Fuchs et al. *Res. Number Theory*
https://doi.org/10.1007/s40993-018-0121-2

Research in Number Theory

RESEARCH

Diophantine triples in linear recurrences of Pisot type

Clemens Fuchs[1*], Christoph Hutle[1] and Florian Luca[2,3,4]

*Correspondence: clemens.fuchs@sbg.ac.at
[1] University of Salzburg, Hellbrunner Str. 34/I, 5020 Salzburg, Austria
Full list of author information is available at the end of the article

Abstract

The study of Diophantine triples taking values in linear recurrence sequences is a variant of a problem going back to Diophantus of Alexandria which has been studied quite a lot in the past. The main questions are, as usual, about existence or finiteness of Diophantine triples in such sequences. Whilst the case of binary recurrence sequences is almost completely solved, not much was known about recurrence sequences of larger order, except for very specialised generalisations of the Fibonacci sequence. Now, we will prove that any linear recurrence sequence with the Pisot property contains only finitely many Diophantine triples, whenever the order is large and a few more not very restrictive conditions are met.

Keywords: Diophantine triples, Linear recurrence sequences, Diophantine equations, Application of the Subspace theorem

Mathematics Subject Classification: Primary 11D72, 11B39; Secondary 11J87

1 Introduction

The problem of Diophantus of Alexandria about tuples of integers $\{a_1, a_2, a_3, \ldots, a_m\}$ such that the product of each distinct two of them plus 1 always results in an integer square has already quite a long history (see [8]). It is easy to see that there are infinitely many such sets with $m = 2$ since $\{a, b\} = \{r - 1, r + 1\}$ is a Diophantine pair for every $r \geq 2$. One of the main questions was, how many such Diophantine m-tuples exist for a fixed $m \geq 3$. Already Euler proved that there are infinitely many Diophantine quadruples, demonstrating it with the family

$$\{a, b, a + b + 2\sqrt{ab + 1}, 4(a + \sqrt{ab + 1})(b + \sqrt{ab + 1})\sqrt{ab + 1}\}$$

for a and b such that $ab+1$ is a perfect square. For $\{a, b\} = \{r-1, r+1\}$ Euler's extension reduces to $\{a, b, c, d\} = \{r-1, r+1, 4r, 16r^3 - 4r\}$. Much later Arkin, Hoggatt and Strauss [5] proved that every Diophantine triple can be extended to a Diophantine quadruple. More precisely, let $\{a, b, c\}$ be a Diophantine triple and

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2,$$

where r, s, t are positive integers. Define

$$d_+ := a + b + c + 2abc + 2rst.$$

Then $\{a, b, c, d_+\}$ is a Diophantine quadruple. Dujella proved in [9], that there are no Diophantine sextuples and also that there are only finitely many Diophantine quintuples.

This result is even effective, since an upper bound of the form $\log_{10}(\log_{10}(\max\{a_i\})) < 26$ was given on the members of such a quintuple. It is conjectured, that there are no quintuples at all and, even stronger, that if $\{a, b, c, d\}$ is a Diophantine quadruple and $d > \max\{a, b, c\}$, then $d = d_+$. The "weaker" conjecture has recently been settled by He, Togbé and Ziegler (cf. [19]), whereas the stronger conjecture still remains open.

Now it is an interesting variation of the original problem of Diophantus to consider a linear recurrence sequence instead of the sequence of squares. So we ask for bounds m on the size of tuples of integers $\{a_1, a_2, a_3, \ldots, a_m\}$ with $a_ia_j + 1$ being members of a given linear recurrence for $1 \leq i < j \leq m$. We shall call this set a *Diophantine m-tuple with values in the linear recurrence* (or a Diophantine m-tuple in the recurrences, for short). Here, the first result was due to Fuchs, Luca and Szalay, who proved in [12] that for a binary linear recurrence sequence $(u_n)_{n\geq 0}$, there are only finitely many Diophantine triples, if certain conditions are met. The Fibonacci sequence and the Lucas sequence both satisfy these conditions and all Diophantine triples with values in these sequences were computed in [22] and [23]. Further results in this direction can be found in [2,20] and [21]. Moreover, in [1] it is shown that there are no balancing Diophantine triples; see also [3] for a related result. In [4] it is shown that there are no Diophantine triples taking values in Pellans sequence.

The first result on linear recurrence sequences of higher order than 2 came up in 2015, when the authors jointly with Irmak and Szalay proved (see [13]) that there are only finitely many Diophantine triples with values in the Tribonacci sequence $(T_n)_{n\geq 0}$ given by

$$T_0 = T_1 = 0, \quad T_2 = 1, \quad T_{n+3} = T_{n+2} + T_{n+1} + T_n \quad \text{for } n \geq 0.$$

In [17] it was shown that a Tribonacci Diophantine quadruple does not exist. A related result can be found in [18]. One year later in [14], this result was generalized to k-generalized Fibonacci sequences: For any integer $k \geq 3$, define $(F_n^{(k)})_{n\geq 0}$ by $F_0^{(k)} = \ldots = F_{k-2}^{(k)} = 0, F_{k-1}^{(k)} = 1$ and

$$F_{n+k}^{(k)} = F_{n+k-1}^{(k)} + \cdots + F_n^{(k)} \quad \text{for } n \geq 0.$$

Then for any fixed k, only finitely many Diophantine triples with values in $\{F_n^{(k)}; n \geq 0\}$ exist. None of these results are constructive, since the proof uses a version of the Subspace theorem. It is not clear, whether there are any Diophantine triples with values in those sequences at all.

The result in this paper deals with a significantly larger class of linear recurrence sequences:

Let $(F_n)_{n\geq 0}$ be a sequence of integers satisfying a linear recurring relation. Assume that the recurrence is of *Pisot type*, i.e., that its characteristic polynomial is the minimal polynomial (over $\mathbb{Q}$) of a Pisot number. We denote the power sum representation (Binet formula) by $F_n = f_1\alpha_1^n + \cdots + f_k\alpha_k^n$. Assume w.l.o.g. that $\alpha = \alpha_1$ is the Pisot number; i.e., α is a real algebraic integer of degree k satisfying $\alpha > 1$ and if $\alpha_2, \ldots, \alpha_k$ denote the conjugates of α over $\mathbb{Q}$ then $\max\{|\alpha_2|, \ldots, |\alpha_k|\} < 1$. We remark that by a result of Mignotte (cf. [24]) it immediately follows that the sequence is non-degenerate, and that the characteristic roots are all simple and irrational.

We show that there are only finitely many triples of integers $1 \leq a < b < c$ such that

$$1 + ab = F_x, \quad 1 + ac = F_y, \quad 1 + bc = F_z$$

if at least one of the following conditions holds:

- Neither the leading coefficient f_1 nor $f_1\alpha$ is a square in $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$.
- $k \geq 2$ and α is not a unit.
- $k \geq 4$.

The previously treated k-generalized Fibonacci sequences satisfy this Pisot property and neither their leading coefficient f_1 nor $f_1\alpha_1$ is a square. However, the new result in this paper helps us to obtain finiteness for many more linear recurrence sequences.

For example, let us consider the irreducible polynomial $X^3 - X - 1$, which has the Pisot property. Its Pisot root $\theta := 1.3247179572\ldots$ is the smallest existing Pisot number by [6]. This number is also known as the *plastic constant*. Its corresponding linear recurrence sequence $(F_n)_{n\geq 0}$, given by $F_{n+3} = F_{n+1} + F_n$, is of Pisot type. If the initial values are not $F_0 = 6, F_1 = -9, F_2 = 2$, then neither the leading coefficient nor the leading coefficient times θ are squares in the splitting field of $X^3 - X - 1$ over $\mathbb{Q}$. So the theorem can be applied and we obtain, that there are only finitely many Diophantine triples with values in this sequence. However it is yet not clear, what happens in the case $F_0 = 6, F_1 = -9, F_2 = 2$.

Another example for which the theorem can be applied is the polynomial

$$X^{2k+1} - \frac{X^{2k} - 1}{X - 1}.$$

This polynomial defines a Pisot number of degree $2k + 1$ by a result of Siegel (see [25]) and its corresponding linear recurrence sequence is of Pisot type. Independently of its initial values, the result applies to all $k \geq 2$ since the degree is sufficiently large. The same applies to

$$X^{2k+1} - \frac{X^{2k+2} - 1}{X^2 - 1},$$

for $k \geq 2$.

Furthermore, all polynomials of the form

$$X^k(X^2 - X - 1) + X^2 + 1$$

are known to define Pisot numbers. So, again for $k \geq 2$ the theorem applies.

We quickly discuss the main shape of the recurrences we study in this paper. Let $(F_n)_{n\geq 0}$ be a recurrence of Pisot type as described above. Let us denote $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$. Since $F_n \in \mathbb{Z}$ it follows that each element of the Galois group of K over $\mathbb{Q}$ permutes the summands in the power sum representation of F_n. Moreover, each summand is a conjugate of the leading term $f_1\alpha_1^n$ over $\mathbb{Q}$ and each conjugate of it appears exactly once in the Binet formula. Therefore F_n is just the trace $\mathrm{Tr}_{K/\mathbb{Q}}(f_1\alpha_1^n)$. Since f_1 might not be integral, we write $f_1 = f/d$ with $d \in \mathbb{Z}$ and f being an integral element in K. Thus, conversely starting with a Pisot number α, an integer $d \in \mathbb{Z}$ and an integral element f in the Galois closure K of α over $\mathbb{Q}$ such that $dF_n = \mathrm{Tr}_{K/\mathbb{Q}}(f\alpha^n)$ for every $n \in \mathbb{N}$, we can easily construct further examples for which our result applies.

The proof will be given in several steps: First, a more abstract theorem is going to be proved, which guarantees the existence of an algebraic equality, that needs to be satisfied, if there were infinitely many Diophantine triples. This works on utilizing the Subspace theorem (cf. [10]) and a parametrization strategy in a similar manner to that of [14]. If the leading coefficient is not a square in $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$, we obtain the contradiction quite immediately from this equality. In a second step, we will use divisibility arguments and algebraic parity considerations in order to show that this equality can also not be satisfied if the order k is large enough. Let us now state the results.

2 The results

We start with a general and more abstract statement which gives necessary conditions in case infinitely many Diophantine triples exist. It is derived by using the Subspace theorem (cf. [10]).

