DIOPHANTINE EQUATIONS WITH PRODUCTS OF CONSECUTIVE MEMBERS OF BINARY RECURRENCES

ATTILA BÉRCZES, YURI F. BILU, AND FLORIAN LUCA

ABSTRACT. We prove a finiteness result for the number of solutions of a Diophantine equation of the form $u_n u_{n+1} \cdots u_{n+k} \pm 1 = \pm u_m^2$, where $\{u_n\}_{n\geq 1}$ is a binary recurrent sequence whose characteristic equation has roots which are real quadratic units.

1. INTRODUCTION

Let $\{F_n\}_{n\geq 1}$ be the Fibonacci sequence given by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 1$. In [6], inspired by the still unsolved problem of Brocard and Ramanujan asking to determine all positive integer solutions (n,x) of the Diophantine equation

$$n! + 1 = x^2,$$

Marques fixed a positive integer t and showed that the Diophantine equation

$$F_1 \cdot F_2 \cdots F_n + 1 = F_m^t$$

has only finitely many positive integer solutions (n,m). He also computed all solutions when $t \in [1,10]$. The fact that the above equation has only finitely many solutions with t a variable as well follows as a byproduct of the results

A.B. was supported by the University of Debrecen, by a János Bolyai Scholarship of the Hungarian Academy of Sciences, and by grants K100339 and NK104208 of the Hungarian National Foundation for Scientific Research. F. L. worked on this paper when he visited the University of Debrecen in Juy 2016 and while he visited the Max Planck Institute for Mathematics in Bonn in 2017. He thanks both these institutions for hospitality and support. He was also supported by grants CPRR160325161141 and an A-rated researcher award both from the NRF of South Africa and by grant no. 17-02804S of the Czech Granting Agency.

2010 Mathematics Subject Classification: 11B39, 11D61.

Keywords and Phrases: Diophantine equations, binary recurrences, applications of linear forms in logarithms.

from [2], where it was shown among other things that the largest integer solution (k,ℓ,m,n) of

$$|F_nF_{n+1}\cdots F_{n+k-1}-F_m^{\ell}|\le 100 \qquad \text{with} \qquad k\ge 1,\ \ell\ge 1,\ m\ge 3,\ n\ge 3$$

(and $m\ne n$ when $k=\ell=1$) is

$$|F_9\cdots F_{13}-F_{11}^5|=89.$$

Here by largest solution it is understood the solution with maximal value of $\max\{F_nF_{n+1}\cdots F_{n+k-1},F_m^{\ell}\}$. This maximal value is 5584059449. Szalay [9], solved completely the Diophantine equation

$$G_{n_1}G_{n_2}\cdots G_{n_k}+1=G_m^2$$

in positive integer unknowns $k,\ m$ and $n_1<n_2<\cdots<n_k$ where $\{G_n\}_{n\ge 1}$ is in a certain family of Lucas sequences including the Fibonacci sequence. Further generalizations of this problem were considered by Szikszai [10].

The proofs from [6], [9] and [10] all have in common the fact that they use the existence of primitive divisors for terms of Lucas sequences. Here we study the same question (or a variant of) but for a very different kind of sequence $\{u_n\}_{n\ge 1}$ which we now describe. We assume that $\{u_n\}_{n\ge 1}$ is a binary recurrent sequence of integers satisfying $u_{n+2}=ru_{n+1}+su_n$, for all $n\ge 1$, where r and s are fixed nonzero integers. We assume that the characteristic equation $x^2-rx-s=0$ has two roots $\alpha\ne\beta$ (so $\Delta=r^2+4s\ne 0$) and that α/β is not a root of 1. Such sequences are called *nondegenerate*. In this case it is known that

$$u_n=c\alpha^n+d\beta^n \qquad \text{holds for all} \qquad n\ge 1, \tag{1.1}$$

where c and d can be computed in terms of $u_1,\ u_2$. In fact,

$$(c,d)=\left(\frac{u_2-\beta u_1}{\alpha^2-\alpha\beta},\frac{u_2-\alpha u_1}{\beta^2-\alpha\beta}\right). \tag{1.2}$$

We further assume that $s=\pm 1$. The above restrictions insure that $\Delta>0$ so α and β are real. We label these roots in such a way that $|\alpha|>1>|\beta|$ (note that $\beta=-s\alpha^{-1}=\pm\alpha^{-1}$). We find it convenient to use the recurrence for $\{u_n\}_{n\ge 1}$ and define u_0 such that $u_2=:ru_1+su_0$. That is, $u_0:=s^{-1}(u_2-ru_1)$, which is an integer since $s\in\{\pm 1\}$. Then formula (1.1) holds with $n=0$ as well, while (1.2) can be replaced by the somewhat simpler looking expression

$$(c,d)=\left(\frac{u_1-\beta u_0}{\alpha-\beta},\frac{u_1-\alpha u_0}{\alpha-\beta}\right). \tag{1.3}$$

Classically, Lucas sequences are obtained when $u_0 = 0$ (so, $c/d = -1$) or when $u_0 = 2,\ u_1 = r$ (case in which $c = d = 1$, so $c/d = 1$). To essentially shift away from the situation of a primitive divisor theorem in disguise (so to avoid dealing with some binary recurrent sequence which is the subsequence of a Lucas sequence obtained, for example, by only selecting the terms of a Lucas sequence with indices in a fixed arithmetic progression), we make the assumption that

$$c/d \quad \text{and} \quad \alpha/\beta \quad \text{are multiplicatively independent.} \tag{1.4}$$

Note that since $\alpha/\beta = \pm\alpha^2$, it follows that the above condition is equivalent to c/d and α being multiplicatively independent, but the notation of (1.4) is more symmetric in the variables c, d, α, β which is why we keep the above formulation. Then we have the following theorem.

Theorem 1.1. *Assume that $\{u_n\}_{n\ge 0}$ is a nondegenerate binary recurrent sequence of integers of characteristic equation $x^2 - rx - s = 0$ with $s \in \{\pm 1\}$ whose roots are α and β. Assume that in the formula (1.1) the parameters c/d and α/β satisfy (1.4). Then the Diophantine equation*

$$u_n u_{n+1} \cdots u_{n+k-1} \pm 1 = \pm u_m^2 \tag{1.5}$$

has at most finitely many positive integer solutions (k, m, n). Moreover, the solutions are effectively computable and satisfy

$$m < 10^{53}(Y+2)^{64}, \tag{1.6}$$

where

$$Y := \max\{|u_0|, |u_1|, |r|\}.$$

Our arguments can be applied to deal with the situation when the term ± 1 is replaced by any nonzero integer, but the details are much more cumbersome.

As a toy example, we solve equation (1.5) in the concrete case when $\{u_n\}_{n\ge 0}$ is given by $u_0 = -9,\ u_1 = 7$ and $u_{n+2} = u_{n+1} + u_n$ for all $n \ge 1$. The first few values of this sequence are

$$-9,\ 7,\ -2,\ 5,\ 3,\ 8,\ 11,\ 19,\ 30,\ 49,\ 79,\ 128,\ \ldots$$

Then $(\alpha, \beta) = ((1+\sqrt{5})/2, (1-\sqrt{5})/2)$ and

$$(c, d) = \left(\frac{23 - 9\sqrt{5}}{2\sqrt{5}}, -\frac{23 + 9\sqrt{5}}{2\sqrt{5}}\right).$$

Condition (1.4) is satisfied since c/d has trace $-467/31$ in $\mathbb{Q}(\sqrt{5})$, so in particular it is not an algebraic integer. Thus, c/d and α/β are multiplicatively independent, otherwise c/d will be a unit in $\mathbb{Q}(\sqrt{5})$, in particular an algebraic integer. We have the following result.

Theorem 1.2. *For the sequence $\{u_n\}_{n\geq 0}$ given by $u_1=-9$, $u_2=7$ and $u_{n+2}=u_{n+1}+u_n$ for all $n\geq 1$, the only solutions of equation (1.5) are*

$$\begin{aligned} u_3-1 &= u_2^2, \\ u_4+1 &= u_2^2, \\ u_5+1 &= u_4^2, \\ u_0u_1-1 &= -u_5^2, \\ u_2u_3+1 &= -u_4^2, \\ u_4u_5+1 &= u_3^2, \\ u_3u_4u_5+1 &= u_6^2. \end{aligned}$$

2. PRELIMINARIES

Next let us notice that $u_n\neq 0$ for any $n\geq 0$. Indeed, if $u_n=0$ for some $n\geq 0$, then equation (1.1) shows that $c/d=-(\alpha/\beta)^{-n}$, contradicting (1.4). Thus, $|u_n|\geq 1$ for all $n\geq 1$. Next we justify that we may assume that $r>0$. Indeed, if $r=0$, then $\alpha/\beta=-1$, which is not allowed. If $r<0$, we may replace the pair (r,s) by the pair $(-r,s)$. This has as effect replacing the pair (α,β) by $(-\alpha,-\beta)$. With (1.1), we get easily that, by keeping u_0 and changing the sign of u_1, we keep the values of c and d and, in particular, u_n is then replaced by $(-1)^n u_n$. Hence, $|u_n|$ does not change under the above transformations. Since equation (1.5) is

$$|u_m|^2=|u_nu_{n+1}\cdots u_{n+k}\pm 1|=|u_n||u_{n+1}|\cdots|u_{n+k}|\pm 1,$$

(for the last formula above we used the fact that $|u_\ell|\geq 1$ for all $\ell\geq 1$), it follows that we may indeed assume that $r>0$. Since $|\alpha|>1$, it follows that in fact α is positive, so

$$(\alpha,\beta)=\left(\frac{r+\sqrt{\Delta}}{2},\frac{r-\sqrt{\Delta}}{2}\right).$$

Further, if $c<0$, we then replace (c,d) by $(-c,-d)$. This has as effect changing the sequence $\{u_n\}_{n\geq 1}$ to $\{-u_n\}_{n\geq 1}$, but as we already saw above, such transformation does not affect the solutions of (1.5). Hence, we assume that $c>0$.

