LUCAS DIOPHANTINE TRIPLES

Florian Luca ${ }^{1}$<br>Instituto de Matemáticas UNAM, Morelia, Michoacán, Mexico<br>fluca@matmor.unam.mx<br>László Szalay ${ }^{2}$<br>Institute of Mathematics and Statistics, University of West Hungary, Sopron, Hungary<br>laszalay@ktk.nyme.hu

Received: 1/8/09, Accepted: 5/8/09


#### Abstract

In this paper, we show that the only triple of positive integers $a<b<c$ such that $a b+1, a c+1$ and $b c+1$ are all members of the Lucas sequence $\left(L_{n}\right)_{n \geq 0}$ is $(a, b, c)=(1,2,3)$.


## 1. Introduction

A Diophantine m-tuple is a set $\left\{a_{1}, \ldots, a_{m}\right\}$ of positive rational numbers, or integers, such that $a_{i} a_{j}+1$ is a square for all $1 \leq i<j \leq m$. Diophantus found the rational quadruple $\{1 / 16,33 / 16,17 / 4,105 / 16\}$. Fermat found the first recorded integer quadruple $\{1,3,8,120\}$. Infinitely many Diophantine quadruples of integers are known and it is conjectured that there is no Diophantine quintuple. By results of Dujella [4], it is now known that there is no Diophantine sextuple and there can be at most finitely many Diophantine quintuples which are all effectively computable. In the rational case, it is not known if the size $m$ of the Diophantine $m$-tuples must be universally bounded. A few examples with $m=6$ are known by the work of Gibbs [7]. Several generalizations of this problem, when the squares are replaced by higher powers of fixed, or variable exponents, were treated in many papers (see [1], [2], [8], [9]) and [10]).

In the paper [6], the following variant of this problem was treated. Let $\left(u_{n}\right)_{n \geq 0}$ be a binary recurrent sequence of integers satisfying the recurrence

$$
u_{n+2}=r u_{n+1}+s u_{n} \quad \text { for all } n \geq 0
$$

Here, $r$ and $s$ are nonzero integers satisfying the condition that $\Delta=r^{2}+4 s \neq 0$. It is then well-known that if we write $\alpha$ and $\beta$ for the two distinct roots of the characteristic equation $x^{2}-r x-s=0$, then there exist constants $\gamma, \delta \in \mathbb{Q}[\alpha]$ such that

$$
\begin{equation*}
u_{n}=\gamma \alpha^{n}+\delta \beta^{n} \quad \text { holds for all } n \geq 0 \tag{1}
\end{equation*}
$$

[^0]Assume further that the sequence $\left(u_{n}\right)_{n \geq 0}$ is nondegenerate in the sense that $\gamma \delta \neq 0$ and $\alpha / \beta$ is not root of unity. Say that the positive integers $a<b<c$ form $a$ Diophantine triple with values in the set $\mathcal{U}=\left\{u_{n}: n \geq 0\right\}$ if $a b+1, a c+1$ and $b c+1$ are all three in $\mathcal{U}$. Note, for example, that if $u_{n}=2^{n}+1$ for all $n \geq 0$ (i.e., $(r, s)=(3,-2)$ and $\left.\left(u_{0}, u_{1}\right)=(2,3)\right)$, then there are infinitely many such triples (namely, just take $a<b<c$ to be all three powers of two). The main result in [6] shows that the above example is representative for the nondegenerate binary recurrent sequences $\left(u_{n}\right)_{n \geq 0}$ with real roots $\alpha$ and $\beta$ for which there exist infinitely many Diophantine triples with values in $\mathcal{U}$. The precise result proved there is the following.

Theorem 1. Assume that $\left(u_{n}\right)_{n \geq 0}$ is a nondegenerate binary recurrence sequence with $\Delta>0$ such that there exist infinitely many sextuples of nonnegative integers ( $a, b, c ; x, y, z$ ) with $1 \leq a<b<c$ satisfying

$$
\begin{equation*}
a b+1=u_{x}, \quad a c+1=u_{y} \quad \text { and } \quad b c+1=u_{z} \tag{2}
\end{equation*}
$$

Then $\beta \in\{ \pm 1\}, \delta \in\{ \pm 1\}, \alpha, \gamma \in \mathbb{Z}$. Furthermore, for all but finitely many of the sextuples ( $a, b, c ; x, y, z$ ) as above one has $\delta \beta^{z}=\delta \beta^{y}=1$ and one of the following holds:
(i) $\delta \beta^{x}=1$. In this case, one of $\delta$ or $\delta \alpha$ is a perfect square;
(ii) $\delta \beta^{x}=-1$. In this case, $x \in\{0,1\}$.

No finiteness result was proved for the case when $\Delta<0$. The proof of Theorem 1 uses deep results from Diophantine approximation such as the subspace theorem, the finiteness of the number of nondegenerate solutions of unit equations with variables in a finitely generated multiplicative group of $\mathbb{C}^{*}$, as well as nontrivial bounds for the greatest common divisor of values of two rational functions at unit points in the number fields setting. Due to the ineffective nature of the results used in the proof of Theorem 1, the proof of this theorem is also ineffective in the sense that given a nondegenerate binary recurrent sequence $\left(u_{n}\right)_{\geq 0}$ for which Theorem 1 guarantees the existence of only finitely many Diophantine triples with values in the set $\mathcal{U}$, we do not know how to actually compute all such triples.

As usual, let $\left(F_{n}\right)_{n \geq 0}$ and $\left(L_{n}\right)_{n \geq 0}$ be the sequences of Fibonacci and Lucas numbers given by $F_{0}=0, F_{1}=1, L_{0}=2, L_{1}=1$ and by the recurrence relations

$$
F_{n+2}=F_{n+1}+F_{n} \quad \text { and } \quad L_{n+2}=L_{n+1}+L_{n} \quad \text { for all } n \geq 0
$$

respectively. Putting $\alpha=(1+\sqrt{5}) / 2$ and $\beta=(1-\sqrt{5}) / 2=-1 / \alpha$ for the two roots of the common characteristic equation $x^{2}-x-1=0$ of the sequences of Fi bonacci and Lucas numbers, the formulae (1) of the general terms of these particular
sequences are

$$
\begin{equation*}
F_{n}=\frac{\alpha^{n}-\beta^{n}}{\alpha-\beta} \quad \text { and } \quad L_{n}=\alpha^{n}+\beta^{n} \tag{3}
\end{equation*}
$$

for all $n \geq 0$, respectively.
According to Theorem 1, there should be only finitely many triples of distinct positive integers $\{a, b, c\}$ such that $a b+1, a c+1$ and $b c+1$ are either all three Fibonacci numbers or all three Lucas numbers. In [12], we showed that there is no such triple for the case of the Fibonacci sequence. In this paper, we deal with the same problem for the case of the Lucas sequence. Our main result says that there is only one such triple.

Theorem 2. The only positive integers $a<b<c$ such that

$$
\begin{equation*}
a b+1=L_{x}, \quad a c+1=L_{y} \quad \text { and } \quad b c+1=L_{z} \tag{4}
\end{equation*}
$$

hold with some positive integers $x, y$ and $z$ are $(a, b, c)=(1,2,3)$.