Theorem 1 *Let $(F_n)_{n\geq 0}$ be a sequence of integers satisfying a linear recurrence relation of Pisot type of order $k \geq 2$. Denote its power sum representation as*

$$F_n = f_1\alpha_1^n + \cdots + f_k\alpha_k^n.$$

If there are infinitely many positive integers $1 < a < b < c$, such that

$$ab + 1 = F_x, \qquad ac + 1 = F_y, \qquad bc + 1 = F_z \tag{1}$$

hold for integers x, y, z, then one can find fixed integers $(r_1, r_2, r_3, s_1, s_2, s_3)$ with r_1, r_2, r_3 positive, $\gcd(r_1, r_2, r_3) = 1$ such that infinitely many of the solutions (a, b, c, x, y, z) can be parametrized as

$$x = r_1\ell + s_1, \quad y = r_2\ell + s_2, \quad z = r_3\ell + s_3.$$

Furthermore, following the parametrization of x, y, z in ℓ, there must exist a power sum $c(\ell)$ of the form

$$c(\ell) = \alpha_1^{(-r_1+r_2+r_3)\ell+\eta}\left(e_0 + \sum_{j\in J_c} e_j \prod_{i=1}^{k} \alpha_i^{v_{ij}\ell}\right)$$

with $\eta \in \mathbb{Z} \cup (\mathbb{Z} + 1/2)$, J_c an index set, e_j being coefficients in $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ and integers v_{ij} with the property that $v_{ij} \geq 0$ if $i \in \{2, \ldots, n\}$ and $v_{ij} < 0$ if $i = 1$, all independent of ℓ, such that

$$(F_x - 1)c(\ell)^2 = (F_y - 1)(F_z - 1).$$

Similarly there are $a(\ell)$ and $b(\ell)$ of the same shape with

$$(F_z - 1)a(\ell)^2 = (F_x - 1)(F_y - 1) \quad \text{and} \quad (F_y - 1)b(\ell)^2 = (F_x - 1)(F_z - 1).$$

The proof is given in Sect. 4.

This theorem looks quite abstract. However, it can be applied to a huge family of linear recurrences. Firstly, it can be applied to all linear recurrences, in which the leading coefficient is not a square:

Theorem 2 *Let $(F_n)_{n\geq 0}$ be a sequence of integers satisfying a linear recurring relation $F_{n+k} = A_1\, F_{n+k-1} + A_2\, F_{n+k-2} + \cdots + A_k\, F_n$ of Pisot type of order $k \geq 2$, that is, the characteristic polynomial*

$$X^k - A_1\, X^{k-1} - A_2\, X^{k-2} - \cdots - A_k = (X - \alpha_1)\,(X - \alpha_2)\,\cdots\,(X - \alpha_k)$$

is an irreducible polynomial of degree k, has integer coefficients A_i, and has roots satisfying $\alpha_1 > 1$ and $\max\{|\alpha_2|, \ldots, |\alpha_k|\} < 1$. If furthermore neither f_1 nor $f_1\alpha_1$ are squares in $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$, then there are only finitely many Diophantine triples with values in $\{F_n; n \geq 0\}$.

The proof of this theorem is given in Sect. 5.

Another consequence of Theorem 1 applies to linear recurrences of sufficiently large order. Namely if $k \geq 4$, the existence of such a $c(\ell)$ leads to a contradiction. The same holds already for $k = 2, 3$, if we assume that the Pisot element α_1 is not a unit in the ring of integers of $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$. Thus, we obtain the following result.

Theorem 3 *Let $(F_n)_{n\geq 0}$ be a sequence of integers satisfying a linear recurring relation $F_{n+k} = A_1 F_{n+k-1} + A_2 F_{n+k-2} + \cdots + A_k F_n$ of Pisot type of order $k \geq 2$, that is, the characteristic polynomial*

$$X^k - A_1 X^{k-1} - A_2 X^{k-2} - \cdots - A_k = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k)$$

is an irreducible polynomial of degree k, has integer coefficients A_i, and has roots satisfying $\alpha_1 > 1$ and $\max\{|\alpha_2|, \ldots, |\alpha_k|\} < 1$. Then there are only finitely many Diophantine triples $1 < a < b < c$ with

$$ab + 1 = F_x, \quad ac + 1 = F_y, \quad bc + 1 = F_z,$$

with values in $\{F_n; n \geq 0\}$ if one of the following conditions holds:

(i) *$k \geq 2$ and α_1 is not a unit.*
(ii) *$k \geq 4$.*

This theorem is proved in Sect. 6.

Before we give the proofs we first start with several useful lemmas that will be used in the sections afterwards.

3 Some useful lemmas

Assume that we have infinitely many solutions $(x, y, z) \in \mathbb{N}^3$ to (1) with $1 < a < b < c$. Obviously, we have $x < y < z$. First, one notices that not only for z, but for all three components, we necessarily have arbitrarily "large" solutions.

Lemma 1 *Let us assume, we have infinitely many solutions $(x, y, z) \in \mathbb{N}^3$ to (1). Then for each N, there are still infinitely many solutions $(x, y, z) \in \mathbb{N}^3$ with $x > N$.*

Proof It is obvious that we must have arbitrarily large solutions for y and for z, since otherwise, a, b, c would all be bounded as well, which is an immediate contradiction to our assumption.

If we had infinitely many solutions (x, y, z) with $x < N$, then there is at least one fixed x which forms a solution with infinitely many pairs (y, z). Since $F_x = ab + 1$, we have a bound on these two variables as well and can use the same pigeon hole argument again to find fixed a and b, forming a Diophantine triple with infinitely many $c \in \mathbb{N}$.

Using these fixed a, b, we obtain from the other two equations in (1), that $bF_y - aF_z = b - a$ and therefore, the expressions $bf_1\alpha_1^y$ and $af_1\alpha_1^z$ (having the largest growth rate) must be equal. So

$$\alpha_1^{z-y} = \frac{b}{a},$$

which is a constant. Hence, $z - y$ must be some constant $\rho > 0$ as well and we can write $z = y + \rho$ for our infinitely many solutions in y and z.

Using the power sum representations in $bF_y - aF_{y+\rho} = b - a$, we get

$$b\left(f_1\alpha_1^y + \cdots + f_k\alpha_k^y\right) - a\left(f_1\alpha_1^{y+\rho} + \cdots + f_k\alpha_k^{y+\rho}\right) = b - a. \tag{2}$$

So the terms with the largest growth rate, which are $bf_1\alpha_1^y$ and $af_1\alpha_1^{y+\rho}$, must be equal and this gives us $b = a\alpha_1^\rho$. Inserting this into (2) and cancelling on both sides gives us

$$\alpha_1^\rho\left(f_2\alpha_2^y + \cdots + f_k\alpha_k^y\right) - \left(f_2\alpha_2^{y+\rho} + \cdots + f_k\alpha_k^{y+\rho}\right) = \alpha_1^\rho - 1.$$

Now for $y \to \infty$, the left hand side converges to 0. The right hand side is a constant larger than 0. So this equality can not be true when y is large enough. This contradiction completes the proof. □

Next, we prove the following result, which generalizes Proposition 1 in [13]. Observe that the upper bound depends now on k.

Lemma 2 *Let $y < z$ be sufficiently large. Then there is a constant C_1 such that*

$$\gcd(F_y - 1, F_z - 1) < C_1\alpha_1^{\frac{k}{k+1}z}. \tag{3}$$

Proof Denote $g := \gcd(F_y - 1, F_z - 1)$. Observe here and below that the numbers $F_x - 1, F_y - 1, F_z - 1$ are positive integers. Furthermore, let us assume that y (and hence z) is large enough such that

$$\max\left\{\left|f_2\alpha_2^y + \cdots + f_k\alpha_k^y\right|, \left|f_2\alpha_2^z + \cdots + f_k\alpha_k^z\right|\right\} < 1/2.$$

Let κ be a constant to be determined later. If $y \le \kappa z$, then

$$g \le F_y - 1 < |f_1|\alpha_1^y \le |f_1|\alpha_1^{\kappa z}. \tag{4}$$

Now let us assume that $y > \kappa z$. We denote $\lambda := z - y < (1-\kappa)z$. Note that

$$g \mid (F_z - 1) - \alpha_1^\lambda(F_y - 1) \qquad \text{in} \qquad \mathbb{Q}(\alpha_1).$$

Thus, we can write

$$g\pi = (F_z - 1) - \alpha_1^\lambda(F_y - 1),$$

where π is some algebraic integer in $\mathbb{Q}(\alpha_1)$. Note that the right-hand side above is not zero, for if it were, we would get $\alpha_1^\lambda = (F_z - 1)/(F_y - 1) \in \mathbb{Q}$, which is false for $\lambda > 0$. We compute norms from $\mathbb{Q}(\alpha_1)$ to $\mathbb{Q}$. Observe that

$$\begin{aligned}
&\left|(F_z - 1) - \alpha_1^\lambda(F_y - 1)\right| \\
&\quad = \left|\left(f_1\alpha_1^z + \cdots + f_k\alpha_k^z - 1\right) - \alpha_1^\lambda\left(f_1\alpha_1^y + \cdots + f_k\alpha_k^y - 1\right)\right| \\
&\quad = \left|\alpha_1^\lambda\left(1 - f_2\alpha_2^y - \cdots - f_k\alpha_k^y\right) - \left(1 - f_2\alpha_2^z - \cdots - f_k\alpha_k^z\right)\right| \\
&\quad \le \frac{3}{2}\alpha_1^\lambda - \frac{1}{2} < \frac{3}{2}\alpha_1^\lambda < \frac{3}{2}\alpha_1^{(1-\kappa)z}.
\end{aligned}$$

Further, let σ_i be any Galois automorphism that maps α_1 to α_i. Then for $i \geq 2$, we have

$$\begin{aligned}\left|\sigma_i\left((F_z-1)-\alpha_1^{\lambda}(F_y-1)\right)\right| &= \left|(F_z-1)-\alpha_i^{\lambda}(F_y-1)\right|\\ &< F_z-1+F_y-1 < |f_1|\alpha_1^z+|f_1|\alpha_1^y-1\\ &< |f_1|\left(1+\alpha_1^{-1}\right)\alpha_1^z \leq C_2\alpha_1^z,\end{aligned}$$

with C_2 being a suitable constant (e.g. $C_2=|f_1|\left(1+\alpha_1^{-1}\right)$).