Below we record some lemmas.

Lemma 2.1. *We have* $\max\{|u_0|,|u_1|,|u_2|,|u_3|\} > 1$.

As the referee pointed out, this lemma is a special case of Theorem 3 in [1]. We give a short proof here, the argument from [1] being quite involved.

Proof. Assume that $|u_0| = |u_1| = 1$. Replacing $\{u_n\}_{n\ge 0}$ by $\{-u_n\}_{n\ge 0}$ if necessary, we may assume that $u_0 = 1$. Since $s = \pm 1$ we either have $s = u_2$ or $s = -u_2$. If $u_2 = \pm 1$, we then get $\pm 1 = u_2 = ru_1 + su_0 = \pm r + s$. If $s = u_2$, we get $r = 0$, which is not allowed. So, $s = -u_2$ and $r = 2u_1u_2$. Since $r > 0$, we first get that $r = 2$, then that the characteristic equation must be $x^2 - 2x - 1 = 0$ (for the other option $x^2 - 2x + 1 = 0$ has a double root at $x = 1$, which is not allowed), so $s = 1 = -u_2$ and $2 = r = 2u_1u_2 = -2u_1$, so $u_1 = -1$. Then $u_3 = ru_2 + su_1 = -2 - 1 = -3$, which gives us the desired conclusion. □

Lemma 2.2. *Let p be any prime. Then* $\{u_n\}_{n\ge 1}$ *is periodic modulo p with period at most* $p^2 - 1$.

Proof. This is well-known. □

We next need bounds on $|u_n|$ which are explicit. First, let us recall some terminology.

Let η be an algebraic number of degree $\deg(\eta)$, whose minimal polynomial over the integers is

$$g(x) := a_0 \prod_{i=1}^{\deg(\eta)} (x - \eta^{(i)}).$$

We assume that $a_0 > 0$. The logarithmic height of η is defined as

$$h(\eta) := \frac{1}{\deg(\eta)} \left(\log a_0 + \sum_{i=1}^{d} \log \max\{|\eta^{(i)}|, 1\} \right).$$

We put

$$\lceil\overline{\eta}\rceil := \max\{|\eta^{(i)}| : i = 1, \ldots, \deg(\eta)\}.$$

In particular,

$$\log \lceil\overline{\eta}\rceil < \deg(\eta) h(\eta). \tag{2.1}$$

We also put $\mathrm{den}(\eta)$ for the smallest positive integer k such that $k\eta$ is an algebraic integer. Since $\mathrm{den}(\eta)$ divides a_0, it follows that

$$\log \mathrm{den}(\eta) \le \deg(\eta) h(\eta). \tag{2.2}$$

Recall that

$$Y := \max\{r, |u_0|, |u_1|\}. \tag{2.3}$$

Note that $Y \ge 2$, for if $Y = 1$, then $r = |u_0| = |u_1| = 1$, so $s = 1$ and then $\{u_n\}_{n\ge 0}$ is, up to signs, some shift of the Fibonacci sequence, more precisely $\{u_n\}_{n\ge 0}$ is one of $\{F_{n+1}\}_{n\ge 0}$, $\{-F_{n+1}\}_{n\ge 0}$, $\{F_{n-2}\}_{n\ge 0}$ or $\{-F_{n-2}\}_{n\ge 0}$, all of which fail condition (1.4). In what follows, we write $\mathbb{K} := \mathbb{Q}(\sqrt{\Delta})$.

The following results are similar to some results from [3].

Lemma 2.3. *We have*

$$\max\{h(\alpha), h(\beta), h(\alpha/\beta), h(c), h(d), h(c/d)\} < 6\log(Y+1). \tag{2.4}$$

Proof. Since $\alpha + \beta = r \le Y$ and $|\beta| < 1$, we have that $1 < \alpha < Y + 1$. Thus,

$$h(\alpha) = \frac{1}{2}\log\alpha < \frac{1}{2}\log(Y+1).$$

Since $\beta = \pm\alpha^{-1}$, we have that $h(\beta) = h(\alpha)$. Since $c = (u_1 - u_0\beta)/(\alpha - \beta)$ and c and d are conjugates in $\mathbb{K}$, it follows that $h(c) = h(d)$. Further,

$$\max\{|c|, |d|\} \le \max\{|u_0|, |u_1|\}\left(\frac{\alpha+1}{\alpha-\beta}\right) \le Y(Y+2) < (Y+1)^2, \tag{2.5}$$

where we used the fact that $\alpha - \beta = \sqrt{\Delta} \ge 1$ and $\alpha + 1 < Y + 2$. Finally, it is easy to see that if a_0 is the leading coefficient of the minimal polynomial (over $\mathbb{Z}$) of c, then $a_0 \mid (\alpha - \beta)^2$. Thus,

$$a_0 \le (\alpha - \beta)^2 = \Delta = r^2 + 4s \le r^2 + 4 < (Y+1)^2. \tag{2.6}$$

Putting all these facts together we get that

$$\begin{aligned} h(c) = h(d) &= \frac{1}{2}(\log a_0 + \log\max\{1, |c|\} + \log\max\{1, |d|\}) \\ &< \frac{1}{2}\left(\log(Y+1)^2 + 2\log(Y+1)^2\right) = 3\log(Y+1). \end{aligned}$$

Finally,

$$h(c/d) \le h(c) + h(d) < 6\log(Y+1).$$

□

We put

$$C_0 := 6\log(Y+1)+2.$$

Lemma 2.4. *We have*

$$|u_n| < \alpha^{n+C_0}$$

for all $n \geq 0$.

Proof. Using (1.1) and (1.3) we have

$$|u_n| \leq \max\{|c|,|d|\}(\alpha^n+1) \leq 2\alpha^n(Y+1)^2 = \alpha^{n+\frac{\log 2}{\log\alpha}+\frac{2\log(Y+1)}{\log\alpha}} < \alpha^{n+C_0},$$

where we used the fact that $\alpha \geq (1+\sqrt{5})/2$. □

Lemma 2.5. *If* $n \geq C_0$, *then*

$$|u_n| > \alpha^{n-C_0}.$$

Proof. We write by (1.1)

$$|u_n| = |c|\alpha^n\left|1+\frac{d}{c}\left(\frac{\beta}{\alpha}\right)^n\right|. \tag{2.7}$$

Note that

$$2\left|\frac{d}{c}\right| = 2\left(\frac{|u_1-\alpha u_0|^2}{|N_{\mathbf{K}}(u_1-\alpha u_0)|}\right) \leq 2\max\{|u_0|,|u_1|\}^2(1+\alpha)^2 < 2(Y+2)^4.$$

Here, $N_{\mathbb{K}}(\bullet)$ is the norm from $\mathbb{K}$ to $\mathbb{Q}$. In the above (and later throughout the paper), we used that $u_1-\alpha u_0$ is a nonzero algebraic integer in $\mathbb{K}$, therefore $|N_{\mathbb{K}}(u_1-\alpha u_0)| \geq 1$. But $\alpha \geq (1+\sqrt{5})/2 > e^{1/3}$ and $n \geq C_0$, so the above inequality implies

$$\left|\frac{\alpha}{\beta}\right|^n = \alpha^{2n} > e^{2n/3} > e^{4\log(Y+2)+4/3} > 2(Y+2)^4 > 2\left|\frac{d}{c}\right|,$$

showing that

$$\left|\frac{d}{c}\left(\frac{\beta}{\alpha}\right)^n\right| < \frac{1}{2}. \tag{2.8}$$

It follows, from (2.8), (2.7) and the absolute value inequality, that

$$|u_n| > \frac{|c|\alpha^n}{2} = \frac{|N_{\mathbb{K}}(u_1-\alpha u_0)|\alpha^n}{2(\alpha-\beta)|u_1-\alpha u_0|} \geq \frac{\alpha^n}{2(\alpha+1)^2Y} \geq \frac{\alpha^{n-4}}{(Y+2)^2} > \alpha^{n-C_0},$$

where for the last inequality we used $\alpha > e^{1/3}$, $2Y < (Y+2)^2$, $\alpha^2 \geq \alpha+1$. □