In [12], the crucial point of the proof for the case of the Fibonacci sequence was the existence of a factorization of $F_{n}-1$ (see Lemma 6) in terms of smaller Fibonacci and Lucas numbers. Here, the case of the Lucas numbers is more complicated since such a factorization of $L_{n}-1$ exists if and only if $n$ is odd. To deal with the remaining situation, we proved that $L_{n}-1$ divides $F_{3 n}$ (see Lemma 13). This relation can be usefully applied and the bounds we obtain have similar size as the bounds obtained in the case of the Fibonacci numbers.

Allowing equalities, namely $0 \leq a \leq b \leq c$, we additionally gain only trivial solutions. Indeed, applying the result of Finkelstein [5] related to the Lucas numbers of the form $k^{2}+1$, it follows easily that either $(x, y, z ; a, b, c)=\left(0, t, t ; 1,1, L_{t}-1\right)$, or $(x, y, z)=(1,1,1), a=b=0$, and $c$ is arbitrary. If we allow $a=0$, then we obtain $x=y=1$, and $(x, y, z ; a, b, c)=(1,1, s ; 0, b, c)$, where $b c=L_{s}-1$. This is why we only deal with the case $0<a<b<c$.

Thus, in the sequel, we only examine system (4) under the conditions

$$
\begin{equation*}
2 \leq x<y<z \quad \text { and } \quad 1 \leq a<b<c \tag{5}
\end{equation*}
$$

Note also that there is at least one additional rational solution with $0<a<b<c$, namely

$$
(a, b, c ; x, y, z)=\left(\frac{2}{5}, 5,15 ; 2,4,9\right)
$$

It would be interesting to decide whether equations (4) have only finitely many positive rational solutions $(a, b, c ; x, y, z)$, and in the affirmative case whether the above one is the only one.

There are many identities involving Fibonacci and Lucas numbers. For the sake of brevity, we introduce the notation $E_{n}$ for the $n$th term of either the Fibonacci or the

Lucas sequence. Further, we let $\delta_{e}$ equal 5 if we are dealing with Fibonacci numbers, and equal 1 if we are dealing with Lucas numbers. Finally, we write $\overline{E_{n}}$ to mean the $n$th term of the complimentary sequence (i.e., $\overline{F_{n}}=L_{n}$ and vice versa).

As an example of our notation, the second statement of Lemma 6 for $n$ odd is reformulated as $L_{n}-1=\delta_{e} E_{\frac{n-1}{2}} E_{\frac{n+1}{2}}$. In the sequel, we will exploit the advantages of the notation $E_{n}, \overline{E_{n}}$ and $\delta_{e}$.

Before proving our main result, Theorem 2, we remark that the auxiliary results used throughout its proof, namely Lemmas 1-10, are located in the last section.

## 2. The Proof of Theorem 2

Case 1. $z \leq 98$
In this case, we ran an exhaustive computer search to detect all the positive integer solutions of system (4). Observe that we have

$$
a=\sqrt{\frac{\left(L_{x}-1\right)\left(L_{y}-1\right)}{L_{z}-1}}, \quad 2 \leq x<y<z \leq 98
$$

Going through all possible values for $x, y$ and $z$ and checking if the above number $a$ is an integer, we found only the triple $(x, y, z)=(2,3,4)$.

Case 2. $z \geq 99$
We distinguish four main cases depending on the parities of the indices $y$ and $z$.

### 2.1. Both y and z Are Odd

Here, we recall the method developed in [12] to deal with the Fibonacci Diophantine triples. Put $G=\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right)$. Since $y$ and $z$ are odd, by Lemma 6, we have

$$
G=\left\{\begin{array}{lll}
\operatorname{gcd}\left(5 F_{\frac{y-1}{2}} F_{\frac{y+1}{2}}, 5 F_{\frac{z-1}{2}} F_{\frac{z+1}{2}}\right) & \text { if } y, z \equiv 1 \quad(\bmod 4),  \tag{6}\\
\operatorname{gcd}\left(5 F_{\frac{y-1}{2}} F_{\frac{y+1}{2}}, L_{\frac{z-1}{2}} L_{\frac{z+1}{2}}\right) & \text { if } y \equiv 1 \quad(\bmod 4), z \equiv 3 \quad(\bmod 4), \\
\operatorname{gcd}\left(L_{\frac{y-1}{2}} L_{\frac{y+1}{2}}, 5 F_{\frac{z-1}{2}} F_{\frac{z+1}{2}}\right) & \text { if } y \equiv 3 \quad(\bmod 4), z \equiv 1 \quad(\bmod 4), \\
\operatorname{gcd}\left(L_{\frac{y-1}{2}} L_{\frac{y+1}{2}}, L_{\frac{z-1}{2}} L_{\frac{z+1}{2}}\right) & \text { if } y, z \equiv 3 \quad(\bmod 4)
\end{array}\right.
$$

The lower three branches can be joined since 5 does not divide $L_{n}$ for any $n \geq 0$ (see Lemma 3). Therefore, it remains to investigate the following two cases:

$$
G \leq\left\{\begin{array}{c}
G_{1}=5 \operatorname{gcd}\left(F_{\frac{y-1}{2}}, F_{\frac{z-1}{2}}\right) \operatorname{gcd}\left(F_{\frac{y-1}{2}}, F_{\frac{z+1}{2}}\right)  \tag{7}\\
\times \operatorname{gcd}\left(F_{\frac{y+1}{2}}, F_{\frac{z-1}{2}}\right) \operatorname{gcd}\left(F_{\frac{y+1}{2}}, F_{\frac{z+1}{2}}\right) \\
G_{234}=\operatorname{gcd}\left(A_{\frac{y-1}{2}}, B_{\frac{z-1}{2}}\right) \operatorname{gcd}\left(A_{\frac{y-1}{2}}, B_{\frac{z+1}{2}}\right) \\
\times \operatorname{gcd}\left(A_{\frac{y+1}{2}}, B_{\frac{z-1}{2}}\right) \operatorname{gcd}\left(A_{\frac{y+1}{2}}, B_{\frac{z+1}{2}}\right)
\end{array}\right.
$$

where $\left(A_{u}, B_{v}\right)$ equals either $\left(E_{u}, \bar{E}_{v}\right)$, or $\left(L_{u}, L_{v}\right)$. In the sequel, we prove upper bounds on $\operatorname{gcd}\left(A_{u}, B_{v}\right)$. Recalling Lemma 5 , the above number is 1,2 , or a term of the Lucas sequence. Since we are interested only in upper bounds, we may ignore the values 1 or 2 provided that we work with an upper bound which is at least $L_{2}=3$.