Altogether, we obtain

$$\begin{aligned}g^k &\leq |N_{\mathbb{Q}(\alpha_1)/\mathbb{Q}}(g\pi)|\\ &\leq \left|N_{\mathbb{Q}(\alpha_1)/\mathbb{Q}}\left((F_z-1)-\alpha_1^{\lambda}(F_y-1)\right)\right|\\ &= \left|\prod_{i=1}^{k}\sigma_i\left((F_z-1)-\alpha_1^{\lambda}(F_y-1)\right)\right|\\ &< \frac{3}{2}\alpha_1^{(1-\kappa)z}(C_2\alpha_1^z)^{k-1} = C_3\alpha_1^{(k-\kappa)z},\end{aligned}$$

where $C_3 = 3C_2^{k-1}/2$. Hence,

$$g \leq C_4\alpha_1^{(1-\kappa/k)z} \tag{5}$$

with $C_4 = C_3^{1/k}$. In order to balance between (4) and (5), we choose κ such that $\kappa = 1-\kappa/k$, giving $\kappa = k/(k+1)$ and

$$g \leq \max\{|f_1|, C_4\}\alpha_1^{\frac{k}{k+1}z} = C_1\alpha_1^{\frac{k}{k+1}z},$$

where $C_1 = \max\{|f_1|, C_4\}$, which proves the lemma. □

The next lemma states the irreducibility (over $\mathbb{C}$) of a certain polynomial. This lemma will be used in the proof of Theorem 3.

Lemma 3 *Assume that $k \geq 1$. For $n \geq 3$, and non-zero complex numbers $c_1, \dots, c_n$ the polynomial*

$$c_1X_1^k + \cdots + c_nX_n^k \in \mathbb{C}[X_1, \dots, X_n]$$

is irreducible.

Proof For $n=2$, we have the factorization $c_1X_1^k + c_2X_2^k = c_1\prod_{I=1}^{k}(X_1 - d_iX_2)$, where $d_1, \dots, d_k$ are all the roots of $z^k + c_2/c_1 = 0$. This polynomial is square-free, that is it does not have multiple factors of degree ≥ 1. In particular, for $n=3$,

$$c_1X_1^k + P(X_2, X_3) \in \mathbb{C}[X_2, X_3][X_1],$$

is such that $P(X_2, X_3) = c_2X_2^k + c_3X_3^k$ is square-free. Let p be some irreducible factor of $P(X_2, X_3)$. Then the polynomial above is Eisenstein with respect to p (since p^2 does not divide $P(X_2, X_3)$), so the polynomial is irreducible. Now for $n \geq 4$ we apply induction on n noting that

$$c_1X_1^k + P(X_2, \dots, X_n) \in \mathbb{C}[X_2, \dots, X_n][X_1],$$

where $P(X_2,\dots,X_n) = c_2X_2^k + \cdots + c_nX_n^k$ is irreducible for $n \geq 4$ (by the induction hypothesis), so our polynomial is Eisenstein with respect to the prime $p := P(X_2,\dots,X_n)$. This proves the lemma. □

Corollary 1 *Assume that $k \geq 1$. If $n \geq 2$, the polynomial $c_1X_1^k + \cdots + c_nX_n^k - 1$ is irreducible.*

Proof Indeed, for if not, the homogenized polynomial

$$c_1X_1^k + \cdots + c_nX_n^k - X_{n+1}^k$$

is reducible in $\mathbb{C}[X_1,\dots,X_{n+1}]$, which is impossible by Lemma 3. □

Now we need to deal with the case when we have a Laurent-polynomial which looks as follows

$$P = c_1X_1^k + \cdots + c_nX_n^k - c_{n+1}/(X_1\cdots X_n)^k.$$

Clearing up the powers of X_i from the denominators and calculating $P-1$, it will be necessary for the proof of Theorem 3 to look at

$$(X_1\cdots X_n)^k\big(c_1X_1^k + \cdots + c_nX_n^k - 1\big) - c_{n+1}$$

which is a polynomial in $\mathbb{C}[X_1,\dots,X_n]$.

Lemma 4 *Assume that $k \geq 1$. Let $n \geq 3$ and $c_1,\dots,c_n$ be non-zero complex numbers. Then*

$$(X_1\cdots X_n)^k\big(c_1X_1^k + \cdots + c_nX_n^k - 1\big) - c_{n+1}$$

is irreducible.

Proof We rewrite the polynomial as

$$X_1^{2k}\big(c_1(X_2\cdots X_n)^k\big) + X_1^k(X_2\cdots X_n)^k\big(c_2X_2^k + \cdots + c_nX_n^k - 1\big) - c_{n+1} = f\big(X_1^k\big),$$

where

$$f(X) = X^2\big(c_1(X_2\cdots X_n)^k\big) + X(X_2\cdots X_n)^k\big(c_2X_2^k + \cdots + c_nX_n^k - 1\big) - c_{n+1}.$$

By Capelli's theorem, the given polynomial is irreducible if we succeed to show that:

(i) $f(X)$ is irreducible over $\mathbb{C}[X_2,\dots,X_n]$;

(ii) If α is a root of $f(X)$, then α is not of the form β^q for some element $\beta \in \mathbb{C}(X_2,\dots,X_n)(\alpha)$ and any $q \mid k$.

We consider it easier to work with the reciprocal polynomial

$$\begin{aligned} f^*(X) &= X^2 f(1/X) \\ &= -c_{n+1}X^2 + X(X_2\cdots X_n)^k\big(c_2X_2^k + \cdots + c_nX_n^k - 1\big) + c_1(X_2\cdots X_n)^k. \end{aligned}$$

Additionally, since $-c_{n+1}f^*(X) = g(-c_{n+1}X)$, where

$$g(X) = X^2 + X(X_2\cdots X_n)^k\big(c_2X_2^k + \cdots + c_nX_n^k - 1\big) + c_1'(X_2\cdots X_n)^k,$$

where $c_1' = -c_1c_{n+1}$, we can work with $g(X)$ instead of $f^*(X)$. Note that (i) and (ii) hold for $f(X)$ if and only if they hold for $g(X)$. So, let us check parts (i) and (ii). Part (i) is easy. We just compute the discriminant of $g(X)$:

$$\begin{aligned}&(X_2\cdots X_n)^{2k}\big(c_2X_2^k+\cdots+c_nX_n^k-1\big)^2-4c_1'(X_2\cdots X_n)^k\\&\quad=(X_2\cdots X_n)^k\left((X_2\cdots X_n)^k\big(c_2X_2^k+\cdots+c_nX_n^k-1\big)^2-4c_1'\right).\end{aligned}$$

We show that the polynomial in parenthesis is square-free. Assume p^2 is a divisor of it for some irreducible polynomial p of positive degree. Putting

$$H:=c_2X_2^k+\cdots+c_nX_n^k-1$$

and taking derivatives with respect to X_2, we get that p divides

$$\begin{aligned}&\frac{\partial}{\partial X_2}\left((X_2\cdots X_n)^kH^2-4c_1'\right)\\&\quad=kX_2^{k-1}(X_3\cdots X_n)^kH^2+2(X_2\cdots X_n)^kH\big(kc_2X_2^{k-1}\big)\\&\quad=kX_2^{k-1}(X_3\cdots X_n)^kH\big(H+2c_2X_2^k\big).\end{aligned}$$

Clearly, since p is irreducible, it is coprime to $X_2,\ldots,X_n$ and H, so p must divide $H+2c_2X_2^k=(3c_2)X_2^k+c_3X_3^k+\cdots+c_nX_n^k-1$ and by Corollary 1, it must be associated to this last polynomial since this is irreducible. Since $n\geq 3$, the same argument using the partial derivative with respect to X_3 instead gives that p is associated to $c_2X_2^k+(3c_3)X_3^k+\cdots+X_n^k-1$ as well, a contradiction. This proves (i).

For part (ii), note that

$$\alpha=\frac{(X_2\cdots X_n)^kH+(X_2\cdots X_n)^{\lfloor k/2\rfloor}\sqrt{\Delta}}{2},$$

where

$$\Delta:=(X_2\cdots X_n)^r\big((X_2\cdots X_n)^kH^2-4c_1'\big),$$

with $r=k-2\lfloor k/2\rfloor\in\{0,1\}$. Further, from what we proved above, Δ is square-free as a polynomial in $\mathbb{C}[X_2,\ldots,X_n]$. Let $L:=\mathbb{C}(X_2,\ldots,X_n)$ and $\mathbf{x}=(X_2,\ldots,X_n)$. We need to show that α is not of the form β^q for some prime $q\mid k$ and $\beta\in L(\alpha)$. Assume there is such β and let it be

$$\beta=A(\mathbf{x})+B(\mathbf{x})\sqrt{\Delta},\quad\text{where}\qquad A(\mathbf{x}),B(\mathbf{x})\in L.$$

Since $\beta^q=\alpha$, it follows that β is integral over $\mathbb{C}[X_2,\ldots,X_n][\sqrt{\Delta}]$, and since $\sqrt{\Delta}$ is integral over $\mathbb{C}[X_2,\ldots,X_n]$, it follows that β is integral over $\mathbb{C}[X_2,\ldots,X_n]$. The same is true for $\gamma=A(\mathbf{x})-B(\mathbf{x})\sqrt{\Delta}$ since γ^q is the other root of $g(X)$. Thus, $2A(\mathbf{x})=\beta+\gamma$ is integral over $\mathbb{C}[X_2,\ldots,X_n]$, and since $A(\mathbf{x})\in L$, the fraction field of this last ring, it follows that $A(\mathbf{x})\in\mathbb{C}[X_2,\ldots,X_n]$. Now the element $\beta\gamma=A(\mathbf{x})^2-B(\mathbf{x})^2\Delta$ is also integral over $\mathbb{C}[X_2,\ldots,X_n]$, therefore so is $B(\mathbf{x})^2\Delta$. Thus, $B(\mathbf{x})^2\Delta$ is a polynomial and since Δ is square-free, it follows that $B(\mathbf{x})$ is itself a polynomial.

Now assume $q=2$. We then have

$$\begin{aligned}\frac{(X_2\cdots X_n)^kH+(X_2\ldots X_n)^{\lfloor k/2\rfloor}\sqrt{\Delta}}{2}&=(A(\mathbf{x})+B(\mathbf{x})\sqrt{\Delta})^2\\&=A(\mathbf{x})^2+B(\mathbf{x})^2\Delta+2A(\mathbf{x})B(\mathbf{x})\sqrt{\Delta},\end{aligned}$$

which gives

$$(X_2 \cdots X_n)^k H = 2A(\mathbf{x})^2 + 2B(\mathbf{x})^2 \Delta, \quad (X_2 \cdots X_n)^{\lfloor k/2 \rfloor} = 4A(\mathbf{x})B(\mathbf{x}). \tag{6}$$

The right equation above shows that both $A(\mathbf{x})$ and $B(\mathbf{x})$ are non-zero monomials of degree $\le \lfloor k/2 \rfloor$ in each variable. Thus, $\deg_{X_2}(A(\mathbf{x})^2) \le 2\lfloor k/2 \rfloor \le k$ and $\deg_{X_2}(B(\mathbf{x})^2 \Delta) \ge \deg_{X_2}(\Delta) \ge 3k > k \ge \deg_{X_2}(A(\mathbf{x})^2)$, showing that

$$\deg(2A(\mathbf{x})^2 + 2B(\mathbf{x})^2 \Delta) = \deg(2B(\mathbf{x})^2 \Delta) \ge 3k,$$

so the left equation in (6) is impossible since the polynomial on the left-hand side has X_2-degree $\deg_{X_2}((X_2 \cdots X_n)^k H) = 2k < 3k$.

