pp. 89–105.

[11] A. J. MacLeod, 14-term arithmetic progressions on quartic elliptic curves, *J. Integer Seq.* **9** (2006), Article 06.1.2.

[12] A. Pethő and V. Ziegler, Arithmetic progressions on Pell equations, *J. Number Theory* **128** (2008), 1389–1409.

[13] Á. Pintér and V. Ziegler, On arithmetic progressions in recurrences - a new characterization of the Fibonacci sequence, *J. Number Theory* **132** (2012), 1686–1706.

[14] H. P. Schlickewei and W. M. Schmidt, The number of solutions of polynomial-exponential equations, *Compos. Math.* **120** (2000), 193–225.

2010 *Mathematics Subject Classification*: Primary 11B39. Secondary 11B25, 11D61.
Keywords: Lucas sequence, arithmetic progression, S-unit equation.

(Concerned with sequences A000032, A000045, A001045, A014551, and A039834.)

Received March 20 2017; revised versions received August 7 2017; August 11 2017. Published in *Journal of Integer Sequences*, September 3 2017.

Return to Journal of Integer Sequences home page.