We now apply Lemma 5 in (7) to conclude that

$$
\begin{aligned}
G_{1} & =5 F_{\operatorname{gcd}\left(\frac{y-1}{2}, \frac{z-1}{2}\right)} F_{\operatorname{gcd}\left(\frac{y-1}{2}, \frac{z+1}{2}\right)} F_{\operatorname{gcd}\left(\frac{y+1}{2}, \frac{z-1}{2}\right)} F_{\operatorname{gcd}\left(\frac{y+1}{2}, \frac{z+1}{2}\right)} \\
G_{234} & \leq G_{2}=L_{\operatorname{gcd}\left(\frac{y-1}{2}, \frac{z-1}{2}\right)} L_{\operatorname{gcd}\left(\frac{y-1}{2}, \frac{z+1}{2}\right)} L_{\operatorname{gcd}\left(\frac{y+1}{2}, \frac{z-1}{2}\right)} L_{\operatorname{gcd}\left(\frac{y+1}{2}, \frac{z+1}{2}\right)}
\end{aligned}
$$

which, together with $F_{n} \leq L_{n}$, yield $G \leq 5 G_{2}$.
Put
$\operatorname{gcd}\left(\frac{y \mp 1}{2}, \frac{z-1}{2}\right)=\frac{z-1}{2 d_{\mp 1}} \quad$ and $\quad \operatorname{gcd}\left(\frac{y \mp 1}{2}, \frac{z+1}{2}\right)=\frac{z+1}{2 d_{\mp 2}} \quad$,
respectively. If all the four $d$ 's above are at least 5 , then we use Lemma 7 with $u_{0}=z_{0}>8$ and Lemma 9 with $(a, b)=(5,0)$, to derive that $\varepsilon_{1}<0.01, \kappa<3.35$, and

$$
\begin{equation*}
G \leq 5 G_{2} \leq 5 L_{\frac{z+1}{10}}^{4}<5\left(\alpha^{\frac{z+1}{10}+0.01}\right)^{4}<\alpha^{\frac{2}{5} z+3.79} \tag{9}
\end{equation*}
$$

Combining the above inequality with Lemma 12, we get the inequality

$$
\frac{z}{2}-0.01<\frac{2}{5} z+3.79
$$

which leads to the contradiction $z<38$.
Suppose now, that one of $d_{-1}, d_{+1}, d_{-2}$ and $d_{+2}$ is at most 4. For simplicity, write $d \in\{1,2,3,4\}$.

One of the factors of $G_{2}$ may be large since $\operatorname{gcd}\left(\frac{z+\eta_{1}}{2}, \frac{y+\eta_{2}}{2}\right)=\frac{z+\eta_{1}}{2 d}$ for some $\eta_{1}, \eta_{2} \in\{ \pm 1\}$. We now proceed to show that the other three factors of $G_{2}$ are small. Fixing $\eta_{1}$ and $\eta_{2}$, it follows that there exists a positive integer $c$ coprime to $d$ such that

$$
\begin{equation*}
\frac{y+\eta_{2}}{2}=c \frac{z+\eta_{1}}{2 d} \tag{10}
\end{equation*}
$$

Observe that the only possibilities for the pair $(d, c)$ are:

$$
\begin{equation*}
(d, c)=\underbrace{(4,1),(3,1)}_{\text {group } 1}, \underbrace{(4,3),(3,2),(2,1)}_{\text {group } 2},(1,1) . \tag{11}
\end{equation*}
$$

The groups arranged in (11) are motivated by the forthcoming treatment.

Part 2.1.1: Group $1(d=4$ or 3 , and $c=1)$.
From (10) and Lemma 11, we get that

$$
z=\frac{d}{c}\left(y+\eta_{2}\right)-\eta_{1}=d\left(y+\eta_{2}\right)-\eta_{1} \leq 2 y
$$

Hence, $(d-2) y \leq \eta_{1}-d \eta_{2}$. By Lemma 11 again, we obtain

$$
z \leq \frac{2\left(\eta_{1}-d \eta_{2}\right)}{d-2} \leq \frac{2(d+1)}{d-2} \leq 8
$$

Thus, $z$ is too small.

Part 2.1.2: Group $2((d, c)=(4,3),(3,2),(2,1))$.
Here, (10) implies $y=\frac{c z+c \eta_{1}-d \eta_{2}}{d}$. Put $\eta_{1}^{\prime}, \eta_{2}^{\prime} \in\{ \pm 1\}$ such that $\left(\eta_{1}^{\prime}, \eta_{2}^{\prime}\right) \neq\left(\eta_{1}, \eta_{2}\right)$. Then

$$
\frac{y+\eta_{2}^{\prime}}{2}=\frac{c z+c \eta_{1}-d \eta_{2}+d \eta_{2}^{\prime}}{2 d}
$$

Using the fact that $d=c+1$ and Lemma 10 with $\lambda=c$, we get

$$
\begin{aligned}
\operatorname{gcd}\left(\frac{z+\eta_{1}^{\prime}}{2}, \frac{y+\eta_{2}^{\prime}}{2}\right) & =\operatorname{gcd}\left(\frac{z+\eta_{1}^{\prime}}{2}, \frac{c z+c \eta_{1}-d \eta_{2}+d \eta_{2}^{\prime}}{2 d}\right) \\
& \leq\left|\frac{c \eta_{1}^{\prime}-\left(c \eta_{1}-d \eta_{2}+d \eta_{2}^{\prime}\right)}{2}\right| \\
& \leq c+d \leq 7
\end{aligned}
$$

Here, we used that the numerator is nonzero. To see that this is indeed so, observe that by assuming that it were zero we would get $c \eta_{1}^{\prime}-\left(c \eta_{1}-d \eta_{2}+d \eta_{2}^{\prime}\right)=0$, leading to $c\left(\eta_{1}^{\prime}-\eta_{1}\right)=d\left(\eta_{2}^{\prime}-\eta_{2}\right)$, which contradicts the fact that $\left(\eta_{1}^{\prime}, \eta_{2}^{\prime}\right) \neq\left(\eta_{1}, \eta_{2}\right)$. We now have

$$
\alpha^{\frac{z}{2}-0.01}<5 L_{\frac{z+\eta_{1}}{2 d}} L_{c+d}^{3} \leq 5 \alpha^{\frac{z+1}{2 d}+0.01} L_{7}^{3}<\alpha^{\frac{z}{2 d}+24.6}
$$

where we used the fact that $\frac{1}{2 d} \leq 0.25$. In the above inequality, we used Lemma 9 with $a=5 L_{7}^{3}$ and $\kappa<24.34$. Thus,

$$
\frac{z}{2}-0.01<\frac{z}{2 d}+24.6
$$

and the last inequality above leads to $z<\frac{24.61 \cdot 2 d}{d-1} \leq 98.44$, which is not the case is being considered now.

Part 2.1.3: $d=1$ and $c=1$.
Here,

$$
\frac{z+\eta_{1}}{2}=\frac{y+\eta_{2}}{2}
$$

yields $z=y+\eta_{2}-\eta_{1}$. Since $y<z$, we get that $z=y+2$. In particular, $y \not \equiv z(\bmod 4)$. Therefore, by (6) together with the fact that $5 \nmid L_{n}$, we get that $\operatorname{gcd}\left(L_{z-2}-1, L_{z}-1\right)$ does not exceed

$$
\begin{equation*}
\operatorname{gcd}\left(E_{\frac{z-3}{2}}, \bar{E}_{\frac{z-1}{2}}\right) \operatorname{gcd}\left(E_{\frac{z-3}{2}}, \bar{E}_{\frac{z+1}{2}}\right) \operatorname{gcd}\left(E_{\frac{z-1}{2}}, \bar{E}_{\frac{z-1}{2}}\right) \operatorname{gcd}\left(E_{\frac{z-1}{2}}, \bar{E}_{\frac{z+1}{2}}\right) \tag{12}
\end{equation*}
$$

Thus, by Lemmas 5 and 12, we get
$\alpha^{\frac{z}{2}-0.01}<\operatorname{gcd}\left(L_{z-2}-1, L_{z}-1\right) \leq \max \left\{L_{1}, 2\right\} \cdot \max \left\{L_{2}, 2\right\} \cdot 2 \cdot \max \left\{L_{1}, 2\right\}=24$,
leading to $z<13.3$, which is again too small.