Assume next that $q \ge 3$. Taking the trace from $L(\sqrt{\Delta})$ to L in the relation $\alpha = \beta^q$, we get

$$(X_2 \cdots X_n)^k H = (A(\mathbf{x}) + B(\mathbf{x})\sqrt{\Delta})^q + (A(\mathbf{x}) - B(\mathbf{x})\sqrt{\Delta})^q.$$

The right-hand side factors into $(q+1)/2$ polynomials in $\mathbb{C}[X_2, \ldots, X_n]$ as follows. For $k \in \{1, \ldots, q\}$, let $\zeta_k = e^{\frac{2k\pi i}{q}}$. These are all the roots of $\zeta^q = 1$. Further, $\zeta_q = 1$, and $\zeta_{q-k} = \zeta_k^{-1}$ for $k = 1, \ldots, (q-1)/2$. Thus,

$$\begin{aligned}
&(A(\mathbf{x}) + B(\mathbf{x})\sqrt{\Delta})^q + (A(\mathbf{x}) - B(\mathbf{x})\sqrt{\Delta})^q \\
&\quad = \prod_{k=1}^{q} \Big((A(\mathbf{x}) + B(\mathbf{x})\sqrt{\Delta}) + \zeta_k (A(\mathbf{x}) - B(\mathbf{x})\sqrt{\Delta}) \Big) \\
&\quad = 2A(\mathbf{x}) \prod_{k=1}^{(q-1)/2} \prod_{\zeta \in \{\zeta_k, \zeta_k^{-1}\}} \Big((A(\mathbf{x}) + B(\mathbf{x})\sqrt{\Delta}) + \zeta (A(\mathbf{x}) - B(\mathbf{x})\sqrt{\Delta}) \Big) \\
&\quad = 2A(\mathbf{x}) \prod_{k=1}^{(q-1)/2} \Big(\big(2 + \zeta_k + \zeta_k^{-1}\big) A(\mathbf{x})^2 + \big(2 - \zeta_k - \zeta_k^{-1}\big) B(\mathbf{x})^2 \Delta \Big).
\end{aligned}$$

If $\deg_{X_2}(A(\mathbf{x})^2) \ne \deg_{X_2}(B(\mathbf{x})^2 \Delta)$, then each of the polynomials in the above product on the right has X_2-degree exactly

$$\max \Big\{ \deg_{X_2}(A(\mathbf{x})^2), \deg_{X_2}(B(\mathbf{x})^2 \Delta) \Big\} \ge \deg_{X_2}(\Delta) \ge 3k,$$

and such a polynomial cannot divide $(X_2 \cdots X_n)^k H$, a polynomial of X_2-degree $2k$. For the above deduction we used the fact that $B(\mathbf{x}) \ne 0$, which is clear. Assume next that $\deg_{X_2}(A(\mathbf{x})^2) = \deg_{X_2}(B(\mathbf{x})^2 \Delta)$ and let a_0, b_0 be the leading X_2-coefficients (as polynomials in $\mathbb{C}[X_3, \ldots, X_n]$) of $A(\mathbf{x})^2$ and $B(\mathbf{x})^2 \Delta$. Then the polynomial

$$\big(2 + \zeta_k + \zeta_k^{-1}\big) A(\mathbf{x})^2 + \big(2 - \zeta_k - \zeta_k^{-1}\big) B(\mathbf{x})^2 \Delta$$

has X_2-degree $\deg_{X_2}(B(\mathbf{x})^2 \Delta)$ except if $(2 + \zeta_k + \zeta_k^{-1})a_0 = -(2 - \zeta_k - \zeta_k^{-1})b_0$. If that happens then a_0/b_0 must be constant and determines uniquely the amount $\zeta_k + \zeta_k^{-1} = 2\cos(2k\pi/q)$, and since $k \in \{1, \ldots, (q-1)/2\}$, this in turn determines k uniquely as well. So, this shows that in this case there is at most one k in $\{1, \ldots, (q-1)/2\}$ for which the polynomials from the product appearing in the right-most side of (7) can have X_2-degree less than $\deg_{X_2}(\Delta)$, while all the other $(q-3)/2$ factors have degree at least $\deg_{X_2}(\Delta) \ge 3k$

but such polynomials cannot be divisors of the polynomial $(X_2 \cdots X_n)^k H$ of X_2-degree $2k$. This shows that our equation is impossible for $q > 3$. Thus, $q = 3$ and we get

$$(X_2 \dots X_n)^k H = 2A(\mathbf{x})(A(\mathbf{x})^2 + 3B(\mathbf{x})^2\Delta). \tag{7}$$

Recall that H is irreducible by Corollary 1. If $A(\mathbf{x})$ divides $(X_2 \cdots X_n)^k$, it follows that $\deg_{X_2}(A(\mathbf{x})) \leq k$, so $\deg_{X_2}(A(\mathbf{x})^2) \leq 2k$. Thus, we deduce that $\deg_{X_2}(A(\mathbf{x})^2 + 3B(\mathbf{x})^2\Delta) = \deg_{X_2}(3B(\mathbf{x})^2\Delta) \geq 3k$, and we get the same contradiction as before. Thus, $H \mid A(\mathbf{x})$, showing that

$$A(\mathbf{x})^2 + 3B(\mathbf{x})^2\Delta = aM,$$

where a is some non-zero complex number and $M = X_2^{a_2} \cdots X_n^{a_n}$ is some monomial. We also have the relation

$$A(\mathbf{x})^2 - B(\mathbf{x})^2\Delta = N_{L(\sqrt{\Delta})/L}(\alpha)^{1/3} = c_1''(X_2 \cdots X_n)^{k/3} = c_1''M_1,$$

where $c_1'' = \sqrt[3]{c_1'}$ (some cubic root of c_1') and M_1 is also a monomial. Further, since

$$(X_2 \cdots X_n)^{\lfloor k/2 \rfloor} = \frac{\beta^3 - \gamma^3}{\sqrt{\Delta}} = 2B(\mathbf{x})(3A(\mathbf{x})^2 + B(\mathbf{x})^2\Delta),$$

we see that $B(\mathbf{x})$ is a divisor of $(X_2 \cdots X_n)^{\lfloor k/2 \rfloor}$, so $B(\mathbf{x}) = M_2$ is also a monomial. Thus, we get

$$\Delta = \frac{aM - c_1''M_1}{4M_2^2}.$$

The right-hand side above is a polynomial and since M, M_1, M_2 are monomials, it follows that $M_2^2 \mid M$ and $M_2^2 \mid M_1$. Thus, $\Delta = cM_3 + dM_4$ is a sum of two monomials with some non-zero coefficients. However, this is impossible since a quick look at Δ shows that as a polynomial in X_2 it has non-zero coefficients for $X_2^{3k+r}, X_2^{2k+r}, X_2^{k+r}$ and X_2^r, where $r = k - 2\lfloor k/2 \rfloor \in \{0, 1\}$. This contradiction finishes (ii); hence, the proof. □

4 Proof of Theorem 1

The aim of this section is to prove Theorem 1.

Proof We first show that if there are infinitely many solutions to (1), then all of them can be parametrized by finitely many expressions as given in (14) for c below. The arguments in this section follow the arguments from [13] and [14].

From now on, we assume w.l.o.g. that $\alpha_1 = |\alpha_1| > |\alpha_2| \geq \cdots \geq |\alpha_k|$.

We assume that there are infinitely many solutions to (1). Then, for each integer solution (a, b, c), we have

$$a = \sqrt{\frac{(F_x - 1)(F_y - 1)}{F_z - 1}},\ b = \sqrt{\frac{(F_x - 1)(F_z - 1)}{F_y - 1}},\ c = \sqrt{\frac{(F_y - 1)(F_z - 1)}{F_x - 1}}.$$

Our first aim is to prove, that the growth-rates of these infinitely many x, y and z have to be the same, except for a multiplicative constant. Let us recall that we trivially have $x < y < z$ and that, by Lemma 1, the solutions of x need to diverge to infinity as well. We now want to prove that there exists a constant $C_5 > 0$ such that $C_5 z < x$ for infinitely many triples (x, y, z).

In order to prove this, we choose x (and hence y, z) large enough. We denote by $g := \gcd(F_y - 1, F_z - 1)$. Then we use Lemma 2 to obtain

$$\begin{aligned}|f_1|\alpha_1^x > F_x - 1 \geq \frac{F_x - 1}{a} = b = \frac{F_z - 1}{c} \geq \frac{F_z - 1}{g} \geq \frac{|f_1|\alpha_1^z - 2}{C_1\alpha_1^{\frac{kz}{k+1}}}\\ \geq \frac{|f_1|}{C_1}\alpha_1^{\frac{z}{k+1}-1} > |f_1|\alpha_1^{\frac{z}{k+1}-C_6}\end{aligned}$$

and hence

$$x > \frac{z}{k+1} - C_6$$

which implies $x > C_7 z$ for a suitable new constant C_7 (depending only on k) and x, z being sufficiently large.