3. On the numbers $u_m \pm 1$ and $u_m \pm i$

Rewriting equation (1.5) as

$$u_n u_{n+1} \cdots u_{n+k-1} = \pm(u_m^2 \pm 1) = \pm(u_m + \varepsilon)(u_m - \varepsilon) \quad \text{with} \quad \varepsilon \in \{1, i\},$$

it follows that it makes sense to study the expressions $u_m - \varepsilon$ for $\varepsilon \in \{\pm 1, \pm i\}$. Using (1.1), we get

$$u_m - \varepsilon = c\alpha^{-m}\left(\alpha^{2m} - \frac{\varepsilon}{c}\alpha^m + \frac{(-s)^m d}{c}\right) = c\alpha^{-m}(\alpha^m - z_1^{(m,\varepsilon)})(\alpha^m - z_2^{(m,\varepsilon)}),$$

where

$$z_{1,2}^{(m,\varepsilon)} = \frac{\frac{\varepsilon}{c} \pm \sqrt{\left(\frac{\varepsilon}{c}\right)^2 - \frac{4(-s)^m d}{c}}}{2} = \frac{\varepsilon \pm \sqrt{\varepsilon^2 - 4(-s)^m cd}}{2c}. \tag{3.1}$$

In the above calculation, we used that $c > 0$. Note that also that expressions (3.1) and (1.3) show that

$$z_{1,2}^{(m,\varepsilon)} = \frac{\varepsilon\sqrt{\Delta} \pm \sqrt{\varepsilon^2\Delta - 4(-s)^m N_{\mathbb{K}}(u_1 - \alpha u_0)}}{2\sqrt{\Delta}c}. \tag{3.2}$$

In particular, the number $(2\sqrt{\Delta}cz_{1,2}^{(m,\varepsilon)})^2$ is an algebraic integer of degree at most 2. For simplicity, we write ζ for any of $\zeta_{1,2}^{(m,\varepsilon)}$. Let us give some estimates on $h(\zeta)$. We start with the following lemma.

Lemma 3.1. *If $\zeta \in \mathbb{Q}$, then $c + d = \pm 1$ and $\zeta \in \{\pm 1\}$.*

Proof. Assume $\zeta \in \mathbb{Q}$. We have either

$$\zeta^2 - \frac{\varepsilon}{c}\zeta + \frac{(-s)^m d}{c} = 0, \tag{3.3}$$

or

$$\zeta^2 - \frac{\varepsilon}{d}\zeta + \frac{(-s)^m c}{d} = 0. \tag{3.4}$$

Assume first that $\varepsilon \in \{\pm i\}$. Then applying the complex conjugation we conclude that if ζ satisfies either of (3.3) or (3.4), then it will also satisfy the same equation with ε replaced by $-\varepsilon$. Subtracting the two resulting relations, we get that either $2\varepsilon\zeta/c = 0$ (or $2\varepsilon\zeta/d = 0$), so $\zeta = 0$, implying $d/c = 0$, a contradiction. Thus, $\varepsilon \in \{\pm 1\}$. Using the conjugation from $\mathbb{K}$ we conclude that ζ satisfies both (3.3) and (3.4). With the substitution $c_1 := -\varepsilon c$ and $d_1 := -\varepsilon(-s)^m d$, we get that the two quadratics

$$X^2 + \frac{1}{c_1}X + \frac{d_1}{c_1} \qquad \text{and} \qquad X^2 + \frac{1}{d_1}X + \frac{c_1}{d_1}$$

have a common root. Their resultant is

$$\frac{(c_1 - d_1)^2((c_1 + d_1)^2 - 1)}{(c_1 d_1)^2}.$$

Imposing that it is zero, we get that either $c_1 = d_1$, or $c_1 + d_1 = \pm 1$. The first case leads to $c/d = \pm 1$, which is not possible because of condition (1.4). The second leads to either $c - d = \pm 1$ or $c + d = \pm 1$. The possibility $c - d = \pm 1$ together with $c + d = c + c^\sigma \in \mathbb{Q}$, leads to $c \in \mathbb{Q}$. Since c and d are conjugated, we get that $c/d = 1$, which is again impossible. Thus, $c_1 + d_1 = \pm 1$ implies $c + d = \pm 1$, leading to $(-s)^m = 1$. Putting now $\varepsilon_1 := \varepsilon(c + d)$, we get

$$\begin{aligned} u_m - \varepsilon &= (c\alpha^m + d\alpha^{-m}) - \varepsilon_1(c + d) \\ &= c(\alpha^m - \varepsilon_1) + d(\alpha^{-m} - \varepsilon_1) \\ &= c\alpha^{-m}(\alpha^m - \varepsilon_1)(\alpha^m - d\varepsilon_1/c), \end{aligned}$$

and we recognize our rational root $\zeta = \varepsilon_1 \in \{\pm 1\}$. □

Lemma 3.2. *We have*

$$h(\zeta) < 6 \log(Y + 2).$$

Proof. Since ζ is a root of a quadratic polynomial with coefficients in $\mathbb{K}(i)$, it follows that $\deg(\zeta) \leq 8$. Further, Lemma 3.1 shows that if $\zeta \in \mathbb{Q}$, then $\zeta = \pm 1$, so $h(\zeta) = 0$. Thus, we may assume that $\zeta \notin \mathbb{Q}$, therefore $\deg(\zeta) \geq 2$. We use expression (3.2) for ζ. Thus, the conjugates of ζ have similar formulas with ε replaced eventually by $-\varepsilon$ or $\pm\overline{\varepsilon}$ and with $\sqrt{\Delta}$ replaced by $-\sqrt{\Delta}$. Further, $\sqrt{\Delta}c$ and $\sqrt{\Delta}d$ are conjugated quadratic integers, so their reciprocals in absolute value are at most

$$\sqrt{\Delta} \max\{|c|, |d|\} = \max\{|u_1 - \alpha u_0|, |u_1 - \beta u_0|\}.$$

Thus,

$$
\begin{aligned}
\lceil\zeta\rceil &\le \frac{1}{2}\left(\sqrt{Y^2+4}+\sqrt{Y^2+4+4|N_{\mathbb{K}}(u_1-\alpha u_0)|}\right)\sqrt{\Delta}\max\{|c|,|d|\}\\
&\le \frac{1}{2}\left(2Y+\sqrt{Y^2+4+8\max\{|u_0|,|u_1|\}^2(1+\alpha)}\right)\max\{|u_1|,|u_0|\}(1+\alpha)\\
&\le \frac{1}{2}\left(2Y+\sqrt{Y^2+4+8Y^2(Y+2)}\right)Y(Y+2)\\
&\le \frac{1}{2}\left(2Y+(Y+2)^{3/2}\sqrt{8}\right)(Y+2)^2<2(Y+2)^{7/2}\le (Y+2)^4.
\end{aligned}
$$

Also, we can see that a_0 divides Δcd, which is an integer. Its size is

$$
|N_{\mathbb{K}}(u_1-\alpha u_0)|\le 2\max\{|u_1|,|u_0|\}^2(1+\alpha)<2Y^2(Y+2)<(Y+2)^4.
$$

Thus,

$$
\begin{aligned}
h(\zeta) &< \frac{1}{\deg(\zeta)}\left(\log(Y+2)^4+\deg(\zeta)\log(Y+2)^4\right)\\
&= 4\log(Y+2)\left(1+\frac{1}{\deg(\zeta)}\right)\le 6\log(Y+2).
\end{aligned}
$$

□

We need to understand whether ζ, c/d and α can be multiplicatively dependent. We have the following lemma.

Lemma 3.3. *Assume that there are integers (x,y,z) not all zero with with*

$$
\zeta^z(c/d)^y\alpha^x=1. \tag{3.5}
$$

Then there exist a nonzero integer vector (x_0,y_0,z_0) and an integer λ such that

$$
\zeta^{z_0}(c/d)^{y_0}\alpha^{x_0}=\pm1,\qquad \max\{|x_0|,|y_0|,|z_0|\}<250000(\log(Y+2))^2,
$$

and

$$
(x,y,z)=\lambda(x_0,y_0,z_0).
$$

The proof of this lemma is based on the following result of Masser [7, Theorem $\mathbf{G}_m$ on page 253], which tells that the group of multiplicative relations of several non-zero algebraic numbers has bounded generators.

Proposition 3.4 (Masser)**.** *Let $\gamma_1,\dots\gamma_n$ be non-zero algebraic numbers and let $\Gamma=\langle\gamma_1,\dots\gamma_n\rangle$ the multiplicative group they generate. Further, let*

$$
\eta=\min\{h(\gamma):\gamma\in\Gamma,h(\gamma)>0\}
$$

be the smallest positive height of an element of Γ, *and* ω *the total number of roots of unity in the number field* $\mathbb{Q}(\gamma_1,\dots,\gamma_n)$. *Then the subgroup of* $\mathbb{Z}^n$ *consisting of* $(x_1,\dots,x_n)$ *such that* $\gamma_1^{x_1}\cdots\gamma_n^{x_n}=1$ *has a generating set consisting of elements satisfying*

$$\max\{|x_1|,\dots,|x_n|\} \le n^{n-1}\omega\left(\frac{h}{\eta}\right)^{n-1},$$

where $h=\max\{h(\gamma_1),\dots,h(\gamma_n)\}$.