### 2.2. Both y and z Are Even

By Lemmas 5 and 13, we have

$$
\begin{equation*}
\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right) \leq \operatorname{gcd}\left(F_{3 y}, F_{3 z}\right)=F_{\operatorname{gcd}(3 y, 3 z)}=F_{3 \operatorname{gcd}(y, z)} \tag{13}
\end{equation*}
$$

Put $d=\operatorname{gcd}(y, z), y=d y_{1}, z=d z_{1}$, where $d$ is even. Furthermore, $y_{1}$ and $z_{1}$ are coprime.

Part 2.2.1: $d \leq z / 7$.
In this case, Lemma 7 (with $\delta_{1}<-1.67$ ), Lemma 12, and relation (13), imply the contradiction

$$
\alpha^{\frac{z}{2}-0.01}<\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right) \leq F_{\frac{3 z}{7}}<\alpha^{\frac{3 z}{7}-1.67}
$$

Part 2.2.2: $d>z / 7$.
The above condition is equivalent to $z_{1}=\frac{z}{d} \leq 6$. On the other hand, the condition $d=\operatorname{gcd}(y, z) \leq y<z$ implies that $2 \leq z_{1}$. Thus, in order to get an upper bound on the greatest common divisor of $L_{y_{1} d}-1$ and $L_{z_{1} d}-1$, it is sufficient to consider the pairs $\left(y_{1}, z_{1}\right)$ with coprime components, where $z_{1}=2,3, \ldots, 6$ and $y_{1}=\left\lceil z_{1} / 2\right\rceil, \ldots, z_{1}-1$. Note that, by Lemma 11, we have that $\left\lceil z_{1} / 2\right\rceil \leq y_{1}$. Since $d$ is even, we have that $L_{d}=\alpha^{d}+\alpha^{-d}$. Furthermore, for any positive integer $k$ there exists a polynomial $C_{k}(t) \in \mathbb{Z}[t]$ such that $L_{k d}=C_{k}\left(L_{d}\right)$. Indeed, $C_{0}(t)=2$ since $L_{0 \cdot d}=2$. Since $L_{1 \cdot d}=L_{d}$, we have that $C_{1}(t)=t$. Moreover,

$$
\alpha^{(k+1) d}+\alpha^{-(k+1) d}=\left(\alpha^{k d}+\alpha^{-k d}\right)\left(\alpha^{d}+\alpha^{-d}\right)-\left(\alpha^{(k-1) d}+\alpha^{-(k-1) d}\right)
$$

provides the second order recurrence relation $C_{k+1}(t)=t C_{k}(t)-C_{k-1}(t)$. The resulting polynomials are called Cardan polynomials $C_{k}(t)$ (see, for instance [13]). It is worth noticing that if $T_{n}(t)$ denotes the $n t h$ Chebyshev polynomial, then $C_{k}(t)=$ $2 T_{k}(t / 2)$.

Table 1 gives the Cardan polynomials $C_{k}(t)$ for those values of $k$ in the range $0 \leq k \leq 12$ which are of interest to us here and in the forthcoming subsections.

| $k$ | $C_{k}(t)$ |
| :---: | :--- |
| 1 | $t$ |
| 2 | $t^{2}-2$ |
| 3 | $t^{3}-3 t$ |
| 4 | $t^{4}-4 t^{2}+2$ |
| 5 | $t^{5}-5 t^{3}-5 t$ |
| 6 | $t^{6}-6 t^{4}+9 t^{2}-2$ |
| 7 | $t^{7}-7 t^{5}+14 t^{3}-7 t$ |
| 11 | $t^{11}-11 t^{9}+44 t^{7}-77 t^{5}+55 t^{3}-11 t$ |
| 12 | $t^{12}-12 t^{10}+54 t^{8}-112 t^{6}+105 t^{4}-36 t^{2}+2$ |

Table 1: Polynomials $C_{k}(t)$

We next determine the greatest common divisor of the values of two Cardan polynomials shifted by -1 , since

$$
\begin{equation*}
\operatorname{gcd}\left(L_{d y_{1}}-1, L_{d z_{1}}-1\right)=\operatorname{gcd}\left(C_{y_{1}}\left(L_{d}\right)-1, C_{z_{1}}\left(L_{d}\right)-1\right) \tag{14}
\end{equation*}
$$

Consider the greatest common divisor $\operatorname{gcd}_{\mathrm{pol}}\left(C_{y_{1}}(t)-1, C_{z_{1}}(t)-1\right)$ of the two polynomials $C_{y_{1}}(t)-1$ and $C_{z_{1}}(t)-1$. This can be determined by applying the Euclidean algorithm for polynomials with rational coefficients. If we write $\operatorname{gcd}_{\mathrm{pol}}\left(C_{y_{1}}(t)-\right.$ $\left.1, C_{z_{1}}(t)-1\right)=\gamma D(t)$, where $\gamma \in \mathbb{Q}$ and $D(t) \in \mathbb{Z}[t]$ is a primitive polynomial, then

$$
\operatorname{gcd}\left(C_{y_{1}}\left(L_{d}\right)-1, C_{z_{1}}\left(L_{d}\right)-1\right) \mid \operatorname{num}(|\gamma|) D\left(L_{d}\right)
$$

where num $(|\gamma|)$ denotes the absolute value of the numerator of the rational number $\gamma$.

| $\left(z_{1}, y_{1}\right)$ | $(2,1)$ | $(3,2)$ | $(4,3)$ | $(5,3)$ | $(5,4)$ | $(6,5)$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\operatorname{gcd}_{\mathrm{pol}}$ | -2 | -1 | 1 | 3 | 2 | 1 |

Table 2: $\operatorname{gcd}_{p o l}\left(C_{z_{1}}(t)-1, C_{y_{1}}(t)-1\right)$ provided by the Euclidean algorithm

Table 2 shows the values of $\operatorname{gcd}_{p o l}\left(C_{z_{1}}(t)-1, C_{y_{1}}(t)-1\right)$ provided by Euclidean algorithm for the possible pairs $\left(y_{1}, z_{1}\right)$ that are of interest for us. In all the six cases,
we find $D(t)=1$ and num $|\gamma| \leq 3$. Thus, we can conclude

$$
\begin{equation*}
\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right)=\operatorname{gcd}\left(L_{y_{1} d}-1, L_{z_{1} d}-1\right) \leq 3 \tag{15}
\end{equation*}
$$

Comparing this relation to Lemma 12, we get the contradiction $z<4.6$.

## 2.3. y is Odd and z is Even

It follows, from Lemmas 3, 6 and 13, that

$$
\begin{align*}
\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right) & \leq \operatorname{gcd}\left(\delta_{e} E_{\frac{y-1}{2}} E_{\frac{y+1}{2}}, F_{3 z}\right) \\
& \leq \delta_{e} \operatorname{gcd}\left(E_{\frac{y-1}{2}}, F_{3 z}\right) \operatorname{gcd}\left(E_{\frac{y+1}{2}}, F_{3 z}\right) \\
& \leq \sqrt{5} L_{\operatorname{gcd}\left(\frac{y-1}{2}, 3 z\right)} L_{\operatorname{gcd}\left(\frac{y+1}{2}, 3 z\right)} \tag{16}
\end{align*}
$$

The last inequality in (16) holds by Lemma 4 when $E_{n}=F_{n}$ (i.e., when $\delta_{e}=5$ ), and it is trivial when $E_{n}=L_{n}$ (i.e., $\delta_{e}=1$ ). In both these cases we have also used Lemma 5.