Next, we do a Taylor series expansion for c which was given by

$$c = \sqrt{\frac{(F_y - 1)(F_z - 1)}{F_x - 1}}. \tag{8}$$

Using the power sum representations of F_x, F_y, F_z, we get

$$\begin{aligned}c =& \sqrt{f_1}\alpha_1^{(-x+y+z)/2}\\ &\times \left(1 + (-1/f_1)\alpha_1^{-x} + (f_2/f_1)\alpha_2^x\alpha_1^{-x} + \cdots + (f_k/f_1)\alpha_k^x\alpha_1^{-x}\right)^{-1/2}\\ &\times \left(1 + (-1/f_1)\alpha_1^{-y} + (f_2/f_1)\alpha_2^y\alpha_1^{-y} + \cdots + (f_k/f_1)\alpha_k^y\alpha_1^{-y}\right)^{1/2}\\ &\times \left(1 + (-1/f_1)\alpha_1^{-z} + (f_2/f_1)\alpha_2^z\alpha_1^{-z} + \cdots + (f_k/f_1)\alpha_k^z\alpha_1^{-z}\right)^{1/2}.\end{aligned}$$

We then use the binomial expansion to obtain

$$\begin{aligned}(1 \ &+ (-1/f_1)\alpha_1^{-x} + (f_2/f_1)\alpha_2^x\alpha_1^{-x} + \cdots + (f_k/f_1)\alpha_k^x\alpha_1^{-x})^{1/2}\\ &= \sum_{j=0}^{T}\binom{1/2}{j}\left((-1/f_1)\alpha_1^{-x} + (f_2/f_1)\alpha_2^x\alpha_1^{-x} + \cdots + (f_k/f_1)\alpha_k^x\alpha_1^{-x}\right)^j\\ &\quad + \mathcal{O}(\alpha_1^{-(T+1)x}),\end{aligned}$$

where $\mathcal{O}$ has the usual meaning, using estimates from [15] and where T is some index, which we will specify later. Let us write $\mathbf{x} := (x, y, z)$. Since $x < z$ and $z < x/C_7$, the remainder term can also be written as $\mathcal{O}(\alpha_1^{-T\|\mathbf{x}\|/C_7})$, where $\|\mathbf{x}\| = \max\{x, y, z\} = z$. Doing the same for y and z likewise and multiplying those expressions gives

$$\begin{aligned}c &= \sqrt{f_1}\,\alpha_1^{(-x+y+z)/2} \cdot \left[1 + \frac{-1 + \sum_{p=2}^{k} f_p\,\alpha_p^x}{f_1\,\alpha_1^x}\right]^{-1/2}\\ &\quad \times \left[1 + \frac{-1 + \sum_{q=2}^{k} f_q\,\alpha_q^y}{f_1\,\alpha_1^y}\right]^{1/2} \left[1 + \frac{-1 + \sum_{r=2}^{k} f_r\,\alpha_r^z}{f_1\,\alpha_1^z}\right]^{1/2}\\ &= \sqrt{f_1}\,\alpha_1^{(-x+y+z)/2}\\ &\quad \times \left(\sum_{p_1=0}^{T}\sum_{q_1=0}^{T}\sum_{r_1=0}^{T}\ \sum_{p_0+p_2+\cdots+p_k=p_1}\ \sum_{q_0+q_2+\cdots+q_k=q_1}\ \sum_{r_0+r_2+\cdots+r_k=r_1} d_{\mathbf{p},\mathbf{q},\mathbf{r}}\,M_{\mathbf{p},\mathbf{q},\mathbf{r}}\right)\\ &\quad + \mathcal{O}\left(\alpha_1^{T\|\mathbf{x}\|/C_9}\right)\end{aligned}$$

in terms of

$$d_{\mathbf{p},\mathbf{q},\mathbf{r}} = \frac{\left(-\frac{1}{2}\right)! p_1! \, \frac{1}{2}! \, \frac{1}{2}!}{\left(-\frac{1}{2} - p_1\right)! \, \left(\frac{1}{2} - q_1\right)! \, \left(\frac{1}{2} - r_1\right)!} \\ \times \frac{(-1)^{p_0+q_0+r_0}}{p_0! \, q_0! \, r_0!} f_1^{-p_1-q_1-q_1} \frac{f_2^{p_2+q_2+r_2}}{p_2! \, q_2! \, r_2!} \cdots \frac{f_k^{p_k+q_k+r_k}}{p_k! \, q_k! \, r_k!}$$

and

$$M_{\mathbf{p},\mathbf{q},\mathbf{r}} = \alpha_1^{-p_1 x - q_1 y - r_1 z} \, \alpha_2^{p_2 x + q_2 y + r_2 z} \, \cdots \, \alpha_k^{p_k x + q_k y + r_k z}$$

where $\mathbf{p} = (p_0, p_1, \ldots, p_k)$, $\mathbf{q} = (q_0, q_1, \ldots, q_k)$, and $\mathbf{r} = (r_0, r_1, \ldots, r_k)$ are vectors of non-negative integers satisfying

$$p_0 + p_2 + \cdots + p_k = p_1, \quad q_0 + q_2 + \cdots + q_k = q_1, \quad r_0 + r_2 + \cdots + r_k = r_1,$$

and $\|\mathbf{p}\|, \|\mathbf{q}\|, \|\mathbf{r}\| \leq T$. Since there are only finitely many such vectors, we may label the coefficients $d_{\mathbf{p},\mathbf{q},\mathbf{r}}$ and monomials $M_{\mathbf{p},\mathbf{q},\mathbf{r}}$ as $d_0, \, d_1, \, \ldots, \, d_{n-1}$ and $M_0, \, M_1, \, \ldots, \, M_{n-1}$, respectively, where we choose $d_0 = M_0 = 1$. In summary we have

$$c = \sqrt{f_1} \alpha_1^{(-x+y+z)/2} \left(1 + \sum_{j=1}^{n-1} d_j M_j\right) + \mathcal{O}(\alpha_1^{-T\|\mathbf{x}\|/C_7}), \tag{9}$$

where the integer n depends only on T, d_j are non-zero coefficients in the field $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$, and M_j is a monomial of the form

$$M_j = \prod_{i=1}^{k} \alpha_i^{L_{i,j}(\mathbf{x})},$$

in which $L_{i,j}(\mathbf{x})$ are linear forms in $\mathbf{x} \in \mathbb{R}^3$ with integer coefficients which are all non-negative if $i = 2, \ldots, k$ and negative if $i = 1$. Set $J = \{1, \ldots, n-1\}$. Note that each monomial M_j is "small", that is there exists a constant $\kappa > 0$ (which we can even choose independently of k), such that

$$|M_j| \leq e^{-\kappa x} \qquad \text{for all} \qquad j \in J. \tag{10}$$

This follows easily from the following fact: By the Pisot property of F_n, we can write $\alpha_1 = |\alpha_1| > 1 + \zeta$ for a suitable $\zeta > 0$ (a conjecture of Lehmer asserts that ζ can be chosen to be an absolute constant). Using this notation and a suitable κ, we have

$$\begin{aligned} |M_j| &= |\alpha_1|^{L_{1,j}(\mathbf{x})} \cdot |\alpha_2|^{L_{2,j}(\mathbf{x})} \cdots |\alpha_k|^{L_{k,j}(\mathbf{x})} \\ &\leq (1+\zeta)^{L_{1,j}(\mathbf{x})} \cdot 1 \cdots 1 \\ &\leq (1+\zeta)^{-x} \\ &\leq e^{-\kappa x} \qquad \text{for all} \qquad j \in J. \end{aligned}$$

Our next aim is to apply a version of the Subspace theorem given in [10] to show that there is a finite expansion of c involving terms as in (9); the version we are going to use can also be found in Section 3 of [16], whose notation - in particular the notion of heights - we follow.

We work with the field $K = \mathbb{Q}(\alpha_1, \dots, \alpha_k)$ and let S be the finite set of places (which are normalized so that the Product Formula holds, cf. [10]), that are either infinite or in the set $\{v \in M_K : |\alpha_1|_v \neq 1 \vee \dots \vee |\alpha_k|_v \neq 1\}$. Observe that we may choose $\alpha_1, \dots, \alpha_k$ in $\mathbb{C}$ and therefore view K as a subfield of $\mathbb{C}$. We denote by $|\cdot|_\infty$ the unique place such that $|\beta|_\infty = |\beta| = \sqrt{\Re(\beta)^2 + \Im(\beta)^2}$ for all $\beta \in \mathbb{C}$. According to whether $-x+y+z$ is even or odd, we set $\epsilon = 0$ or $\epsilon = 1$ respectively, such that $\alpha_1^{(-x+y+z-\epsilon)/2} \in K$. By going to a still infinite subset of the solutions, we may assume that ϵ is always either 0 or 1.

Using the fixed integer n (depending on T) from above, we now define $n+1$ linearly independent linear forms in indeterminants $(C, Y_0, \dots, Y_{n-1})$. For the place ∞ introduced above, we set

$$l_{0,\infty}(C, Y_0, \dots, Y_{n-1}) := C - \sqrt{f_1\alpha_1^\epsilon}\, Y_0 - \sqrt{f_1\alpha_1^\epsilon} \sum_{j=1}^{n-1} d_j Y_j, \tag{11}$$

where $\epsilon \in \{0, 1\}$ is as explained above, and

$$l_{i,\infty}(C, Y_0, \dots, Y_{n-1}) := Y_{i-1} \quad \text{for } i = 1, \dots, n.$$

For all other places v in S, we define

$$l_{0,v} := C, \qquad l_{i,v} := Y_{i-1} \quad \text{for } i = 1, \dots, n.$$

We will show, that there is some $\delta > 0$, such that the inequality

$$\prod_{v \in S} \prod_{i=0}^{n} \frac{|l_{i,v}(\mathbf{y})|_v}{|\mathbf{y}|_v} < \left(\prod_{v \in S} |\det(l_{0,v}, \dots, l_{n,v})|_v \right) \cdot \mathcal{H}(\mathbf{y})^{-(n+1)-\delta} \tag{12}$$

is satisfied for all vectors

$$\mathbf{y} = \left(c, \alpha_1^{(-x+y+z-\epsilon)/2}, \alpha_1^{(-x+y+z-\epsilon)/2} M_1, \dots, \alpha_1^{(-x+y+z-\epsilon)/2} M_{n-1} \right).$$

We shall use the notation $\mathbf{y} = (c, y_0, \dots, y_{n-1})$ below. The use of the correct $\epsilon \in \{0, 1\}$ guarantees that these vectors are indeed in K^{n+1}.