Proof of Lemma 3.3. We will apply Masser's result to the numbers α^2, $(c/d)^2$ and ζ^2. Note using (3.2) that

$$\zeta^2=\left(\frac{\varepsilon\sqrt{\Delta}\pm\sqrt{\varepsilon^2\Delta-4(-s)^m N_{\mathbb{K}}(u_1-\alpha u_0)}}{2\sqrt{\Delta}c}\right)^2=\frac{A+\sqrt{C}}{\Delta c^2}. \tag{3.6}$$

for some integers A and C. It follows that ζ^2 is of degree at most 2 over the field $\mathbb{Q}(\sqrt{\Delta})$. In particular, α^2, $(c/d)^2$ and ζ^2 generate a field of degree at most 4, which implies that the parameter ω in Masser's result is bounded by 12.

Furthermore, the smallest non-zero height of an algebraic number of degree at most 4 is that of the root of X^4-X-1, and this height is equal to

$$\frac{1}{4}\log 1.38027756\ldots > 0.08$$

(see [5, page 477]). Hence, $\eta>0.08$. Finally, Lemmas 2.3 and 3.2 imply that $h=12\log(Y+2)$ would do.

Since α and c/d are multiplicatively independent by (1.4), the group of integral vectors (x,y,z) satisfying $\zeta^{2z}(c/d)^{2y}\alpha^{2x}=1$ is of rank 1. By the result of Masser, this group is generated by $(x_0,y_0,z_0)\in\mathbb{Z}^3$ satisfying

$$\max\{|x_0|,|y_0|,|z_0|\}\le 3^2\cdot 12\cdot\left(\frac{12\log(Y+2)}{0.08}\right)^2<250000(\log(Y+2))^2.$$

We have clearly $\zeta^{z_0}(c/d)^{y_0}\alpha^{x_0}=\pm1$, and our (x,y,z) is an integral multiple of (x_0,y_0,z_0). □

4. On the greatest common divisor of $\alpha^{m_1}\pm c/d$ and $\alpha^{m_2}-\zeta_{1,2}^{(m,\varepsilon)}$

We keep our α and let $\zeta_1=\pm c/d$ and $\zeta_2=\zeta$ for some fixed m and ε. Let $\mathbb{L}$ be some number field containing α,ζ_1,ζ_2 of degree D. Put

$$Z:=\max\{h(\alpha),h(\zeta_1),h(\zeta_2)\}.$$

Note that $Z \leq 6\log(Y+2)$. We need the following lemma.

Lemma 4.1. *Let m_1 and m_2 be positive integers and I be an ideal of $\mathcal{O}_{\mathbb{L}}$ dividing both $\alpha^{m_1} - \zeta_1$ and $\alpha^{m_2} - \zeta_2$. Then putting $M := \max\{m_1, m_2, 3\}$, one of the following holds:*

(i) $N_{\mathbb{L}}(I) < \exp(6D^2 Z\sqrt{M})$.

(ii) *There exist integers (x_0, y_0, z_0) not all 0 with*

$$\max\{|x_0|, |y_0|, |z_0|\} \leq 250000(\log(Y+2))^2, \tag{4.1}$$

such that

$$z_0 m_1 + y_0 m_2 + x_0 = 0.$$

Proof. Write $\alpha^{m_i} \equiv \zeta_i \pmod{I}$ with $i = 1, 2$. There exist integers (v_1, v_2) not both zero such that $\max\{|v_1|, |v_2|\} \leq \sqrt{M}$ and $|v_1 m_1 + v_2 m_2| \leq 3\sqrt{M}$ (see Lemma 1 in [4]). Up to replacing (v_1, v_2) by $(-v_1, -v_2)$, if needed, we may assume that $v_1 m_1 + v_2 m_2 \geq 0$. Exponentiating the above congruences to the powers v_1 (for $i = 1$) and v_2 (for $i = 2$) and multiplying the resulting congruences we get

$$\alpha^{v_1 m_1 + v_2 m_2} \equiv \zeta_1^{v_1} \zeta_2^{v_2} \pmod{I}.$$

Thus, I divides the algebraic number

$$\alpha^{v_1 m_1 + v_2 m_2} - \zeta_1^{v_1} \zeta_2^{v_2}.$$

We now look at the above number. Assume first that the number shown at (4.2) is nonzero. Let Γ be a common denominator of $\zeta_1^{\pm 1}, \zeta_2^{\pm 1}$. By inequality (2.2), it follows that

$$\log \Gamma \leq DZ.$$

Putting $v := 2\max\{|v_1|, |v_2|\}$, we get that

$$I \mid \Gamma^{v}(\alpha^{v_1 m_1 + v_2 m_2} - \zeta_1^{v_1} \zeta_2^{v_2}) = \Gamma^{v} \alpha^{v_1 m_1 + v_2 m_2} - \Gamma^{v'}(\Gamma \zeta_1^{\varepsilon_1})^{|v_1|}(\Gamma \zeta_2^{\varepsilon_2})^{|v_2|},$$

where $\varepsilon_i = \operatorname{sign}(v_i)$ for $i = 1, 2$, and $v' = v - v_1 - v_2 \geq 0$. The last number above is a nonzero algebraic integer in $\mathbb{L}$. Computing norms in $\mathbb{L}$, we get

$$\begin{aligned}
|N_{\mathbb{L}}(I)| &\leq \prod_{i=1}^{D} \left| \Gamma^{v}(\alpha^{(i)})^{v_1 m_1 + v_2 m_2} - \Gamma^{v'}(\Gamma \zeta_1^{(i)})^{v_1}(\Gamma \zeta_2^{(i)})^{v_2} \right| \\
&\leq 2^D \Gamma^{2D\sqrt{M}} \left(\max\{\overline{|\alpha|}^3, \overline{|\zeta_1|}\,\overline{|\zeta_2|}\} \right)^{D\sqrt{M}} \\
&\leq \exp(D\log 2 + 2D\sqrt{M}\log\Gamma + D\sqrt{M}\max\{3\log\overline{|\alpha|}, \log(\overline{|\zeta_1|}\,\overline{|\zeta_2|})\}) \\
&< \exp\left(6D^2 Z\sqrt{M}\right).
\end{aligned}$$

In the above, we used in addition to estimates (2.1) and (2.2), the fact that $\log|\Gamma| \le DZ$ together with the fact that $DZ\sqrt{M} \ge \sqrt{3}\log((1+\sqrt{5})/2) > \log 2$. This is exactly (i).

Assume now that the number shown at (4.2) is zero. Then

$$\zeta^{v_2}(\pm c/d)^{v_1}\alpha^{-(v_1m_1+v_2m_2)} = 1. \tag{4.2}$$

Lemma 3.3 shows that there exist integers $\lambda \neq 0$ and x_0, y_0, z_0 not all three zero satisfying inequality (4.1) such that

$$v_2 = \lambda z_0, \qquad v_1 = \lambda y_0, \qquad v_1m_1 + v_2m_2 = -\lambda x_0.$$

Inserting the first two into the third we get

$$y_0m_1 + z_0m_2 + x_0 = 0,$$

which is (ii). $\square$

5. The proof of Theorem 1.1

We split the proof in various steps. We assume that m is sufficiently large (with respect to Y), where sufficiently large will be made explicit at each step.

5.1. Bounding $n+k$ in terms of m.

Lemma 5.1. *If $m > 3C_0 + 3$, then $n+k < 3m$.*

Proof. If $n+k < C_0+1$, then there is nothing to prove. Thus, assume that $n+k \ge C_0+1$. In particular, $n+k > 4$, so $|u_n|\cdots|u_{n+k-1}| \ge 2$ by Lemma 2.1. We then have, by Lemmas 2.5 and 2.4, that

$$\begin{aligned} \alpha^{n+k-C_0-3} &< \frac{\alpha^{n+k-1-C_0}}{2} \le \frac{|u_{n+k-1}|}{2} \le |u_n||u_{n+1}|\cdots|u_{n+k-1}| - 1 \\ &\le |u_nu_{n+1}\cdots u_{n+k-1} \pm 1| = |u_m|^2 < \alpha^{2m+2C_0}, \end{aligned}$$

so

$$n+k < 2m + 3C_0 + 3 < 3m.$$

$\square$

5.2. **A dichotomy.** Assume that $m > 100C_0$. We rewrite our equation as

$$\begin{aligned}\prod_{i=0}^{k-1}(c\alpha^{n+i}+d\beta^{n+i}) &= \prod_{i=0}^{k-1}u_{n+i}=u_m^2\pm 1=(u_m-\varepsilon)(u_m+\varepsilon)\\ &= c^2\alpha^{-2m}\prod_{\substack{j=1,2\\ \delta\in\{\pm\varepsilon\}}}(\alpha^m-z_j^{(m,\delta)}).\end{aligned}$$

We fix m and ε and work in the field $\mathbb{L}$ containing $\mathbb{K}$ and all four numbers $z_{1,2}^{(m,\pm\varepsilon)}$, which is of degree

$$D\le 16, \tag{5.1}$$

since it is contained in $\mathbb{Q}(\alpha,i)(z_1^{(m,\varepsilon)},z_1^{(m,-\varepsilon)})$ and each of $z_1^{(m,\pm\varepsilon)}$ is at most quadratic over $\mathbb{Q}(\sqrt{\Delta},i)$. Letting

$$Z:=\max\{h(\alpha),h(c/d),h(z_{1,2}^{(m,\pm\varepsilon)})\},$$

we get that

$$Z\le 6\log(Y+2), \tag{5.2}$$

by Lemmas 2.3 and 3.2.