Next let us write

$$
\begin{equation*}
\operatorname{gcd}\left(\frac{y-1}{2}, 3 z\right)=\frac{3 z}{d_{1}} \quad \text { and } \quad \operatorname{gcd}\left(\frac{y+1}{2}, 3 z\right)=\frac{3 z}{d_{2}} \tag{17}
\end{equation*}
$$

Furthermore, let us write

$$
\begin{equation*}
\frac{y-1}{2}=c_{1} \frac{3 z}{d_{1}} \quad \text { and } \quad \frac{y+1}{2}=c_{2} \frac{3 z}{d_{2}} \tag{18}
\end{equation*}
$$

where $\operatorname{gcd}\left(c_{i}, d_{i}\right)=1$ for $i=1,2$. By Lemma 11, we have that $z / 2 \leq y<z$. Together with the fact that $y=\frac{6 c_{1}}{d_{1}} z+1$, and $y=\frac{6 c_{2}}{d_{2}} z-1$, respectively, we get

$$
\begin{equation*}
\frac{19}{240} d_{1}<c_{1}<\frac{1}{6} d_{1} \quad \text { and } \quad \frac{1}{12} d_{2}<c_{2} \leq \frac{1}{6} d_{2} \tag{19}
\end{equation*}
$$

where the lower bound on $c_{1}$ holds because $z>40$.

Part 2.3.1: $d_{i} \geq 13$ for $i=1,2$.
By Lemmas 7 and 12, together with inequality (16), we derive

$$
\alpha^{\frac{z}{2}-0.01}<\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right) \leq \sqrt{5} L_{\frac{3 z}{13}}^{2}<\sqrt{5}\left(\alpha^{\frac{3 z}{13}+0.01}\right)^{2}<\alpha^{\frac{6 z}{13}+1.7}
$$

This leads to the contradiction $z<44.5$.

Part 2.3.2: $1 \leq d_{1} \leq 12$, or $1 \leq d_{2} \leq 12$.
Here, we return to the direct estimate of the upper bound on $\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right)$. First, $d_{1}>6$ since if $d_{1} \leq 6$, then there is no positive integer $c_{1}$ satisfying relations (19). Similar arguments show that $d_{2} \geq 6$. Again by estimates (19) together with the condition that $d_{i} \leq 12$ for some $i=1,2$, it follows that $c_{1}=1$, and $c_{2} \leq 2$, respectively. Recall, that $\operatorname{gcd}\left(c_{i}, d_{i}\right)=1$ for $i=1$, 2 , which excludes the pair $\left(c_{2}, d_{2}\right)=(2,12)$. Thus $c_{2}=1$, also holds. Put $\varepsilon_{i}=(-1)^{i}$ for $i=1,2$. Then the relation $\frac{y+\varepsilon_{i}}{2}=\frac{3 c_{i}}{d_{i}} z$ implies that $y=\frac{6 c_{i}}{d_{i}} z-\varepsilon_{i}$. Putting $\operatorname{gcd}\left(6 c_{i}, d_{i}\right)=f_{i}$, it follows that we can write $6 c_{i}=a f_{i}$ and $d_{i}=b f_{i}$ with $\operatorname{gcd}(a, b)=1$. Clearly, $y=\frac{a}{b} z-\varepsilon_{i}$, where the possible fractions $\frac{a}{b}$ are

$$
\begin{equation*}
\frac{a}{b}=\frac{1}{1}, \frac{6}{7}, \frac{3}{4}, \frac{2}{3}, \frac{3}{5}, \frac{6}{11}, \frac{1}{2} \tag{20}
\end{equation*}
$$

Most of the fractions shown in (20) occur for both $i=1$ and $i=2$ except for $\frac{1}{1}$ and $\frac{1}{2}$ which appear only if $i=2$, and $i=1$, respectively.

Since $y$ is odd, we get that $\frac{a}{b} z$ is even. There exist a positive even integer $s$ such that $z=b s$. For $b$ odd (i.e., $b=1,7,3,5,11$ ) this is trivial, while for $b$ even (i.e., $b=4,2$ ) this comes from the fact that $a$ is odd and the integer $\frac{a}{b} z$ even; thus, entailing that $b$ is divisible by a smaller power of 2 than $z$ is.

After these preparations, we are ready to give an upper bound on the number

$$
W:=\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right)=\operatorname{gcd}\left(L_{\frac{a}{b} z-\varepsilon_{i}}-1, L_{z}-1\right)
$$

We start with

$$
\begin{align*}
W & =\operatorname{gcd}\left(L_{a s-\varepsilon_{i}}-1, L_{b s}-1\right)=\operatorname{gcd}\left(\delta_{e} E_{\frac{a s}{2}} E_{\frac{a s}{2}-\varepsilon_{i}}, L_{b s}-1\right) \\
& =\operatorname{gcd}\left(E_{\frac{a s}{2}}, L_{b s}-1\right) \operatorname{gcd}\left(E_{\frac{a s}{2}-\varepsilon_{i}}, L_{b s}-1\right)=: W_{1} W_{2} \tag{21}
\end{align*}
$$

In the above, we used the fact that $5 \not \backslash\left(L_{b s}-1\right)$ and $\operatorname{gcd}\left(E_{\frac{a s}{2}}, E_{\frac{a s}{2}-\varepsilon_{i}}\right)=1$.
Observe that $\left.E_{\frac{a s}{2}} \right\rvert\, F_{a s}$. Thus, the first factor $W_{1}=\operatorname{gcd}\left(E_{\frac{a s}{2}}, L_{b s}-1\right)$ of the rightmost product in formula (21) is at most

$$
\begin{align*}
\operatorname{gcd}\left(F_{a s}, L_{b s}-1\right) & \leq \operatorname{gcd}\left(5 F_{a s}^{2}, L_{b s}-1\right)=\operatorname{gcd}\left(L_{a s}^{2}-4, L_{b s}-1\right) \\
& =\operatorname{gcd}\left(C_{a}^{2}(s)-4, C_{b}(s)-1\right) \tag{22}
\end{align*}
$$

Next, we follow the procedure involving shifted Cardan polynomials from Part 2.2. Table 3 gives the greatest common divisor of the polynomials $C_{a}^{2}(t)-4$ and $C_{b}(t)-1$.

We now distinguish two cases. If $\operatorname{gcd}_{p o l}$ is constant, then $W_{1} \leq$ num $|\gamma| \leq 3$. When $\operatorname{gcd}_{p o l}$ is linear, then num $|\gamma| \leq 11$, and therefore $W_{1} \leq 11\left(L_{s}-1\right)<11 L_{s}$ (here, clearly, $b \geq 5$ ). Obviously, the second bound on $W_{1}$ is larger.

| $(a, b)$ | $(1,1)$ | $(6,7)$ | $(3,4)$ | $(2,3)$ | $(3,5)$ | $(6,11)$ | $(1,2)$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\operatorname{gcd}_{p o l}$ | -3 | $\frac{7}{9}(t-1)$ | -2 | $-\frac{3}{4}$ | $-\frac{5}{4}(t-1)$ | $-\frac{11}{16}(t-1)$ | -1 |

Table 3: The polynomials $\operatorname{gcd}_{p o l}\left(C_{a}^{2}(t)-4, C_{b}(t)-1\right)$ provided by the Euclidean algorithm