First notice, that the determinant in (12) is given by

$$\det \begin{pmatrix} 1 & -\sqrt{f_1\,\alpha_1^\epsilon} & -\sqrt{f_1\,\alpha_1^\epsilon}\, d_1 & \cdots & -\sqrt{f_1\,\alpha_1^\epsilon}\, d_{n-1} \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

if $v = \infty$ and by

$$\det \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

if $v \neq \infty$. Thus $|\det(l_{0,v}, \dots, l_{n,v})|_v = |1|_v = 1$ for all places v. Notice further, that

$$\mathcal{H}(\mathbf{y}) = \prod_{v} |\mathbf{y}|_v = \prod_{v \in S} |\mathbf{y}|_v \prod_{v \notin S} |\mathbf{y}|_v \leq \prod_{v \in S} |\mathbf{y}|_v$$

since for all $v \notin S$ we have $|\mathbf{y}|_v = \max\{|c|_v, |y_0|_c, \ldots, |y_{n-1}|_v\} \leq 1$, which is a consequence of $c \in \mathbb{Z}$ and the remaining components $y_0, \ldots, y_{n-1}$ of $\mathbf{y}$ being S-units (hence satisfy $|y_i|_v = 1$ for all $v \notin S$). It follows that

$$0 \leq \prod_{v \in S} \prod_{i=0}^{n} \frac{1}{|\mathbf{y}|_v} \leq \mathcal{H}(\mathbf{y})^{-(n+1)}.$$

Thus, for (12) it suffices to consider

$$\prod_{v \in S} \prod_{i=0}^{n} |l_{i,v}(\mathbf{y})|_v < \mathcal{H}(\mathbf{y})^{-\delta},$$

and the double product on the left-hand side can be split up into

$$\left| c - \sqrt{f_1 \alpha_1^{\epsilon}} y_0 - \sqrt{f_1 \alpha_1^{\epsilon}} \sum_{j=1}^{n-1} d_j y_j \right|_{\infty} \cdot \prod_{\substack{v \in M_{K,\infty}, \\ v \neq \infty}} |c|_v \cdot \prod_{v \in S \setminus M_{K,\infty}} |c|_v \cdot \prod_{j=0}^{n-1} \prod_{v \in S} |y_j|_v.$$

Now notice that the last double product equals 1 due to the Product Formula and that

$$\prod_{v \in S \setminus M_{K,\infty}} |c|_v \leq 1,$$

since $c \in \mathbb{Z}$. An upper bound on the number of infinite places in K is $k!$ and hence,

$$\begin{aligned} \prod_{\substack{v \in M_{K,\infty}, \\ v \neq \infty}} |c|_v &< \left(\frac{(F_y - 1)(F_z - 1)}{F_x - 1} \right)^{k!} \\ &\leq \left| f_1 \alpha_1^y + \cdots + f_k \alpha_k^y - 1 \right|^{k!} \left| f_1 \alpha_1^z + \cdots + f_k \alpha_k^z - 1 \right|^{k!} \\ &\leq \left(|f_1| \cdot \alpha_1^{\|\mathbf{x}\|} - 1/2 \right)^{2 \cdot k!} \end{aligned}$$

for y large enough such that $|f_2 \alpha_2^y + \cdots + f_k \alpha_k^y| < 1/2$. And finally the first expression is just

$$\left| \sqrt{f_1 \alpha_1^{\epsilon}} \alpha_1^{(-x+y+z-\epsilon)/2} \sum_{j \geq n} d_j M_j \right|,$$

which, by (9), is smaller than some expression of the form $C_8 \alpha_1^{-T\|\mathbf{x}\|/C_7}$. Therefore, we have

$$\prod_{v \in S} \prod_{i=0}^{n} |l_{i,v}(\mathbf{y})|_v < C_8 \alpha_1^{-\frac{T\|\mathbf{x}\|}{C_9}} \cdot \left(|f_1| \alpha_1^{\|\mathbf{x}\|} - 1/2 \right)^{2 \cdot k!}.$$

Now we choose T (and the corresponding n) large enough such that

$$C_8 \alpha_1^{-\frac{T\|\mathbf{x}\|}{C_7}} < \alpha_1^{-\frac{T\|\mathbf{x}\|}{2C_7}}, \quad \left(|f_1| \alpha_1^{\|\mathbf{x}\|} - 1/2 \right)^{2 \cdot k!} < \alpha_1^{\frac{T\|\mathbf{x}\|}{4C_7}}.$$

Then we can write

$$\prod_{v \in S} \prod_{i=0}^{n} |l_{i,v}(\mathbf{y})|_v < \alpha_1^{\frac{-T\|\mathbf{x}\|}{4C_7}}. \tag{13}$$

For the height of our vector $\mathbf{y}$, we have the estimate

$$\begin{aligned}\mathcal{H}(\mathbf{y}) &\leq C_9 \cdot \mathcal{H}(c) \cdot \mathcal{H}\left(\alpha_1^{\frac{-x+y+z-\epsilon}{2}}\right)^n \cdot \prod_{i=0}^{n-1} \mathcal{H}(M_i) \\ &\leq C_9 \left(|f_1| \alpha_1^{\|\mathbf{x}\|} - 1/2\right)^{k!} \prod_{i=0}^{n-1} \alpha_1^{C_{10}\|\mathbf{x}\|} \\ &\leq \alpha_1^{C_{11}\|\mathbf{x}\|},\end{aligned}$$

with suitable constants C_9, C_{10}, C_{11}. For the second estimate, we used that

$$\mathcal{H}(M_j) \leq \mathcal{H}(\alpha_1)^{C_{\alpha_1}(\mathbf{x})} \mathcal{H}(\alpha_2)^{C_{\alpha_2}(\mathbf{x})} \cdots \mathcal{H}(\alpha_k)^{C_{\alpha_k}(\mathbf{x})}$$

and bounded it by the maximum of those expressions. Furthermore we have

$$\mathcal{H}\left(\alpha_1^{\frac{-x+y+z-\epsilon}{2}}\right)^n \leq \alpha_1^{n\|\mathbf{x}\|},$$

which just changes our constant C_{11}.

Now finally, the estimate

$$\alpha_1^{-\frac{T\|\mathbf{x}\|}{4C_7}} \leq \alpha_1^{-\delta C_{11}\|\mathbf{x}\|}$$

is satisfied provided that we pick δ small enough.

So all the conditions for the Subspace theorem are met. Since we assumed that there are infinitely many solutions (x, y, z) of (12), we now can conclude that all of them lie in finitely many proper linear subspaces. Therefore, there must be at least one proper linear subspace, which contains infinitely many solutions and we see that there exists a finite set J_c and (new) coefficients e_j (for $j \in J_c$) in K such that we have

$$c = \alpha_1^{(-x+y+z-\epsilon)/2}\left(e_0 + \sum_{j \in J_c} e_j M_j\right) \tag{14}$$

with monomials M_j as before.

Likewise, we can find finite expressions of this form for a and b.

Next we use the following parametrization lemma:

Lemma 5 *Suppose, we have infinitely many solutions for* (1)*. Then there exists a line in* $\mathbb{R}^3$ *given by*

$$x(t) = r_1 t + s_1 \quad y(t) = r_2 t + s_2 \quad z(t) = r_3 t + s_3$$

with rationals $r_1, r_2, r_3, s_1, s_2, s_3$*, such that infinitely many of the solutions* (x, y, z) *are of the form* $(x(n), y(n), z(n))$ *for some integer* n*.*

Proof Assume that (1) has infinitely many solutions. We already deduced in Section 4 that c can be written in the form

$$c = \alpha_1^{(-x+y+z-\epsilon)/2}\left(e_{c,0} + \sum_{j \in J_c} e_{c,j} M_{c,j}\right)$$

with J_c being a finite set, $e_{c,j}$ being coefficients in K for $j \in J_c \cup \{0\}$ and $M_{c,j} = \prod_{i=1}^{k} \alpha_i^{L_{c,i,j}(\mathbf{x})}$ with $\mathbf{x} = (x, y, z)$. In the same manner, we can write

$$b = \alpha_1^{(x-y+z-\epsilon)/2} \left(e_{b,0} + \sum_{j \in J_b} e_{b,j} M_{b,j} \right).$$

Since $1 + bc = F_z = f_1 \alpha_1^z + \cdots + f_k \alpha_k^z$, we get

$$f_1 \alpha_1^z + \cdots + f_k \alpha_k^z - \alpha_1^{z-\varepsilon} \left(e_{b,0} + \sum_{j \in J_b} e_{b,j} M_{b,j} \right) \left(e_{c,0} + \sum_{j \in J_c} e_{c,j} M_{c,j} \right) = 1. \tag{15}$$

We now pick $\beta_1, \ldots, \beta_\ell$ as a basis for the multiplicative group generated by $\{\alpha_1, \ldots, \alpha_k, -1\}$. We remark that each element in this group is an S-unit with the set S defined in Sect. 4. We express each $\alpha_1, \ldots, \alpha_k$ as a product of $\beta_1, \ldots, \beta_\ell$ and insert them into (15). We obtain a new equation of the form

$$\sum_{j \in J} e_j \beta_1^{L_{1,j}(\mathbf{x})} \cdots \beta_\ell^{L_{\ell,j}(\mathbf{x})} = 0, \tag{16}$$

where again J is some finite set, e_j are new coefficients in K and $L_{i,j}$ are linear forms in $\mathbf{x}$ with integer coefficients. Note that the sum on the left hand side is not zero, since it contains the summand -1. This is an S-unit equation.

We may assume that infinitely many of the solutions $\mathbf{x}$ are non-degenerate solutions of (16) by replacing the equation by a new equation given by a suitable vanishing subsum if necessary.

We may assume, that $(L_{1,i}, \ldots, L_{\ell,i}) \neq (L_{1,j}, \ldots, L_{\ell,j})$ for any $i \neq j$, because otherwise we could just merge these two terms.

Therefore for $i \neq j$, the theorem on non-degenerate solutions to S-unit equations (see [11]) yields that the set of

$$\beta_1^{L_{1,i}(\mathbf{x}) - L_{1,j}(\mathbf{x})} \cdots \beta_\ell^{L_{\ell,i}(\mathbf{x}) - L_{\ell,j}(\mathbf{x})}$$

is contained in a finite set of numbers. Now since $\beta_1, \ldots, \beta_\ell$ are multiplicatively independent, the exponents $(L_{1,i} - L_{1,j})(\mathbf{x}), \ldots, (L_{\ell,i} - L_{\ell,j})(\mathbf{x})$ take the same value for infinitely many $\mathbf{x}$. Since we assumed, that these linear forms are not all identically zero, this implies, that there is some non-trivial linear form L defined over $\mathbb{Q}$ and some $c \in \mathbb{Q}$ with $L(\mathbf{x}) = c$ for infinitely many $\mathbf{x}$. So there exist rationals r_i, s_i, t_i for $i = 1, 2, 3$ such that we can parametrize

$$x = r_1 p + s_1 q + t_1, \quad y = r_2 p + s_2 q + t_2, \quad z = r_3 p + s_3 q + t_3$$

with infinitely many pairs $(p, q) \in \mathbb{Z}^2$.

We can assume, that r_i, s_i, t_i are all integers. If not, we define Δ as the least common multiple of the denominators of r_i, s_i $(i = 1, 2, 3)$ and let p_0, q_0 be such that for infinitely many pairs (p, q) we have $p \equiv p_0 \mod \Delta$ and $q \equiv q_0 \mod \Delta$. Then $p = p_0 + \Delta\lambda$, $q = q_0 + \Delta\mu$ and

$$\begin{aligned} x &= (r_1\Delta)\lambda + (s_1\Delta)\mu + (r_1 p_0 + s_1 q_0 + t_1) \\ y &= (r_2\Delta)\lambda + (s_2\Delta)\mu + (r_2 p_0 + s_2 q_0 + t_2) \\ z &= (r_3\Delta)\lambda + (s_3\Delta)\mu + (r_3 p_0 + s_3 q_0 + t_3). \end{aligned}$$

Since $r_i\Delta$, $s_i\Delta$ and x, y, z are all integers, $r_ip_0 + s_iq_0 + t_i$ are integers as well. Replacing r_i by $r_i\Delta$, s_i by $s_i\Delta$ and t_i by $r_ip_0 + s_iq_0 + t_i$, we can indeed assume, that all coefficients r_i, s_i, t_i in our parametrization are integers.