The condition $m>100C_0$ insures that

$$m>6DZ. \tag{5.3}$$

For $i\in\{0,1,\ldots,k-1\}$, $j\in\{1,2\}$ and $\delta\in\{\pm\varepsilon\}$, we put

$$I_{i,j}^{(m,\delta)}=\gcd\left(c\alpha^{n+i}+d\beta^{n+i},\alpha^m-\zeta_j^{(m,\delta)}\right)$$

as an ideal of $\mathscr{O}_{\mathbb{L}}$. We show that c is invertible modulo $I_{i,j}^{(m,\delta)}$. For simplicity, let I stand for this last ideal. Well, assume that it isn't. Then there exists a prime ideal π appearing at a positive exponent in the factorization of the fractional ideal $c\mathscr{O}_{\mathbb{L}}$ such that π also divides I. But then π also divides d. In particular, letting p be the prime number sitting above π, we get that p divides u_n for all $n\ge 1$. Reducing equation (1.5) modulo p, we get $\pm 1\equiv 0 \pmod p$, so (1.5) has no positive integer solution at all. Thus,

$$I\mid \gcd(\alpha^{2(n+i)}-\zeta_1,\alpha^m-\zeta_2)\quad\text{where}\quad (\zeta_1,\zeta_2)=\left(-(-s)^{n+i}d/c,\zeta_j^{(m,\delta)}\right).$$

By Lemma 5.1, we can take

$$M=6m, \tag{5.4}$$

and then we have that $\max\{2(n+i),m\} < M$ for all $i \in \{0,1,\ldots,k-1\}$. Lemma 4.1 applies with the parameters D, Z, M bounded as in (5.1), (5.2) and (5.4), and we conclude that either:

Condition (i): *The inequality*

$$N_{\mathbb{L}}(I) < \exp(6\cdot D^2\cdot 6\log(Y+2)\sqrt{6m}) < \exp(2000D\log(Y+2)\sqrt{m}) \tag{5.5}$$

holds true for all $I = I_{i,j}^{(m,\delta)}$ *and all our choices for* i, j *and* δ*;*

or

Condition (ii): *There exists* $i \in \{0,\ldots,k-1\}$, $j \in \{1,2\}$, $\delta \in \{\pm\varepsilon\}$ *and* $(x_0,y_0,z_0) \in \mathbb{Z}^3\backslash\{(0,0,0)\}$ *with*

$$\max\{|x_0|,|y_0|,|z_0|\} < 250000(\log(Y+2))^2,$$

such that

$$2(n+i)z_0 + my_0 + x_0 = 0 \tag{5.6}$$

holds.

From now on we analyze each of the above situations (i) and (ii).

5.3. **The case of Condition (i).** From now on, we assume that Condition (i) of the previous Section 5.2 holds.

5.3.1. *A lower bound for k in terms of m.*

Lemma 5.2. *If* $m > 100C_0$*, then*

$$k > \sqrt{m}/(16000\log(Y+2)).$$

Proof. In this case, we have

$$u_m^2 \pm 1 = \gcd\left(u_m^2 \pm 1, \prod_{i=0}^{k-1} u_{n+i}\right).$$

The right-hand side divides

$$\gcd\left(\prod_{i=0}^{k-1}(c\alpha^{n+i} + d\beta^{n+i}), c^2\alpha^{-2m}\prod_{\substack{j\in\{1,2\}\\ \delta\in\{\pm\varepsilon\}}}(\alpha^m - z_{i,j}^{(m,\delta)})\right),$$

which, in turn, divides $\prod_{i,j,\delta} I_{i,j}^{(m,\delta)}$. Taking norms in $\mathbb{L}$ and using (5.5), we get

$$(u_m^2 \pm 1)^D \le \prod_{i,j,\delta} N_{\mathbb{L}}(I_{i,j}^{(m,\delta)}) \le \exp(8000Dk\log(Y+2)\sqrt{m}),$$

so

$$u_m^2 \pm 1 < \exp(8000k\log(Y+2)\sqrt{m}).$$

Using again Lemma 2.5 and the fact that $\alpha > e^{1/3}$, we get

$$\begin{aligned}\exp(m/2) &< \alpha^{3m/2} < \alpha^{2m-2C_0-2} < \frac{\alpha^{2(m-C_0)}}{2} < \alpha^{2(m-C_0)} \pm 1 < u_m^2 \pm 1\\ &< \exp(8000k\log(Y+2)\sqrt{m}),\end{aligned}$$

giving

$$k > \sqrt{m}/(16000\log(Y+2)), \tag{5.7}$$

which is what we wanted. □

5.3.2. *A small prime factor of $\prod_{i=0}^{k-1} u_{n+i}$ and its multiplicity.* By Lemma 2.1, we have $\max\{|u_0|,|u_1|,|u_2|,|u_3|\} > 1$. Let p_0 be the smallest prime factor of $u_0u_1u_2u_3$. Let us write an upper bound on it.

Since

$$|u_2| \le \max\{|u_0|,|u_1|\}(r+1) \le (Y+1)^2,$$

and by a similar argument

$$|u_3| \le \max\{|u_2|,|u_1|\}(r+1) \le (Y+1)^3,$$

it follows that

$$p_0 \le (Y+1)^3. \tag{5.8}$$

Let ℓ_0 be the period of $\{u_n\}_{n\ge 0}$ modulo p_0. By Lemma 2.2,

$$\ell_0 < p_0^2 < (Y+1)^6. \tag{5.9}$$

Since p_0 divides some term of the sequence $\{u_n\}_{n\ge 1}$ (more precisely, one of the first four), it follows that among $u_n, u_{n+1}, \ldots, u_{n+k-1}$, there are at least $\lfloor k/\ell_0 \rfloor$ of such terms which are all multiples of p_0. Assuming $k \ge 2\ell_0$, it follows that

$$\mathrm{ord}_{p_0}(u_nu_{n+1}\cdots u_{n+k-1}) \ge \lfloor k/\ell_0 \rfloor \ge k/(2\ell_0).$$

Combining the last inequality above with (5.7), we obtain right away the following lemma.

Lemma 5.3. *Assume that* $m > 100C_0$ *and that*

$$m > 2 \cdot 10^9 \ell_0^2 (\log(Y+2))^2. \tag{5.10}$$

Then

$$\operatorname{ord}_{p_0}(u_n u_{n+1} \cdots u_{n+k-1}) \geq \frac{\sqrt{m}}{32000\ell_0 \log(Y+2)}. \tag{5.11}$$

The condition (5.10) insures that $k > \sqrt{m}/(16000\log(Y+2)) > 2\ell_0$. Using (5.9), we arrive at the conclusion that (5.10) is always satisfied for some p_0 if $m > 2 \cdot 10^9 (Y+1)^{14}$ (and this condition implies automatically that $m > 100C_0$), and the lower bound from (5.11) is at least $\sqrt{m}/(32000(Y+1)^7)$, but in practice better bounds are possible which is why we formulated Lemma 5.3 in terms of the parameter ℓ_0.

5.3.3. *A p-adic linear form.* We recall a version of the p-adic linear form in logarithms due to Kunrui Yu. Let $\alpha_1, \ldots, \alpha_l$ be nonzero algebraic numbers in a field $\mathbb{M}$ of degree D_1. Let p be a prime, π a prime ideal of $\mathscr{O}_{\mathbb{M}}$ lying above p, having ramification e and residual degree f. Let $b_1, \ldots, b_l$ be nonzero integers. Put

$$B \geq \max\{|b_1|, \ldots, |b_l|, 3\}.$$

Let

$$H_j \geq \max\{h(\alpha_j), \log p\} \qquad \text{for all} \qquad j = 1, \ldots, l. \tag{5.12}$$

Let

$$\Lambda = \prod_{i=1}^{l} \alpha_i^{b_i} - 1,$$

and assume that $\Lambda \neq 0$. The following result of Kunrui Yu [11] bounds the exponent of π in the prime ideal factorization of Λ inside $\mathscr{O}_{\mathbb{M}}$.

