Collectanea Mathematica (electronic version): http://www.mat.ub.es/CM

Collect. Math. **53**, 2 (2002), 133–156

Euler indicators of binary recurrence sequences

Florian Luca

Mathematical Institute, UNAM, Ap. Postal 61-3 (Xangari)

CP 58 089, Morelia, Michoacán, MEXICO

E-mail: fluca@matmor.unam.mx

Received July 6, 2000. Revised January 8, 2002

Abstract

In this paper, we show that if $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ are two non-degenerate binary recurrent sequences of integers such that $(v_n)_{n\geq 0}$ satisfies some technical assumptions, then the diophantine equation $|v_n| = \phi(|u_m|)$ has only finitely many effectively computable positive integer solutions (m, n). Here, for a non-zero integer k we use $\phi(k)$ to denote the Euler function of k.

1. Introduction

Let r and s be two non-zero integers with $r^2 + 4s > 0$. A *binary recurrence sequence* $(u_n)_{n\geq 0}$ is a sequence such that u_0 and u_1 are integers and

$$u_{n+2} = ru_{n+1} + su_n \qquad \text{for all } n \geq 0.$$

Clearly, u_n is an integer for all $n \geq 0$. Let α and β denote the two roots of the equation

$$x^2 - rx - s = 0.$$

It is well known that

$$u_n = a\alpha^n + b\beta^n \qquad \text{for all } n \geq 0 \tag{1}$$

where a and b are two constants which can be determined using formula (1) with $n = 0,\ 1$. The binary recurrence sequence $(u_n)_{n\geq 0}$ is called *nondegenerate* if $ab \neq 0$ and α/β is not a root of unity.

Keywords: Euler indicator, Lucas sequences.

MSC2000: 11A25, 11B39, 11D75.

If $(r,\ s) = 1$, $u_0 = 0$ and $u_1 = 1$, then $(u_n)_{n\geq 0}$ is called a *Lucas sequence of the first kind*. For such sequences, formula (1) is

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{for all } n \geq 0. \tag{2}$$

If $(r,\ s) = 1$, $u_0 = 2$ and $u_1 = r$, then $(u_n)_{n\geq 0}$ is called a *Lucas sequence of the second kind*. For such sequences, formula (1) is

$$u_n = \alpha^n + \beta^n \qquad \text{for all } n \geq 0. \tag{3}$$

Let $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ be two nondegenerate binary recurrence sequences. Assume that

$$u_{n+2} = r_1 u_{n+1} + s_1 u_n \qquad \text{for } n \geq 0 \tag{4}$$

and

$$v_{n+2} = r_2 v_{n+1} + s_2 v_n \qquad \text{for } n \geq 0 \tag{5}$$

where $r_1^2 + 4s_1 > 0$ and $r_2^2 + 4s_2 > 0$. Let $\alpha_1,\ \beta_1$ and $\alpha_2,\ \beta_2$ be the roots of the characteristic equation

$$x^2 - r_1 x - s_1 = 0$$

and

$$x^2 - r_2 x - s_2 = 0,$$

respectively. Assume that $|\alpha_1| > |\beta_1|$ and that $|\alpha_2| > |\beta_2|$. In particular, $|\alpha_i| > 1$ for $i = 1,\ 2$.

In what follows, we shall work with pairs of binary recurrence sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ satisfying at least one of the following assumptions:

Assumptions

*A*1) *Not all four numbers* $\alpha_1,\ \beta_1,\ \alpha_2,\ \beta_2$ *are integers.*

*A*2) $\log|\alpha_1|$ *and* $\log|\alpha_2|$ *are linearly independent over* $\mathbb{Q}$.

*A*3) $|\alpha_1| > \max\,(|\beta_1|^2,\ |\beta_2|^2) > 1$.

For any positive integer k, let $\phi(k)$ be the Euler totient function of k. Our main result is the following:

Theorem

Let $(u_n)_{n\geq 0}$ *be a nondegenerate binary recurrence sequence. Let* $(v_n)_{n\geq 0}$ *be a binary recurrence sequence satisfying one of the following two conditions:*

(i) $(v_n)_{n\geq 0}$ *is a Lucas sequence of the second kind;*

(ii) $(v_n)_{n\geq 0}$ *is such that* $(r_2,\ s_2)$ *is odd and* s_2 *is even.*

Moreover, assume that the pair of sequences $(u_n)_{n\geq 0}$ *and* $(v_n)_{n\geq 0}$ *satisfies at least one of the assumptions A*1*-A*3*.*

Let a *and* b *be two nonzero integers. Then, the equation*

$$\phi\big(|au_m|\big) = |bv_n| \tag{6}$$

has finitely many solutions $(m,\ n)$*. Moreover, there exists a computable constant* C *depending only on* $a,\ b$ *and the sequences* $(u_n)_{n\geq 0}$ *and* $(v_n)_{n\geq 0}$ *such that all solutions of equation* (6) *satisfy* $\max(m,\ n) < C$.