We continue with an upper bound on the second factor $W_{2}=\operatorname{gcd}\left(E_{\frac{a s}{2}-\varepsilon_{i}}, L_{b s}-\right.$ 1). Using Lemma 13, we have

$$
\begin{equation*}
W_{2} \leq \operatorname{gcd}\left(E_{\frac{a s}{2}-\varepsilon_{i}}, F_{3 b s}\right) \leq \operatorname{gcd}\left(E_{\frac{a s}{2}-\varepsilon_{i}}, F_{3 b s}\right)=E_{\operatorname{gcd}\left(\frac{a s}{2}-\varepsilon_{i}, 3 b s\right)} \tag{23}
\end{equation*}
$$

Recall that $s=2 r$ is even and $6 c_{i}=a f_{1}$. Thus,

$$
\begin{aligned}
\operatorname{gcd}\left(\frac{a s}{2}-\varepsilon_{i}, 3 b s\right) & =\operatorname{gcd}\left(a r-\varepsilon_{i}, 6 b r\right) \leq \operatorname{gcd}\left(6 c_{i} r-\varepsilon_{i} f_{1}, 6 c_{i} b r\right) \\
& =\operatorname{gcd}\left(6 c_{i} r-\varepsilon_{i} f_{1}, \varepsilon_{i} f_{1} b\right) \\
& \leq f_{1} b=d_{i} \leq 17
\end{aligned}
$$

Consequently, by (23), we get that $W_{2} \leq E_{17} \leq L_{17}$. Thus, by Lemma 12 , we have

$$
\alpha^{\frac{z}{2}-0.01}<\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right)<L_{17} \cdot 11 L_{s}<\alpha^{s+0.01+\kappa}
$$

where we can take $\kappa<22$. Since $s=\frac{z}{b}$ and $b \geq 5$ (see Table 3), we obtain $z<71.5$.

## 2.4. $y$ is Even and $z$ is Odd

This is similar to the procedure explained in Section 2.3 , so we shall only emphasize the differences from that case, and omit some of the obvious details.

By Lemmas 3, 6 and 13, we get

$$
\begin{align*}
\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right) & \leq \operatorname{gcd}\left(F_{3 y}, \delta_{e} E_{\frac{z-1}{2}} E_{\frac{z+1}{2}}\right) \\
& \leq \delta_{e} \operatorname{gcd}\left(F_{3 y}, E_{\frac{z-1}{2}}\right) \operatorname{gcd}\left(F_{3 y}, E_{\frac{z+1}{2}}\right) \\
& \leq \sqrt{5} L_{\operatorname{gcd}\left(3 y, \frac{z-1}{2}\right)} L_{\operatorname{gcd}\left(3 y, \frac{z+1}{2}\right)} \tag{24}
\end{align*}
$$

We write again, as in the previous case,

$$
\begin{equation*}
\operatorname{gcd}\left(3 y, \frac{z-1}{2}\right)=\frac{z-1}{2 d_{1}} \quad \text { and } \quad \operatorname{gcd}\left(3 y, \frac{z+1}{2}\right)=\frac{z+1}{2 d_{2}} \tag{25}
\end{equation*}
$$

and put

$$
\begin{equation*}
3 y=c_{1} \frac{z-1}{2 d_{1}} \quad \text { and } \quad 3 y=c_{2} \frac{z+1}{2 d_{2}} \tag{26}
\end{equation*}
$$

where $\operatorname{gcd}\left(c_{i}, d_{i}\right)=1$ for $i=1,2$. By Lemma 11 , the relations $y=\frac{c_{1}}{6 d_{1}}(z-1)$ and $y=\frac{c_{2}}{6 d_{2}}(z+1)$ imply

$$
\begin{equation*}
3 d_{1}<c_{1} \leq 6 d_{1} \quad \text { and } \quad \frac{38}{13} d_{2}<c_{2}<6 d_{2} \tag{27}
\end{equation*}
$$

respectively, where the lower bound on $c_{2}$ holds whenever $z>38$.

Part 2.4.1: $d_{1} \geq 3$ and $d_{2} \geq 3$.
Lemmas 7 and 12 together with (24) yield

$$
\alpha^{\frac{z}{2}-0.01}<\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right) \leq \sqrt{5} L_{\frac{z+1}{6}}^{2}<\sqrt{5}\left(\alpha^{\frac{z}{6}+0.17+0.01}\right)^{2}<\alpha^{\frac{z}{3}+2.04}
$$

We arrive at the contradiction $z<13$.

### 2.5. Part 2.4.2: $d_{1} \leq 2$ or $d_{2} \leq 2$.

Assume that $d_{i} \leq 2$ for some $i=1$, 2. From inequalities (27), it follows that $4 \leq c_{1} \leq 12$ and $3 \leq c_{2}<12$. Put again $\varepsilon_{i}=(-1)^{i}$ for $i=1,2$. Then the relation $3 y=\frac{c_{i}}{2 d_{i}}\left(z+\varepsilon_{i}\right)$ implies $z=\frac{6 d_{i}}{c_{i}} y-\varepsilon_{i}$. Putting $\operatorname{gcd}\left(6 d_{i}, c_{i}\right)=f_{i}$ and writing $6 d_{i}=a f_{i}$ and $c_{i}=b f_{i}$ with $\operatorname{gcd}(a, b)=1$, we get that $z=\frac{a}{b} y-\varepsilon_{i}$, where the fraction $\frac{a}{b}$ is one of the following:

$$
\begin{equation*}
\frac{a}{b}=\frac{2}{1}, \frac{3}{2}, \frac{6}{5}, \frac{1}{1}, \frac{12}{7}, \frac{4}{3}, \frac{12}{11} \tag{28}
\end{equation*}
$$

Most of the fractions in (28) occur for both $i=1$ and $i=2$, except for $\frac{2}{1}$ and $\frac{1}{1}$ which appear only if $i=2$, and $i=1$, respectively. Since $z$ is odd, we get that $\frac{a}{b} y$ is even so that if we write $y=b s$, then $s$ is even.

We again put $W:=\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right)=\operatorname{gcd}\left(L_{y}-1, L_{\frac{a}{b} y-\varepsilon_{i}}-1\right)$, and further write it as

$$
\begin{align*}
W & =\operatorname{gcd}\left(L_{b s}-1, L_{a s-\varepsilon_{i}}-1\right)=\operatorname{gcd}\left(L_{b s}-1, \delta_{e} E_{\frac{a s}{2}} E_{\frac{a s}{2}-\varepsilon_{i}}\right) \\
& =\operatorname{gcd}\left(L_{b s}-1, E_{\frac{a s}{2}}\right) \operatorname{gcd}\left(L_{b s}-1, E_{\frac{a s}{2}-\varepsilon_{i}}\right)=: W_{1} W_{2} \tag{29}
\end{align*}
$$

Now

$$
\begin{align*}
W_{1} & =\operatorname{gcd}\left(L_{b s}-1, E_{\frac{a s}{2}}\right) \leq \operatorname{gcd}\left(L_{b s}-1, F_{a s}\right) \leq \operatorname{gcd}\left(L_{b s}-1,5 F_{a s}^{2}\right) \\
& =\operatorname{gcd}\left(L_{b s}-1, L_{a s}^{2}-4\right)=\operatorname{gcd}\left(C_{b}(s)-1, C_{a}^{2}(s)-4\right) \tag{30}
\end{align*}
$$

Table 4 shows the greatest common divisor polynomial of the two polynomials $C_{b}(t)-1$ and $C_{a}^{2}(t)-4$.

| $(a, b)$ | $(2,1)$ | $(3,2)$ | $(6,5)$ | $(1,1)$ | $(12,7)$ | $(4,3)$ | $(12,11)$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\operatorname{gcd}_{\text {pol }}$ | -3 | -4 | $\frac{5}{4}(t-1)$ | -3 | $-\frac{7}{4}(t-1)$ | -3 | $-\frac{11}{1225}(t-1)$ |

Table 4: The polynomial $\operatorname{gcd}_{p o l}\left(C_{b}(t)-1, C_{a}^{2}(t)-4\right)$ provided by the Euclidean algorithm

When this polynomial is constant, then $W_{1} \leq \operatorname{num}|\gamma| \leq 4$, while when this polynomial linear, then num $|\gamma| \leq 11$ and $W_{1} \leq 11 L_{s}$. Observe that the second bound is larger than the first one.