Lemma 5.4. *With the above notations, we have*

$$\operatorname{ord}_\pi(\Lambda) \leq 19(20\sqrt{l+1}D_1)^{2(l+1)} e^{l-1} \left(\frac{p^f}{(f\log p)^2}\right) \log(e^5 l D_1) H_1 \cdots H_l \log B.$$

5.3.4. *An upper bound on k.* We let π_0 be any prime ideal dividing p_0 in $\mathscr{O}_{\mathbb{L}}$, where $\mathbb{L}$ is a field containing α and all $\zeta_{1,2}^{(m,\pm\varepsilon)}$. We are interested in an upper bound for

$$\begin{aligned} \mathrm{ord}_{\pi_0}(u_m^2 \pm 1) &= \sum_{\substack{j\in\{1,2\}\\ \delta\in\{\pm\varepsilon\}}} \mathrm{ord}_{\pi_0}(\alpha^m - z_j^{(m,\delta)}) \\ &\le 4\max\{\mathrm{ord}_{\pi_0}(\alpha^m - \zeta) : \zeta \in \{z_{1,2}^{(m,\pm\varepsilon)}\}\}. \end{aligned} \tag{5.13}$$

Note that since $u_m^2 \pm 1 = \prod_{i=1}^{k-1} u_{n+i}$ is nonzero, it follows that $\alpha^m - \zeta \neq 0$ for all $\zeta \in \{z_{1,2}^{(m,\pm\varepsilon)}\}$. To bound the right–hand side of (5.13), we use Lemma 5.4. We take $l = 2$, $\alpha_1 = \alpha^{-1}$, $\alpha_2 = \zeta$, $b_1 = m$, $b_2 = 1$. We can take $\mathbb{M} := \mathbb{K}(\zeta)$ which is of degree $D_1 \le 8$. By Lemma 2.3 and inequality (5.8), we can take

$$H_1 = H_2 := 6\log(Y+2),$$

and the inequality (5.12) is satisfied for our situation. Since $ef \le D_1$, we get

$$\mathrm{ord}_{\pi_0}(u_m^2 \pm 1) \le 4\cdot 19(20\sqrt{38})^6 \cdot 6\frac{p_0^8}{(\log p)^2}\log(16e^5)(8\log(Y+2))^2\log m,$$

so

$$\mathrm{ord}_{\pi_0}(u_m^2 \pm 1) < 1.5\cdot 10^{20}\left(\frac{p_0^8}{(\log p_0)^2}\right)(\log(Y+2))^2\log m.$$

Since clearly

$$\mathrm{ord}_{\pi_0}(u_m^2 \pm 1) \ge \mathrm{ord}_{p_0}(u_m^2 \pm 1) = \mathrm{ord}_{p_0}(u_n u_{n+1}\cdots u_{n+k-1}),$$

Lemma 5.3 implies the following result.

Lemma 5.5. *Assume that $m > 100C_0$ and that*

$$m > 2\cdot 10^9 \ell_0^2(\log(Y+2))^2.$$

Then

$$\frac{\sqrt{m}}{32000\ell_0\log(Y+2)} < 1.5\cdot 10^{20}\left(\frac{p_0^8}{(\log p_0)^2}\right)(\log(Y+2))^2\log m. \tag{5.14}$$

At this point the theorem is proved since inequality (5.14) gives a bound on m. If we want a specific bound, we may assume that $m > 3\cdot 10^8(Y+1)^6$, and then, using the fact that $p_0 \le (Y+2)^3$ and the fact that the function $t \mapsto t^8/(\log t)^2$ is increasing for $t \ge 2$, we get that

$$\frac{\sqrt{m}}{32000(Y+1)^7} < 1.5\cdot 10^{20}\left(\frac{(Y+2)^{24}}{(\log(Y+2)^3)^2}\right)(\log(Y+2))^2\log m,$$

which gives

$$\sqrt{m} < 6\cdot 10^{23}(Y+2)^{31}\log m = 12\cdot 10^{23}(Y+2)^{31}\log\sqrt{m}.$$

It is known that if $x/\log x < A$ for some $A > 3$, then $x < 2A\log A$. Applying this with $x := \sqrt{m}$ and $A := 6\cdot 10^{23}(Y+2)^{24}$, we get

$$\begin{aligned}\sqrt{m} &< 2\cdot 12\cdot 10^{23}(Y+2)^{31}(\log(12\cdot 10^{23})+31\log(Y+2))\\ &< 24\cdot 71\cdot 10^{23}(Y+2)^{31}\log(Y+2)\\ &< 2\cdot 10^{26}(Y+2)^{32}.\end{aligned}$$

In the above, we used that

$$\begin{aligned}\log(12\cdot 10^{23})+31\log(Y+2) &\leq \left(\frac{\log(12\cdot 10^{23})}{\log 4}+31\right)\log(Y+2)\\ &< 71\log(Y+2).\end{aligned}$$

Hence,

$$m < 10^{53}(Y+2)^{64},$$

which completes the proof in the case of Condition (i).

5.4. **The case of Condition (ii).** From now on, we work under the Condition (ii).

5.4.1. *The case when $y_0z_0 = 0$.* We look at the relation (5.6). If both $y_0 = z_0 = 0$, then $x_0 = 0$, so $(x_0, y_0, z_0) = (0,0,0)$, which is a contradiction. If $z_0 = 0$, then $|y_0| \geq 1$, so

$$m \leq |x_0| \leq 250000(\log(Y+2))^2,$$

which is a better inequality than (1.6). If $y_0 = 0$, then $|z_0| \geq 1$, so

$$2(n+i)|z_0| \leq |x_0| \leq 250000(\log(Y+2))^2,$$

giving

$$n < 125000(\log(Y+2))^2. \tag{5.15}$$

Assume that $m > 100C_0$. Then Lemmas 2.4 and 2.5 show that

$$\alpha^{nk+(k(k-1)/2+kC_0} > |u_{n+1}|\cdots|u_{n+k}|-1 \geq u_m^2/2 \geq \alpha^{2m-2-2C_0},$$

so

$$k^2+(2n+2C_0)k > 2nk+k(k-1)+2kC_0 > 2(2m-2-C_0) > 2m.$$

The left-hand side above is less than $(k+1000C_0^3)^2$ because

$$(k+1000C_0^3)^2 > k^2+(2000C_0^3)k,$$

and

$$2000C_0^3 > 2n+2C_0, \tag{5.16}$$

an inequality implied by (5.15). We thus get

$$k+2000C_0^3 > \sqrt{2m}.$$

Assuming that

$$m > 10^{13}(\log(Y+2))^6, \tag{5.17}$$

we have that

$$k > \sqrt{2m}-2000C_0^3 > \sqrt{m}.$$

We are now in the conditions of Lemma 5.2, and from now on the rest of the proof from the preceding case applies and leads to the desired inequality (1.6) on m.

From now on, we assume that

$$y_0z_0 \neq 0.$$

5.4.2. *Bounding k.* Since $y_0z_0 \neq 0$, we have

$$m \le m|y_0| \le 2(n+k)|z_0|+|x_0| < 10^6(\log(Y+2))^2(n+k+1). \tag{5.18}$$

Thus, we may assume that $n+k$ is large. Assuming that $n+k > 100C_0$, we get, using again Lemmas 2.4 and 2.5, that

$$|u_n|\cdots|u_{n+k-1}| \ge |u_{n+\lfloor k/2\rfloor}||u_{n+\lfloor k/2\rfloor+1}|\cdots|u_{n+k-1}| \ge \alpha^{(k/2)(n+\lfloor k/2\rfloor-C_0)},$$

while

$$u_m^2 \pm 1 \le 2u_m^2 \le \alpha^{2m+2+2C_0}.$$

We thus get, assuming that $m > 100C_0$, that

$$(k/2)(n+\lfloor k/2\rfloor-C_0) < 2m+2+2C_0 < 3m < 3\cdot 10^6(\log(Y+2))^2(n+k+1).$$

Since $n+k > 100C_0$, we get that $n+\lfloor k/2\rfloor-C_0 > (n+k+1)/3$, so the above inequality gives

$$k < 2\cdot 10^7(\log(Y+2))^2.$$

We record this as a lemma.

Lemma 5.6. *Assuming*

$$m > 100C_0, \tag{5.19}$$

we have that

$$m < 10^6(\log(Y+2))^2(n+k+1). \tag{5.20}$$

Furthermore, if also

$$n+k > 100C_0, \tag{5.21}$$

then

$$k < 2\cdot 10^7(\log(Y+2))^2. \tag{5.22}$$

5.4.3. *A linear form in archimedian logarithms.* From now on, we assume that both (5.19) and (5.21) hold true. We may assume it, because if (5.19) is not true then we have an estimate for m much stronger than (1.6). And if (5.19) is true but (5.21) is not then (5.20) again implies a bound much sharper than (1.6). As a consequence of the lemma above, we have (5.20) and (5.22).

We may also assume that n is large; precisely, that

$$n > 100\log(Y+2). \tag{5.23}$$

Indeed, if this is not true, then (5.20) and (5.22) again imply a much sharper bound than (1.6).