Using a similar argument as in the beginning of the proof, we get that our equation is of the form

$$\sum_{j\in J} e'_j \beta_1^{L'_{1,j}(\mathbf{r})} \cdots \beta_\ell^{L'_{\ell,j}(\mathbf{r})} = 0,$$

where $\mathbf{r} := (\lambda, \mu)$, J is a finite set of indices, e'_j are new non-zero coefficients in K and $L'_{i,j}(\mathbf{r})$ are linear forms in $\mathbf{r}$ with integer coefficients. Again we may assume that we have $(L'_{1,i}(\mathbf{r}), \ldots, L'_{\ell,i}(\mathbf{r})) \neq (L'_{1,j}(\mathbf{r}), \ldots, L'_{\ell,j}(\mathbf{r}))$ for any $i \neq j$.

Applying the theorem of non-degenerate solutions to S-unit equations once more, we obtain a finite set of numbers Λ, such that for some $i \neq j$, we have

$$\beta_1^{(L'_{1,i}-L'_{1,j})(\mathbf{r})} \cdots \beta_\ell^{(L'_{\ell,i}-L'_{\ell,j})(\mathbf{r})} \in \Lambda.$$

So every $\mathbf{r}$ lies on a finite collection of lines and since we had infinitely many $\mathbf{r}$, there must be some line, which contains infinitely many solutions, which proves our lemma. □

We apply this lemma and define Δ as the least common multiple of the denominators of r_1, r_2, r_3. Infinitely many of our n will be in the same residue class modulo Δ, which we shall call r. Writing $n = m\Delta + r$, we get

$$(x, y, z) = ((r_1\Delta)m + (rr_1 + s_1), (r_2\Delta)m + (rr_2 + s_2), (r_3\Delta)m + (rr_3 + s_3)).$$

Replacing n by m, r_i by $r_i\Delta$ and s_i by $rr_i + s$, we can even assume, that r_i, s_i are integers. So we have

$$\frac{-x + y + z - \epsilon}{2} = \frac{(-r_1 + r_2 + r_3)m}{2} + \frac{-s_1 + s_2 + s_3 - \epsilon}{2}.$$

This holds for infinitely many m, so we can choose a still infinite subset such that all of them are in the same residue class χ modulo 2 and we can write $m = 2\ell + \chi$ with fixed $\chi \in \{0, 1\}$. Thus, we have

$$\frac{-x + y + z - \epsilon}{2} = (-r_1 + r_2 + r_3)\ell + \eta,$$

where $\eta \in \mathbb{Z}$ or $\eta \in \mathbb{Z} + 1/2$.

Using this representation, we can write (14) as

$$c(\ell) = \alpha_1^{(-r_1+r_2+r_3)\ell+\eta} \left(e_0 + \sum_{j\in J_c} e_j M_j \right)$$

for infinitely many ℓ, where

$$M_j = \prod_{i=1}^{k} \alpha_i^{L_{i,j}(\mathbf{x})},$$

and $\mathbf{x} = \mathbf{x}(\ell) = (x(2\ell + \chi), y(2\ell + \chi), z(2\ell + \chi))$.

So for infinitely many solutions (x, y, z), we have a parametrization in ℓ, such that c is a power sum in this ℓ with its roots being products of $\alpha_1, \ldots, \alpha_k$. This, together with (8) gives the functional identity

$$(F_x - 1)c^2 = (F_y - 1)(F_z - 1), \tag{17}$$

which proves Theorem 1. □

5 Linear recurrences with nonsquare leading coefficient

The aim of this section is to prove Theorem 2.

Proof We prove this result by contradiction: Suppose we had infinitely many Diophantine triples in $\{F_n; n \geq 0\}$. Then we can apply Theorem 1 and obtain

$$c(\ell) = \alpha_1^{(-r_1+r_2+r_3)\ell+\eta}\left(e_0 + \sum_{j\in J_c} e_j M_j\right) \tag{18}$$

for infinitely many ℓ, where

$$M_j = \prod_{i=1}^{k} \alpha_i^{L_{i,j}(\mathbf{x})},$$

and $\mathbf{x} = \mathbf{x}(\ell) = (x(2\ell+\chi), y(2\ell+\chi)), z(2\ell+\chi))$.

First we observe, that there are only finitely many solutions of (18) with $c(\ell) = 0$. That can be shown by using the fact, that a simple non-degenerate linear recurrence has only finite zero-multiplicity (see [11] for an explicit bound). We will apply this statement here for the linear recurrence in ℓ; it only remains to check, that no quotient of two distinct roots of the form

$$\alpha_1^{L_{1,i}(\mathbf{x}(\ell))}\cdots\alpha_k^{L_{k,i}(\mathbf{x}(\ell))}$$

is a root of unity or, in other words, that

$$\left(\alpha_1^{m_1}\alpha_2^{m_2}\cdots\alpha_k^{m_k}\right)^n = 1$$

has no solutions in $n \in \mathbb{Z}/\{0\}$, $m_1 < 0$ and $m_i > 0$ for $i = 2, \ldots, k$. But this follows at once from Mignotte's result [24].

So, we have confirmed that $c(\ell) \neq 0$ for still infinitely many solutions. We insert the finite expansion (18) in ℓ for c into (17). Furthermore, we use the Binet formula

$$F_x = f_1\alpha_1^x + \cdots + f_k\alpha_k^x \tag{19}$$

and write F_x, F_y, F_z as power sums in x, y and z respectively. We get an equation of the form

$$\begin{aligned}
&\left(f_1\alpha_1^x + \cdots + f_k\alpha_k^x - 1\right)\\
&\quad\times\alpha_1^{-x+y+z-\epsilon}\left(e_0^2 + 2e_0e_1\alpha_1^{-x} + 2e_0e_2\alpha_1^{-y} + 2e_0e_3\alpha_1^{-z} + e_1^2\alpha_1^{-2x} + \cdots\right)\\
&= \left(f_1\alpha_1^y + \cdots + f_k\alpha_k^y - 1\right)\left(f_1\alpha_1^z + \cdots + f_k\alpha_k^z - 1\right),
\end{aligned}$$

Using the parametrization $(x, y, z) = (r_1m + s_1, r_2m + s_2, r_3m + s_3)$ with $m = 2\ell$ or $m = 2\ell + 1$, we have expansions in ℓ on both sides of (17). Since there must be infinitely many solutions in ℓ, the largest terms on both sides have to grow at the same rate.

In order to find the largest terms, let us first note the following: If $e_0 = 0$ for infinitely many of our solutions, then the largest terms were

$$f_1\alpha_1^x\alpha_1^{-x+y+z-\epsilon}e_1^2\alpha_1^{-2x} = f_1\alpha_1^y f_1\alpha_1^z, \tag{20}$$

or some even smaller expression on the left-hand side, if $e_1 = 0$ as well. Note that there could be more than one term in the expansion of c with the same growth rate, for example if y and z are just translates of x and therefore we have $\alpha_1^{-y} = \alpha_1^{-x-c} = C\alpha_1^{-x}$, but this would only change the coefficient e_1 which we do not know anyway. From (20), we get

$$e_1^2\alpha_1^{-2x+y+z-\epsilon} = f_1\alpha_1^{y+z}.$$

Dividing by α_1^{y+z} on both sides, we see that the left-hand side converges to 0, when x grows to infinity (which it does by Lemma 1), while the right-hand side is the constant $f_1 \neq 0$. This is a contradiction.

So we must have that $e_0 \neq 0$ for infinitely many of our solutions. Then $e_0\alpha_1^{(-x+y+z-\epsilon)/2}$ certainly is the largest term in the expansion of c and we have

$$f_1\alpha_1^x\alpha_1^{-x+y+z-\epsilon}e_0^2 = f_1\alpha_1^y f_1\alpha_1^z.$$

for the largest terms, which implies that $e_0^2 = f_1\alpha_1^{\epsilon}$. But this is a contradiction, since we assumed that neither f_1 nor $f_1\alpha_1$ is a square in K. So, the theorem is proved. □

6 Linear recurrences of large order

We now prove Theorem 3.

Proof We follow the same notation as in the proof of Theorem 1. Supposing that we have infinitely many Diophantine triples with values in $\{F_n; n \geq 0\}$, we get the functional identity

$$(F_x - 1)c(\ell)^2 = (F_y - 1)(F_z - 1),$$

where $x = r_1\ell + s_1, y = r_2\ell + s_2, z = r_3\ell + s_3, r_1, r_2, r_3$ positive integers with $\gcd(r_1, r_2, r_3) = 1$ and s_1, s_2, s_3 integers.

We first handle (i) in the theorem. Therefore assume that α is not a unit. Then, by Mignotte's result [24], there is no multiplicative dependence between the roots and thus (e.g. by using Lemma 2.1 in [7]), it follows that if we put $\mathbf{X} = (X_1, \ldots, X_k)$ and

$$P_i(\mathbf{X}) = \sum_{j=1}^{k} f_j\alpha_j^{s_i}X_j^{r_i} - 1 \in K[X_1, \ldots, X_k] \quad \text{for} \quad i = 1, 2, 3,$$

then for each $h \in \{1, 2, 3\}$ putting i, j such that $\{h, i, j\} = \{1, 2, 3\}$, we have that

$$\frac{P_i(\mathbf{X})P_j(\mathbf{X})}{P_h(\mathbf{X})} = Q_h(\mathbf{X})^2, \tag{21}$$

for some $Q_h(\mathbf{X}) \in K[X_1^{\pm 1}, \ldots, X_k^{\pm 1}]$. For this we have to identify the exponential function $\ell \mapsto \alpha_1^\ell$ by X_1, $\ell \mapsto \alpha_2^\ell$ by X_2 and so forth. Actually, Theorem 1 shows that $Q_h(\mathbf{X}) \in K[X_1^{\pm 1}, X_2, \ldots, X_k]$. Since the polynomial on the left-hand side of (21) has no pole at $X_1 = 0$ it follows that the Laurent-polynomial on the right-hand side is a polynomial in X_1 as well. This imposes some conditions on the degrees:

(P) *Parity:* $r_1 + r_2 + r_3 \equiv 0 \pmod 2$. This is clear from degree considerations since $2\deg_{X_1}(Q_h) = \deg_{X_1}(P_i) + \deg_{X_1}(P_j) - \deg_{X_1}(P_h) = r_i + r_j - r_h$.