Applying Lemma 13, we have

$$
\begin{align*}
W_{2} & =\operatorname{gcd}\left(L_{b s}-1, E_{\frac{a s}{2}-\varepsilon_{i}}\right) \leq \operatorname{gcd}\left(F_{3 b s}, E_{\frac{a s}{2}-\varepsilon_{i}}\right) \leq \operatorname{gcd}\left(F_{3 b s}, E_{\frac{a s}{2}-\varepsilon_{i}}\right) \\
& \left.=E_{\operatorname{gcd}\left(3 b s, \frac{a s}{2}-\varepsilon_{i}\right.}\right) \tag{31}
\end{align*}
$$

Since $s=2 r$ and $6 d_{i}=a f_{i}$,

$$
\begin{aligned}
\operatorname{gcd}\left(3 b s, \frac{a s}{2}-\varepsilon_{i}\right) & =\operatorname{gcd}\left(6 b r, a r-\varepsilon_{i}\right) \leq \operatorname{gcd}\left(6 d_{i} b r, 6 d_{i} r-\varepsilon_{i} f_{i}\right) \\
& =\operatorname{gcd}\left(\varepsilon_{i} f_{i} b, 6 d_{i} r-\varepsilon_{i} f_{i}\right) \\
& \leq f_{i} b=c_{i} \leq 12
\end{aligned}
$$

Consequently, by (31), we get $W_{2} \leq E_{12} \leq L_{12}$. Therefore, by Lemma 12 , we have

$$
\alpha^{\frac{z}{2}-0.01}<\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right)<L_{12} \cdot 11 L_{s}<\alpha^{s+0.01+\kappa}
$$

where we can take $\kappa<17$. Since $z=a s-\varepsilon_{i}$, we get that $s \leq \frac{z+1}{6}$, which implies that $z<51.6$.

The proof of the theorem is now complete.

## 3. Lemmas

Lemma 3. (i) $F_{n} \leq L_{n}$, with equality if and only if $n=1$.
(ii) $5 \nmid L_{n}$.
(iii) $5 \nmid\left(L_{n}-1\right)$ if $n$ is even.
(iv) $F_{n} L_{n}=F_{2 n}$.
(v) $L_{n}^{2}-5 F_{n}^{2}=4(-1)^{n}$.
(vi) $L_{2 n}=L_{n}^{2}-2(-1)^{n}$.
(vii) $L_{n+m}=\delta_{e} E_{n} E_{m} \mp(-1)^{m} L_{n-m}$ if $n \geq m$. (Here and anywhere near $E_{u}$, in $\pm$ and $\mp$ the upper sign relates to Lucas numbers, while the lower sign relates to Fibonacci numbers.)
(viii) $F_{n+m}=E_{n} \bar{E}_{m} \pm(-1)^{m} F_{n-m}$ if $n \geq m$.

Proof. These statements are well-known. However, item (i) can be proved, for instance, by induction. Items (ii) and (iii) follow easily by looking at the Lucas sequence modulo 5 . The statements (iv)-(viii) can be verified using the formulae for $L_{n}$ and $F_{n}$ appearing at (3).

Lemma 4. If both $k$ and $n$ are at least 2, then $5 F_{k} F_{n} \leq \sqrt{5} L_{k} L_{n}$.
Proof. We prove that $5 F_{k}^{2} F_{n}^{2} \leq L_{k}^{2} L_{n}^{2}$ holds, under the given condition, and this implies the lemma. The fifth point of Lemma 3 provides $25 F_{k}^{2} F_{n}^{2} \leq\left(L_{k}^{2}+4\right)\left(L_{n}^{2}+4\right)$. Therefore it is sufficient to show that $L_{k}^{2}+L_{n}^{2}+4 \leq L_{k}^{2} L_{n}^{2}$. This last inequality is equivalent to $5 \leq\left(L_{k}^{2}-1\right)\left(L_{n}^{2}-1\right)$, which holds if both $k$ and $n$ are at least 2 .

Lemma 5. The following divisibility relations hold:
(i) $\operatorname{gcd}\left(F_{u}, F_{v}\right)=F_{\operatorname{gcd}(u, v)}$,
(ii) $\operatorname{gcd}\left(L_{u}, L_{v}\right)= \begin{cases}L_{\operatorname{gcd}(u, v)}, & \text { if } \frac{u}{\operatorname{gcd}(u, v)} \equiv \frac{v}{\operatorname{gcd}(u, v)} \equiv 1(\bmod 2), \\ 1 \text { or } 2, & \text { otherwise, }\end{cases}$
(iii) $\operatorname{gcd}\left(F_{u}, L_{v}\right)= \begin{cases}L_{\operatorname{gcd}(u, v),} & \text { if } \frac{u}{\operatorname{gcd}(u, v)} \not \equiv \frac{v}{\operatorname{gcd}(u, v)} \equiv 1(\bmod 2), \\ 1 \text { or } 2, & \text { otherwise. }\end{cases}$

Proof. This is well-known (see, for instance, the proof of Theorem VII in [3]).
Lemma 6. The following formulae hold:
(i)

$$
F_{n}-1=\left\{\begin{array}{lll}
F_{\frac{n-1}{2}} L_{\frac{n+1}{2}}, & \text { if } n \equiv 1 & (\bmod 4) \\
F_{\frac{n+1}{2}} L_{\frac{n-1}{2}}, & \text { if } n \equiv 3 & (\bmod 4) \\
F_{\frac{n-2}{2}} L_{\frac{n+2}{2}}, & \text { if } n \equiv 2 & (\bmod 4) \\
F_{\frac{n+2}{2}} L_{\frac{n-2}{2}}, & \text { if } n \equiv 0 & (\bmod 4)
\end{array}\right.
$$

(ii)

$$
L_{n}-1= \begin{cases}5 F_{\frac{n-1}{2}} F_{\frac{n+1}{2}} & \text { if } n \equiv 1 \quad(\bmod 4) \\ L_{\frac{n-1}{2}} L_{\frac{n+1}{2}} & \text { if } n \equiv 3 \quad(\bmod 4)\end{cases}
$$

Proof. For the first part see, for example, Lemma 2 in [11]. Nevertheless, both parts can be verified by using (3).