It would be nice if one could prove the above theorem without any of the assumptions A1-A3. Unfortunately, as the following example suggests, such a result would be very hard to prove.

Example 1: Let $v_n = u_n = 2^n - 1$ for all $n \geq 0$. Let $a = 1$ and $b = 2$. Equation (6) becomes

$$\phi\big(2^n - 1\big) = 2\big(2^m - 1\big). \tag{7}$$

Notice that if $n = p$ is a prime such that $u_p = 2^p - 1$ is a prime (that is, if u_p is a Mersenne prime), then equation (7) is satisfied for $n = p$ and $m = p - 1$. However, it is not known that there are only finitely many Mersenne primes. In fact, the classical conjecture is that there are infinitely many Mersenne primes.

We also present the following results:

Proposition 1

The only solutions of the equation

$$\phi\Big(a \cdot \frac{10^m - 1}{9}\Big) = b \cdot \frac{10^n - 1}{9} \qquad 1 \leq a,\ b \leq 9 \text{ and } m,\ n \geq 1 \tag{8}$$

are given by $m = n = 1$ and $b = \phi(a)$.

Notice that Proposition 1 asserts that the only positive integers x such that both x and $\phi(x)$, have only one distinct digit (when represented in the decimal system), are precisely the integers x having only one digit.

Proposition 2

Let $(F_n)_{n\geq 0}$ be the Fibonacci sequence given by $F_0 = 0,\ F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. Also let $(L_n)_{n\geq 0}$ be the Lucas sequence given by $L_0 = 2,\ L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$. Then, the only solutions of the equation

$$\phi(L_m) = L_n \tag{9}$$

are $(m,\ n) = (0,\ 1),\ (1,\ 1),\ (2,\ 0),\ (3,\ 0)$.

Moreover, the only solutions of the equation

$$\phi(F_m) = L_n \tag{10}$$

are $(m,\ n) = (1,\ 1),\ (2,\ 1),\ (3,\ 1),\ (4,\ 0),\ (5,\ 3),\ (6,\ 3)$.

It also follows, by the theorem, that there are only finitely many Fibonacci and Lucas numbers whose Euler totient function has only one distinct digit when represented in the decimal system. That is, each one of the equations

$$\phi(F_m) = b \cdot \frac{10^n - 1}{9} \qquad 1 \le b \le 9 \tag{11}$$

and

$$\phi(L_m) = b \cdot \frac{10^n - 1}{9} \qquad 1 \le b \le 9 \tag{12}$$

has only finitely many solutions $(m,\ n,\ b)$. In fact, following the idea of the proof of the Theorem, one can compute upper bounds for all the solutions of equations (11) or (12). The upper bounds obtained in such a way are, most likely, very large. An elementary treatment of the above two equations would certainly be of interest.

It might be worth mentioning that one can conclude that an equation such as (6) has only finitely many solutions even in instances when none of the assumptions A1-A3 is satisfied. For example, in [3], we found all solutions of the equation

$$\phi\big(|x^m + y^m|\big) = \big|x^n + y^n\big| \tag{13}$$

where x and y are integers and m and n are positive integers. Aside from some trivial solutions for which $m = n = 1$ and $|x + y| = 1$ and from two parametric families of solutions for which $x = y \in \{2,\ 3\}$ and $m = n + 1$, the only solution of equation (13) is $(x,\ y,\ m,\ n) = (3,\ 1,\ 2,\ 1)$. Using considerations similar to the ones employed in [3], we also found all solutions of the equation

$$\phi\big(x^m - y^m\big) = x^n + y^n \tag{14}$$

where $x,\ y,\ m,\ n$ are positive integers (see [4]).

As related results, we mention that all solutions of the equation

$$\phi(F_m) = 2^n$$

or

$$\phi(L_m) = 2^n$$

were found in [5]. In fact, in [5], we also found all members of either the Fibonacci or the Lucas sequence for which the divisor sum is a power of 2. Finally, in [6], we found all solutions of the equation

$$\phi\left(\binom{m}{k}\right) = 2^n \tag{15}$$

where $m \ge 2k$. Equation (15) has no solutions for $k \ge 4$.

2. Preliminary results

The proof of the Theorem uses estimations of linear forms in logarithms of algebraic numbers.

For any non-zero algebraic number ζ let $H(\zeta)$ be the height of ζ. Let $\zeta_1, \ldots, \zeta_l$ be algebraic numbers, not 0 or 1, of heights not exceeding $A_1, \ldots, A_l$, respectively. We assume $A_m \geq e$ for $m = 1, \ldots, l$. Put $\Omega = \log A_1 \ldots \log A_l$. Let $\mathbb{F} = \mathbb{Q}(\zeta_1, \ldots, \zeta_l)$ and let $d_{\mathbb{F}} = [\mathbb{F} : \mathbb{Q}]$. Let $n_1, \ldots, n_l$ be integers, not all 0, and let $B \geq \max |n_m|$. We assume $B \geq e$. The following result is due to Baker and Wüstholz.