We look at

$$u_{n+i} = c\alpha^{n+i}\left(1+\frac{(-s)^{n+i}d}{c\alpha^{2n+2i}}\right) := c\alpha^{n+i}(1+\zeta_{n,i}).$$

Note that

$$|\zeta_{n,i}| = \left|\frac{d/c}{\alpha^{2n+2i}}\right| < \frac{1}{\alpha^n},$$

provided $\alpha^n > |d/c|$, which holds whenever (5.23) is true, because

$$\log|d/c| \le 2h(c/d) \le 12\log(Y+2)$$

(by Lemma 2.3), while also $\alpha \ge (1+\sqrt{5})/2$. Thus, equation (1.5) is

$$c^k\alpha^{kn+k(k-1)/2}\prod_{i=0}^{n}(1+\zeta_{n,i}) \pm 1 = c^2\alpha^{2m}(1+\zeta_{m,0})^2.$$

If $|x| < 1/2$, then $|\log(1+x)| < 2|x|$. Thus,

$$\log \prod_{i=0}^{k-1}(1+\zeta_{n,i}) \le 2\sum_{i=0}^{k-1}|\zeta_{n,i}| < \frac{2k}{\alpha^n} < \frac{1}{\alpha^{n/2}},$$

where the last inequality holds provided that

$$\alpha^{n/2} > 4\cdot 10^7(\log(Y+2))^2,$$

because the right-hand side above is an upper bound for $2k$ by Lemma 5.6. The last inequality above is certainly satisfied whenever (5.23) holds. Since $\alpha^{n/2} > 2$, it follows that

$$|\prod_{i=0}^{k-1}(1+\zeta_{n,i}) - 1| < \exp\left(\frac{1}{\alpha^{n/2}}\right) - 1 < \frac{2}{\alpha^{n/2}}.$$

Similarly,

$$|(1+\zeta_{m,0})^2 - 1| < \frac{2}{\alpha^{m/2}}.$$

Thus, we may write

$$u_n\cdots u_{n+k-1} = c^k\alpha^{nk+k(k-1)/2}(1+\eta_{n,k}) \quad \text{and} \quad u_m^2 = c^2\alpha^{2m}(1+\eta_m),$$

where

$$|\eta_{n,k}| < \frac{2}{\alpha^{n/2}} \quad \text{and} \quad |\eta_m| < \frac{2}{\alpha^{m/2}}.$$

Thus, equation (1.5) is

$$c^k\alpha^{nk+k(k-1)/2}(1+\eta_{n,k}) \pm 1 = c^2\alpha^{2m}(1+\eta_m),$$

or

$$c^{k-2}\alpha^{nk+k(k-1)/2-2m}(1+\eta_{n,k}) = (1+\eta_m) \mp \frac{1}{c^2\alpha^{2m}}.$$

We have

$$\frac{1}{2} < |1+\eta_{n,k}| < \frac{3}{2}, \quad \frac{1}{2} < |1+\eta_m| < \frac{3}{2}, \quad \frac{1}{c^2\alpha^{2m}} < \frac{1}{\alpha^m} < \frac{1}{4}. \tag{5.24}$$

Here we used the inequality

$$c^2\alpha^m \ge 1,$$

which is true because $\log(c^2) \ge -4h(c) \ge -4C_0$ (by Lemma 2.3) and on the other hand $\log(\alpha^m) \ge 100C_0 \log\frac{1+\sqrt{5}}{2} > 4C_0$ by (5.19). Using (5.24), we deduce

$$\frac{1}{6} < c^{k-2}\alpha^{nk+k(k-1)/2-2m} < 4.$$

Hence,

$$\begin{aligned} |c^{k-2}\alpha^{nk+k(k-1)/2-2m}-1| &< \frac{1}{c^2\alpha^{2m}}+|\eta_m|+c^{k-2}\alpha^{nk+k(k-1)/2-2m}|\eta_{n,k}| \\ &< \frac{1}{\alpha^m}+\frac{2}{\alpha^{m/2}}+\frac{8}{\alpha^{n/2}} \\ &< \frac{11}{\alpha^{\min\{m/2,n/2\}}}. \qquad (5.25) \end{aligned}$$

We want to estimate the left-hand side from below using the theory of linear forms in logarithms. But we need to ensure that the left-hand side is nonzero. It is not possible that $(k-2, nk+k(k-1)/2, 2m) = (0,0)$, since this leads to $k=2$ and $2n+1=2m$, which is impossible. Thus, if the left-hand side of (5.25) is 0, then c and α are multiplicatively dependent. But since d is conjugate to c and $\beta = \pm\alpha^{-1}$ is conjugate to α, it follows that also d and α are multiplicatively dependent and therefore c/d and α are multiplicatively dependent, which is not possible.

The following result is (a slightly weaker version of) Corollary 2.3 from Matveev [8].

Theorem 5.7. *Let $\mathbb{L}$ be a number field of degree D over $\mathbb{Q}$, $\zeta_1,\dots,\zeta_t$ be positive real numbers of $\mathbb{L}$, and $b_1,\dots,b_t$ be integers. Put*

$$\Lambda := \zeta_1^{b_1}\cdots\zeta_t^{b_t}-1.$$

Let $A_1,\dots,A_t,B$ be real numbers such that

$$A_i \geq \max\{Dh(\zeta_i), |\log\zeta_i|, 0.16\}, \qquad i=1,\dots,t,$$
$$B \geq \max\{|b_1|,\dots,|b_t|\}.$$

Then, assuming that $\Lambda \neq 0$, we have

$$|\Lambda| > \exp(-1.4\cdot 30^{t+3}\cdot t^{4.5}\cdot D^2(1+\log D)(1+\log B)A_1\cdots A_t).$$

For our application, we take $t=2$, $\zeta_1 := c$, $\zeta_2 := \alpha$, $b_1 := k-2$, $b_2 := nk+k(k-1)/2-2m$. We can take $\mathbb{L} = \mathbb{Q}(\alpha)$; in particular, $D \leq 2$. As for the numbers A_1, A_2, we can take

$$A_1 = A_2 = 12\log(Y+2).$$

We take $B = \max\{m, nk+k^2\}$. Then

$$\log|\Lambda| > -1.4\cdot 30^5\cdot 2^{4.5}\cdot 2^2(1+\log 2)(1+\log B)(12\log(Y+2))^2.$$

Thus,

$$\log|\Lambda| > -10^{12}(\log(Y+2))^2(1+\log B).$$

Comparing this with (5.25), we get

$$\min\{n/2, m/2\}\log\alpha - \log 11 < 10^{12}(\log(Y+2))^2(1+\log B).$$

We then get that

$$\min\{n,m\} \le 5\cdot 10^{12}(\log(Y+2))^2(1+\log B). \tag{5.26}$$

We may assume that $n+k+1 > 2\cdot 10^6(\log(Y+2))^2$, otherwise Lemma 5.6 gives us

$$m < 4\cdot 10^{12}(\log(Y+2))^4,$$

which is better than the inequality (1.6). Then Lemma 5.6 shows that

$$m < (n+k+1)^2 \quad \text{therefore} \quad \log B \le 2\log(n+k+1).$$

Thus,

$$\begin{aligned} \min\{n,m\} &\le 5\cdot 10^{12}(\log(Y+2))^2(1+2\log(n+k+1)) \\ &\le 1.5\cdot 10^{13}(\log(Y+2))^2\log(n+k+1). \end{aligned} \tag{5.27}$$

Assume first that $m \le n$. By Lemma 5.1, we get

$$n+k+1 \le 3m+1 < 4m,$$

therefore with $x = 4m$, inequality (5.27) implies

$$x < 6\cdot 10^{13}(\log Y+2))^2\log x.$$

With $A = 6\cdot 10^{13}(\log(Y+2))^2$, we have $x < A\log x$, an inequality which implies that $x < 2A\log A$. Thus,

$$\begin{aligned} 4m &< 12\cdot 10^{13}(\log((Y+2))^2(\log(6\cdot 10^{13})+2\log\log(Y+2)) \\ &< 12\cdot 34\cdot 10^{13}(\log(Y+2))^3, \end{aligned}$$

giving

$$m < 10^{16}(\log((Y+2))^3,$$

which is better than estimate (1.6).

Assume next that $n \le m$. Then inequality (5.27) shows that

$$n \le 1.5\cdot 10^{13}(\log(Y+2))^2\log(n+k+1).$$

With (5.22) we get

$$\begin{aligned} n+k+1 &< 1.5\cdot 10^{13}(\log(Y+2))^2\log(n+k+1) \\ &+ \log(2\cdot 10^6(\log(Y+2))^3)+1 \\ &< 2\cdot 10^{13}(\log(Y+2))^3\log(n+k+1). \end{aligned}$$

As we said, for $A>2$ the inequality $x<A\log x$ implies $x<2A\log A$. Taking $A=2\cdot 10^{13}(\log(Y+2))^2$ and $x:=n+k+1$, we get

$$\begin{aligned} n+k+1 &< 4\cdot 10^{13}(\log(Y+2))^2(13\log 10+2\log\log(Y+2)) \\ &< 2\cdot 10^{15}(\log(Y+2))^3, \end{aligned}$$

which together with (5.20) gives

$$m<2\cdot 10^{22}(\log(Y+2))^5,$$

which is better than the inequality (1.6). This finishes the proof of the theorem.

6. THE PROOF OF THEOREM 1.2

Plugging in our values, we get $Y=9$, so $m<10^{53}\cdot 11^{64}<10^{120}$. The period of $\{u_m\}_{m\ge 0}$ modulo 11 is 10 and $u_6\equiv 0 \pmod{11}$. We show that $k\le 9$. For if not, then $[n,n+k-1]$ contains a number $n+i$ congruent to 6 modulo 10 so $11\mid u_n\cdots u_{n+k-1}$. We get that

$$u_m^2\equiv \pm 1 \pmod{11}.$$

The congruence $u_m^2\equiv -1 \pmod{11}$ is not possible since 11 is a prime congruent to 3 modulo 4 (so, -1 is not a quadratic residue modulo 11). The congruence $u_m^2\equiv 1 \pmod{11}$ implies $u_m\equiv \pm 1 \pmod{11}$. However, the first 10 values of $\{u_n\}_{n\ge 1}$ modulo 11 are

$$2,7,9,5,3,8,0,8,8,5$$

none of which is $\pm 1 \pmod{11}$, so by periodicity we deduce that there is no positive integer m such that $u_m\equiv \pm 1 \pmod{11}$. So, indeed $k\le 9$.