Lemma 7. Let $u_{0}$ be a positive integer. Put

$$
\varepsilon_{i}=\log _{\alpha}\left(1+(-1)^{i-1}\left(\frac{|\beta|}{\alpha}\right)^{u_{0}}\right), \quad \delta_{i}=\log _{\alpha}\left(\frac{1+(-1)^{i-1}\left(\frac{|\beta|}{\alpha}\right)^{u_{0}}}{\sqrt{5}}\right)
$$

for $i=1,2$, respectively, where $\log _{\alpha}$ is the logarithm in base $\alpha$. Then for all integers $u \geq u_{0}$, the two inequalities

$$
\begin{equation*}
\alpha^{u+\varepsilon_{2}} \leq L_{u} \leq \alpha^{u+\varepsilon_{1}} \tag{32}
\end{equation*}
$$

and

$$
\begin{equation*}
\alpha^{u+\delta_{2}} \leq F_{u} \leq \alpha^{u+\delta_{1}} \tag{33}
\end{equation*}
$$

hold.

Proof. This is Lemma 5 in [12].
In order to make the application of Lemma 7 more convenient, we shall suppose that $u_{0} \geq 8$. Then we have the following corollary.

Corollary 8. If $u_{0} \geq 8$, then

$$
-0.01<\varepsilon_{2}, \quad \varepsilon_{1}<0.01, \quad-1.68<\delta_{2}, \quad \delta_{1}<-1.67
$$

Lemma 9. Suppose that $a>0$ and $b \geq 0$ are real numbers, and that $u_{0}$ is a positive integer. Then for all integers $u \geq u_{0}$, the inequality

$$
a \alpha^{u}+b \leq \alpha^{u+\kappa}
$$

holds with $\kappa=\log _{\alpha}\left(a+\frac{b}{\alpha^{u_{0}}}\right)$.

Proof. This is Lemma 6 in [12].

Lemma 10. Assume that $a, b, z$ and $\lambda \neq-1$ are integers. Furthermore, assume that all the expressions appearing inside the gcd's below are also integers. Then the following inequality holds:

$$
\operatorname{gcd}\left(\frac{z+a}{2}, \frac{\lambda z+b}{2(\lambda+1)}\right) \leq \begin{cases}\left|\frac{\lambda a-b}{2}\right|, & \text { if } \lambda a \neq b  \tag{34}\\ \frac{z+a}{2(\lambda+1)}, & \text { otherwise }\end{cases}
$$

Proof. Put $A_{1}=\frac{z+a}{2}, B_{1}=\frac{\lambda z+b}{2(\lambda+1)}$. Further, let $A_{2}=A_{1}-B_{1}, B_{2}=B_{1}-\lambda A_{2}$. Then, using the Euclidean algorithm, we have

$$
\begin{aligned}
G_{7} & =\operatorname{gcd}\left(A_{1}, B_{1}\right)=\operatorname{gcd}\left(A_{2}, B_{1}\right)=\operatorname{gcd}\left(A_{2}, B_{2}\right) \\
& =\operatorname{gcd}\left(\frac{z+(\lambda+1) a-b)}{2(\lambda+1)}, \frac{-\lambda a+b}{2}\right)
\end{aligned}
$$

If $b \neq \lambda a$, then $G_{7} \leq\left|\frac{\lambda a-b}{2}\right|$. Otherwise, if $b=\lambda a$, then $G_{7}=\frac{z+(\lambda+1) a-b}{2(\lambda+1)}=$ $\frac{z+a}{2(\lambda+1)}$.

We point out that the particular cases $\lambda=1$ and $\lambda=3$ of Lemma 10 were used in [12].

Lemma 11. All positive integer solutions of the system (4) satisfy $z \leq 2 y$.

Proof. The last two equations of system (4) imply that $c$ divides both $L_{y}-1$ and $L_{z}-1$. Consequently,

$$
\begin{equation*}
c \mid \operatorname{gcd}\left(L_{y}-1, L_{z}-1\right) \tag{35}
\end{equation*}
$$

Obviously, $L_{z}=b c+1<c^{2}$, hence $\sqrt{L_{z}}<c$. From (35), we obtain $\sqrt{L_{z}}<L_{y}-1$. Clearly,

$$
\begin{equation*}
\sqrt{\alpha^{z}-1}<\sqrt{L_{z}}<L_{y}-1<\alpha^{y} \tag{36}
\end{equation*}
$$

We then get that $\alpha^{z}-1<\alpha^{2 y}$, which easily leads to the conclusion that $2 y \geq z$.

Lemma 12. If the integers $0<a<b<c$ and $0<x<y<z$ satisfy the system (4), then $\alpha^{\frac{z}{2}-0.01}<\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right)$.

Proof. By the proof of Lemma 11 above, we know that $c \mid \operatorname{gcd}\left(L_{y}-1, L_{z}-1\right)$ and that $c>\sqrt{L_{z}}$. Combining these with Lemma 7 (with $u_{0}=z \geq 8$ ), we obtain

$$
\operatorname{gcd}\left(L_{y}-1, L_{z}-1\right)>\sqrt{L_{z}}>\sqrt{\alpha^{z-0.02}}=\alpha^{\frac{z}{2}-0.01}
$$

Lemma 13. If $n$ is even then $L_{n}-1$ divides $F_{3 n}$.
Proof. By Lemma 3.8, it follows immediately that $F_{3 n}=F_{n}\left(L_{2 n}+1\right)$. By Lemma 3.6, this coincides $F_{n}\left(L_{n}^{2}-1\right)=F_{n}\left(L_{n}-1\right)\left(L_{n}+1\right)$ for $n$ even.

## References

[1] Y. Bugeaud and A. Dujella, On a problem of Diophantus for higher powers, Math. Proc. Cambridge Philos. Soc. 135 (2003), 1-10.
[2] Y. Bugeaud and K. Gyarmati, On generalizations of a problem of Diophantus, Illinois J. Math. 48 (2004), 1105-1115.
[3] R. D. Carmichael, On the numerical factors of the arithmetic function $\alpha^{n} \pm \beta^{n}$, Ann. Math. 15 (1913-1914), 30-48.
[4] A. Dujella, There are only finitely many Diophantine quintuples, J. Reine Angew. Math. 566 (2004), 183-214.
[5] R. Finkelstein, On Lucas numbers which are one more then a square, Fibonacci Quart. 13 (1975), 340-343.
[6] C. Fuchs, F. Luca and L. Szalay, Diophantine triples with values in binary recurrences, Ann. Sc. Norm. Super. Pisa Cl. Sc. (5), 7 (2008), 579-608.
[7] P. Gibbs, Some rational Diophantine sextuples, Glas. Mat. Ser. III 41(61) (2006), 195-203.
[8] K. Gyarmati, A. Sarkozy and C. L. Stewart, On shifted products which are powers, Mathematika 49 (2002), 227-230.
[9] K. Gyarmati and C. L. Stewart, On powers in shifted products, Glas. Mat. Ser. III 42 (2007), 273-279.
[10] F. Luca, On shifted products which are powers, Glas. Mat. Ser. III 40 (2005), 13-20.
[11] F. Luca and L. Szalay, Fibonacci numbers of the form $p^{a} \pm p^{b}+1$, Fibonacci Quart., 45 (2007), 98-103.
[12] F. Luca and L. Szalay, Fibonacci diophantine triples, Glas. Mat. Ser. III, 43 (63) (2008), 253-264.
[13] T. J. Osler, Cardan polynomials and the reduction of radicals, Math. Magazine, 47 (2001), 26-32.


[^0]:    ${ }^{1}$ During the preparation of this paper, F. L. was supported in part by Grant SEP-CONACyT 79685 and PAPIIT 100508.
    ${ }^{2}$ The research is supported by a János Bolyai Scholarship of HAS, and by Hungarian National Foundation for Scientific Research Grant No. T 048954 MAT, No. T 61800 FT.