(T) *Triangular inequality:* $r_1 + r_2 > r_3$. It is clear that $r_1 + r_2 \geq r_3$, otherwise $P_1(\mathbf{X})P_2(\mathbf{X})/P_3(\mathbf{X})$ has negative degree as a polynomial in, say, X_1, so it cannot be a polynomial in X_1. To see that the inequality must be in fact strict, assume that equality holds. Then $Q_3(\mathbf{X}) = q_3 \in K[X_1]$. Hence,

$$P_1(\mathbf{X})P_2(\mathbf{X}) = q_3^2P_3(\mathbf{X}).$$

In the left, we have the monomial $X_1^{r_1}X_2^{r_2}$ with non-zero coefficient $f_1f_2\alpha_1^{s_1}\alpha_2^{s_2}$, whenever $r_1 < r_2$. However, such monomials do not appear in the right above. Thus, we must have $r_1 = r_2$, and since further we also have $r_3 = r_1 + r_2$ and $\gcd(r_1, r_2, r_3) = 1$, it follows that $(r_1, r_2, r_3) = (1, 1, 2)$. In this case, the coefficient of X_1X_2 in the left is

$$f_1f_2\left(\alpha_1^{s_1}\alpha_2^{s_2} + \alpha_2^{s_1}\alpha_1^{s_2}\right),$$

and this must be zero since X_1X_2 does not appear in $P_3(\mathbf{X})$. This shows that

$$(\alpha_1/\alpha_2)^{s_1-s_2} = -1,$$

so $s_1 = s_2$. But then $x = y$, which is not allowed.

Observe now that by the corollary to Lemma 3 (proved in Sect. 3) we know that the polynomials $P_i(\mathbf{X})$ are irreducible (as a polynomial in $\mathbb{C}[\mathbf{X}]$). We have that $r_1 \le r_2 \le r_3$. From (21) for $(i, j, h) = (1, 2, 3)$ it follows that $P_h(\mathbf{X})$ divides $P_i(\mathbf{X})$ or $P_j(\mathbf{X})$. By degree considerations, $P_h(\mathbf{X})$ divides $P_j(\mathbf{X})$ (otherwise $r_1 = r_2 = r_3$ and we can take them all to be 1, which is impossible by (P)). So, again by degree considerations, $P_h(\mathbf{X})$ and $P_j(\mathbf{X})$ are associated and $P_i(\mathbf{X})$ is a square which contradicts Lemma 3.

In case (ii) of the theorem, the identification with Laurent-polynomials (e.g. again via Lemma 2.1 in [7]) does not work in the above form. But when α is a unit, then we have the relation $\alpha_1 \cdots \alpha_k = \pm 1$, which allows applying a similar identification as we now explain. We insist again that by Mignotte's result [24] there are no other multiplicative relations between $\alpha_1, \ldots, \alpha_k$. In particular, any $k-1$ of these numbers (e.g. $\alpha_1, \alpha_2, \ldots, \alpha_{k-1}$) are multiplicatively independent. Hence, we may identify $\ell \mapsto \alpha_1^\ell$ by X_1, $\ell \mapsto \alpha_2^\ell$ by X_2 and so forth, which implies that $\ell \mapsto \alpha_k^\ell$ must be identified with $\pm 1/(X_1 \cdots X_{k-1})$. Theorem 1 shows that if we put

$$P_i(\mathbf{X}) = \sum_{j=1}^{k-1} f_j\alpha_j^{s_i}X_j^{r_i} + \frac{f_k\alpha_k^{s_i}}{(X_1\cdots X_{k-1})^{r_i}} - 1 \in K\left[X_1^{\pm 1}, \ldots, X_{k-1}^{\pm 1}\right]$$

for $i = 1, 2, 3$, then for each $h \in \{1, 2, 3\}$ putting i, j for the two indices such that $\{h, i, j\} = \{1, 2, 3\}$, we have that

$$\frac{P_i(\mathbf{X})P_j(\mathbf{X})}{P_h(\mathbf{X})} = Q_h(\mathbf{X})^2, \tag{22}$$

for some $Q_h(\mathbf{X}) \in K[X_1^{\pm 1}, \ldots, X_{k-1}^{\pm 1}]$. We clear on each side denominators and put $P_i'(\mathbf{X}) = P_i(\mathbf{X})(X_1 \cdots X_{k-1})^{r_i} \in K[X_1, \ldots, X_{k-1}]$ for $i = 1, 2, 3$. Then

$$((X_1 \cdots X_{k-1})^{(r_i+r_j-r_h)/2}Q_h(\mathbf{X}))^2 = \frac{P_i'(\mathbf{X})P_j'(\mathbf{X})}{P_h'(\mathbf{X})}.$$

The left-hand side has no non-zero poles at X_i while the right-hand side does not have either a zero or a pole at $X_i = 0$ for $i = 1, \ldots, k-1$, therefore we deduce that $Q_h'(\mathbf{X}) = (X_1 \cdots X_{k-1})^{(r_i+r_j-r_h)/2}Q_h(\mathbf{X})$ is a polynomial. By Lemma 4 the polynomials $P_i'(\mathbf{X}), P_j'(\mathbf{X}), P_h'(\mathbf{X})$ are irreducible (as polynomials in $\mathbb{C}[\mathbf{X}]$). Repeating the arguments from above leads again to the sought contradiction. □

Author details

[1]University of Salzburg, Hellbrunner Str. 34/I, 5020 Salzburg, Austria, [2]School of Mathematics, University of the Witwatersrand, Private Bag X3, Wits 2050, South Africa, [3]Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany, [4]Department of Mathematics, Faculty of Sciences, University of Ostrava, 30 Dubna 22, 701 03 Ostrava 1, Czech Republic.

Acknowlegements

Open access funding provided by Austrian Science Fund. The authors are most grateful to an anonymous referee for very careful reading of the text and for pointing out several inaccuracies which are now corrected in the final version. Clemens Fuchs and Christoph Hutle were supported by FWF (Austrian Science Fund) Grant No. P24574 and by the Sparkling Science Project EMMA Grant No. SPA 05/172. Florian Luca was supported in part by Grant CPRR160325161141 and an A-rated scientist award both from the NRF of South Africa and by Grant No. 17-02804S of the Czech Granting Agency. Part of this work was done when this author was in residence at the Max Planck Institute for Mathematics in Bonn in 2017.

Received: 10 November 2017 Accepted: 5 June 2018
Published online: 25 June 2018

References

1. Alp, M., Irmak, N., Szalay, L.: Balancing Diophantine triples. Acta Univ. Sapientiae Math. **4**, 11–19 (2012)
2. Alp, M., Irmak, N., Szalay, L.: Reduced diophantine quadruples with the binary recurrence $Gn = AG_{n-1} - G_{n-2}$. An. Stiint. Univ. "Ovidius" Constanta Ser. Mat. **23**, 23–31 (2015)
3. Alp, M., Irmak, N., Szalay, L.: Balancing Diophantine triples with distance 1. Period. Math. Hungar. **71**, 1–10 (2015)
4. Alp, M., Irmak, N.: Pellans sequence and its diophantine triples. Publ. Inst. Math. (Beograd) (N.S.) 100(114), 259–269 (2016).
5. Arkin, J., Hoggatt, E., Strauss, E.G.: On Euler's solution of a problem of Diophantus. Fibonacci Quart. **17**, 333–339 (1979)
6. Bertin, M.J., Decomps-Guilloux, A., Grandet-Hugot, M., Pathiaux-Delefosse, M., Schreiber, J.-P.: Pisot and Salem numbers. With a preface by David W. Boyd. Birkhäuser, Basel (1992)
7. Corvaja, P., Zannier, U.: Finiteness of integral values for the ratio of two linear recurrences. Invent. Math. **149**, 431–451 (2002)
8. Dujella, A.: Diophantine *m*-tuples. https://web.math.pmf.unizg.hr/duje/dtuples.html. Accessed 10 Nov, 2017
9. Dujella, A.: There are only finitely many Diophantine quintuples. J. Reine Angew. Math. **566**, 183–214 (2004)
10. Evertse, J.-H.: An improvement of the quantitative Subspace Theorem. Compos. Math. **101**, 225–311 (1996)
11. Evertse, J.H., Schmidt, W.M., Schlickewei, H.P.: Linear equations in variables which lie in a multiplicative group. Ann. Math. **155**(3), 807–836 (2002)
12. Fuchs, C., Luca, F., Szalay, L.: Diophantine triples with values in binary recurrences. Ann. Sc. Norm. Super. Pisa Cl. Sc. (5) **7**, 579–608 (2008)
13. Fuchs, C., Hutle, C., Irmak, N., Luca, F., Szalay, L.: Only finitely many Tribonacci Diophantine triples exist. Math. Slovaca **67**, 853–862 (2017)
14. Fuchs, C., Hutle, C., Luca, F., Szalay, L.: Diophantine triples with values in *k*-generalized Fibonacci sequences. Bull. Malaysian Math. Soc. (2016). https://doi.org/10.1007/s40840-016-0405-4
15. Fuchs, C., Tichy, R.F.: Perfect powers in linear recurrence sequences. Acta Arith. **107**(1), 9–25 (2003)
16. Fuchs, C.: Polynomial-exponential equations and linear recurrences. Glas. Mat. Ser. III **38(58)**(2), 233–252 (2003)
17. Gomez Ruiz, C.A., Luca, F.: Tribonacci Diophantine quadruples. Glas. Mat. Ser. III **50**(1), 17–24 (2015)
18. Gomez Ruiz, C.A., Luca, F.: Diophantine quadruples in the sequence of shifted Tribonacci numbers. Publ. Math. Debrecen **86**(3–4), 473–491 (2015)
19. He, B., Togbé, A., Ziegler, V.: There is no Diophantine quintuple. arXiv:1610.04020. Accessed 10 Nov, 2017
20. Irmak, N., Szalay, L.: Diophantine triples and reduced quadruples with the Lucas sequence of recurrence $u_n = Au_{n-1} - u_{n-2}$. Glas. Mat. Ser. III **49**(69), 303–312 (2014)
21. Luca, F., Munagi, A.O.: Diophantine triples with values in the sequences of Fibonacci and Lucas numbers. Glas. Mat. Ser. III **52**(72), 23–43 (2017)
22. Luca, F., Szalay, L.: Fibonacci Diophantine Triples. Glas. Mat. Ser. III **43**(63), 253–264 (2008)
23. Luca, F., Szalay, L.: Lucas Diophantine Triples. Integers **9**, 441–457 (2009)
24. Mignotte, M.: Sur les conjugués des nombres de Pisot. C. R. Acad. Sci. Paris Sér. I Math. **298**, 21 (1984)
25. Siegel, C.K.: Algebraic numbers whose conjugates lie in the unit circle. Duke Math. J. **11**, 597–602 (1944)