We next show that either $n\le 43$ or $m\le 18$. Assume this is not so. For a positive integer ℓ, we have

$$u_\ell = c\alpha^\ell\left(1+\frac{(-1)^\ell d}{c\alpha^{2\ell}}\right). \tag{6.1}$$

Further,

$$\left|\frac{d}{c}\right| = \frac{23+9\sqrt{5}}{23-9\sqrt{5}} < 15. \tag{6.2}$$

In formula (6.1), we give ℓ the values $n+i$ for $i=0,1,\dots,k-1$ and multiply the resulting expressions to get that

$$\begin{aligned} u_n\cdots u_{n+k-1} &= c^k\alpha^{n+(n+1)+\cdots+(n+k-1)}\prod_{i=0}^{k-1}\left(1+\frac{(-1)^{n+i}d}{c\alpha^{2n+2i}}\right)\\ &= c^k\alpha^{nk+k(k-1)/2}(1+\zeta_{n,k}), \end{aligned} \tag{6.3}$$

where trivially

$$|\zeta_{n,k}| < 2^k\frac{|d/c|^k}{\alpha^{2n}} < \frac{30^9}{\alpha^{2n}} < \frac{1}{\alpha^{2n-64}}. \tag{6.4}$$

Similarly,

$$u_m^2 = c^2\alpha^{2m}\left(1+\frac{(-1)^m d/c}{\alpha^{2m}}\right)^2 = c^2\alpha^{2m}(1+\zeta_m), \tag{6.5}$$

where

$$|\zeta_m| < \frac{3|d/c|^2}{\alpha^{2m}} < \frac{775}{\alpha^{2m}} < \frac{1}{\alpha^{2m-14}}. \tag{6.6}$$

Further, we use the fact that

$$\alpha^{\ell-2} < u_\ell < \alpha^{\ell-1} \qquad \text{for all} \qquad \ell\ge 4, \tag{6.7}$$

which is easy to check by induction on ℓ. Since

$$u_nu_{n+1}\cdots u_{n+k-1}u_m^{-2}-1 = \pm\frac{1}{u_m^2},$$

we use (6.3) and (6.5) to get that

$$c^{k-2}\alpha^{nk+k(k-1)/2-2m}\left(\frac{1+\zeta_{n.k}}{1+\zeta_m}\right)-1 = \pm\frac{1}{u_m^2},$$

which can be rewritten as

$$c^{k-2}\alpha^{nk+k(k-1)/2-2m}-1 = \pm\frac{(1+\zeta_m)}{(1+\zeta_{n,k})u_m^2}+\frac{\zeta_m}{(1+\zeta_{n,k})}-\frac{\zeta_{n,k}}{1+\zeta_{n,k}}.$$

Taking absolute values and using estimates (6.4), (6.6) and (6.7) together with the fact that $\max\{|\zeta_m|,|\zeta_{n,k}|\}<1/2$ in our range of variables $n\ge 44$ and $m\ge 19$, we get

$$\begin{aligned}\left|c^{k-2}\alpha^{nk+k(k-1)/2-2m}-1\right| &\le \left(\frac{3/2}{1/2}\right)\frac{1}{\alpha^{2(m-2)}}+\left(\frac{1}{1/2}\right)\frac{1}{\alpha^{2m-14}}\\ &+ \left(\frac{1}{1/2}\right)\frac{1}{\alpha^{2n-64}}\\ &< \frac{7}{\alpha^{\min\{2n-64,2m-14\}}}\\ &< \frac{1}{\alpha^{\min\{2n-69,2m-19\}}}.\end{aligned}$$

Since we are assuming that $n \ge 44$ and $m \ge 19$, the right–hand side above is $< 1/2$. It is known that if $|e^x - 1| < y$ with $y < 1/2$, then $|x| < 2y$. Applying this to our situation, we get

$$\begin{aligned}|(k-2)\log c-(kn+k(k-1)/2-2m)\log\alpha| &< \frac{2}{\alpha^{\min\{2n-69,2m-19\}}}\\ &< \frac{1}{\alpha^{\min\{2n-71,2m-21\}}}.\end{aligned} \tag{6.8}$$

If $k = 2$, we then get that

$$|2n+1-2m|\log\alpha < \frac{1}{\alpha^{\min\{2n-71,2m-21\}}}.$$

Since $2n+1 \ne 2m$, the left-hand side is at least $\log\alpha > 0.48$, and, for $n \ge 44$ and $m \ge 19$, the right-hand side is at most $\alpha^{-17} < 0.0003$, a contradiction. Hence, $k \ne 2$.

Dividing (6.8) by $(k-2)\log\alpha$, we get

$$\begin{aligned}\left|\frac{kn+k(k-1)/2-2m}{k-2}-\frac{\log c}{\log\alpha}\right| &< \frac{1}{|k-2|(\log\alpha)\alpha^{\min\{2n-71,2m-21\}}}\\ &< \frac{1}{\alpha^{\min\{2n-73,2m-23\}}}.\end{aligned}$$

The continued fraction of $\log c/\log\alpha$ is $[-1,12,5,\ldots]$ with the second convergent being $-11/12$. Since $|\log c/\log\alpha + 11/12| > 0.001$, and since $|k-2| \le 7$ (because $k \le 9$), we infer, from the properties of the continued fractions, that

$$0.001 < \frac{1}{\alpha^{\min\{2n-73,2m-23\}}},$$

giving either $n < 44$ or $m < 19$, which is what we wanted.

If $m \geq 19$, then $n \leq 43$, so

$$\alpha^{2m-6} \leq \frac{\alpha^{2(m-2)}}{2} \leq \frac{u_m^2}{2} \leq u_m^2 \pm 1 = u_n \cdots u_{n+k-1} \leq u_{n+8}^9 \leq u_{51}^9 < \alpha^{450},$$

giving $m < 228$. So, in all cases $m < 228$. As for n, we either have $n < 44$, or $n \geq 44$. But if $n \geq 44$, then $m \leq 18$. Since $\alpha^{n-2} < u_n \leq u_m^2 + 1 < 2u_m^2 < \alpha^{2m} \leq \alpha^{36}$, we get that $n < 38$, contradicting that $n \geq 44$.

So, all solutions have $k \leq 9$, $m \leq 227$, and $n \leq 43$. A quick computation now confirms that the solutions listed in the statement of Theorem 1.2 are the only ones.

Acknowledgements

We thank the referee for careful reading and detecting a flaw in the initial version. We also thank Karim Belabas and Michael Mossinghoff for helpful suggestions.

References

[1] F. Beukers, The multiplicity of binary recurrences, Compositio Math. 40: 251–267, 1980.
[2] J. J. Bravo, T. Komatsu and F. Luca, On the distance between products of consecutive Fibonacci numbers and powers of Fibonacci numbers, *Indag. Math.*, 24:181–198, 2013.
[3] S. Guzman and F. Luca, Linear combinations of factorials and S-units in a Binary Recurrence Sequence, *Ann. Math. Québec*, 38: 169–188, 2014.
[4] T. Komatsu, F. Luca and Y. Tachiya, On the multiplicative order of F_{n+1}/F_n modulo F_m, in “Proc. of the Integers Conference 2011”, *Integers* 12: A8, 2012/2013.
[5] D. H. Lehmer, Factorization of Certain Cyclotomic Functions, *Ann. Math. II* 34: 461-479, 1933.
[6] D. Marques, The Fibonacci version of the Brocard-Ramanujan Diophantine equation, *Far East J. Math. Sci.* 56: 219–224, 2011.
[7] D. W. Masser, Linear relations on algebraic groups, in “New advances in transcendence theory (Durham, 1986)”, 248–262, Cambridge Univ. Press, Cambridge, 1988.
[8] E. M. Matveev, An Explicit Lower Bound for a Homogeneous Rational Linear Form in the Logarithms of Algebraic Numbers II, *Izv. Math.* 64: 1217–1269, 2000.
[9] L. Szalay, Diophantine equations with binary recurrences associated to Brocard-Ramanujan problem, *Portugaliae Math.*, 69: 213–220, 2012.
[10] M. Szikszai, A variant of the Brocard-Ramanujan equation for Lucas sequences, *Preprint*, 2016.
[11] K. Yu, p-adic logarithmic forms and group varieties II, *Acta Arith.* 89: 337–378, 1999.

A. BÉRCZES
INSTITUTE OF MATHEMATICS, UNIVERSITY OF DEBRECEN
H-4010 DEBRECEN, P.O. BOX 12, HUNGARY

Email address: berczesa@science.unideb.hu

YU. F. BILU
INSTITUT DE MATHÉMATIQUES DE BORDEAUX
UNIVERSITÉ DE BORDEAUX AND CNRS, TALENCE, FRANCE

Email address: Yuri.Bilu@math.u-bordeaux1.fr

F. LUCA
SCHOOL OF MATHEMATICS
UNIVERSITY OF THE WITWATERSRAND
PRIVATE BAG X3, WITS 2050, SOUTH AFRICA AND
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCES
UNIVERSITY OF OSTRAVA
30 DUBNA 22, 701 03 OSTRAVA 1, CZECH REPUBLIC

Email address: florian.luca@wits.ac.za