Theorem BW ([1])

If $\zeta_1^{n_1} \ldots \zeta_l^{n_l} \neq 1$, *then*

$$\left|\zeta_1^{n_1} \ldots \zeta_l^{n_l} - 1\right| > \exp\bigl(-(17(l+1)d_{\mathbb{F}})^{2l+7}\Omega \log B\bigr). \tag{16}$$

In fact, Baker and Wüstholz showed that if $\log \zeta_1, \ldots, \log \zeta_l$ are any fixed values of the logarithms and $\Lambda = n_1 \log \zeta_1 + \ldots + n_l \log \zeta_l \neq 0$, then

$$\log |\Lambda| > -\bigl(16 l d_{\mathbb{F}}\bigr)^{2(l+2)}\Omega \log B. \tag{17}$$

Now (16) follows easily from (17) via an argument similar to the one used by Shorey *et al.* in their paper ([7], p. 66).

We also need the following p-adic analogue of Theorem BW which is due to Yu (see Theorem 4 in [9]).

Theorem Y ([9])†

Let π be a prime ideal of $\mathbb{F}$ lying above a prime integer p. Assume that $\mathrm{ord}_\pi \zeta_i = 0$ *for $i = 1, \ldots, l$. If $\zeta_1^{n_1} \ldots \zeta_l^{n_l} \neq 1$, then there exist computable absolute constants C_1 and C_2 such that*

$$\mathrm{ord}_\pi\bigl(\zeta_1^{n_1} \ldots \zeta_l^{n_l} - 1\bigr) < \bigl(C_1 l d_{\mathbb{F}}\bigr)^{C_2 l}\,\frac{p^{d_{\mathbb{F}}}}{\log^2 p}\,\Omega \log\bigl(d_{\mathbb{F}}^2 B\bigr). \tag{18}$$

Let now $(u_n)_{n \geq 0}$ be a nondegenerate binary recurrence sequence given by formula (1). Assume that $|\alpha| > |\beta|$. Then

Theorem S ([8])

There exist computable numbers C_1, C_2 and C_3 depending only on a and b such that

$$|\alpha|^{n+C_1} > |u_n| > |\alpha|^{n - C_2 \log n} \qquad \text{for all } n \geq C_3. \tag{19}$$

---

† Here we use Theorem 4 on page 275 in [9]. However, in [9] the bound is quadratic in $\log(d_{\mathbb{F}}^2 B)$. Kunrui Yu has informed us that the dependence of the bound is, in fact, linear in $\log(d_{\mathbb{F}}^2 B)$, and that the apparent quadratic dependence of the bound in [9] on this term is just a misprint.

Let now $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ be two nondegenerate binary recurrence sequences given by recurrences (4) and (5) respectively.

The following Technical Lemma is essential in the proof of the theorem.

Technical Lemma

Let $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ be the two nondegenerate binary recurrence sequences given by formulae (4) and (5). Let $\gamma_1 \geq 1$, $\gamma_2 > 0$, $\gamma_3 > 0$ and $\gamma_4 \geq 0$ be fixed constants. Let A be a positive rational number and let m and n be positive integers satisfying the following four conditions:

$$\gamma_1 < \frac{|u_m|}{|v_n|} < \gamma_2, \tag{20}$$

$$\log H(A) < \gamma_3(\log m)^{\gamma_4}, \tag{21}$$

$$|Au_m| > |v_n| \tag{22}$$

and

$$A|a_1||\alpha_1|^m \neq |a_2||\alpha_2|^n. \tag{23}$$

Then, there exists a computable constant C depending only on the numbers γ_i for $i = 1, \ldots, 4$ and on the sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ such that, if $m > C$, then

$$\frac{|Au_m| - |v_n|}{|v_n|} > \exp(-(\log m)^{\gamma_4+2}). \tag{24}$$

Proof of the Technical Lemma

By C_1, C_2, ... we denote positive computable constants depending only on the constants γ_i for $i = 1$, ..., 4 and on the sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$. By Theorem S and inequalities (20), it follows that there exist computable numbers C_1, C_2, C_3, C_4 and C_5 such that, if $n > C_1$, then

$$\log \gamma_1 < \log |u_m| - \log |v_n| < (m + C_2)\log|\alpha_1| - (n - C_3 \log n)\log|\alpha_2| \tag{25}$$

and

$$(m - C_4 \log m)\log|\alpha_1| - (n + C_5)\log|\alpha_2| < \log|u_m| - \log|v_n| < \log \gamma_2. \tag{26}$$

In particular, there exist constants C_6, C_7, C_8, C_9, C_{10}, C_{11} and C_{12} such that, if $\min(n,\ m) > C_6$, then

$$-C_7 - C_8 \log m < m \log|\alpha_1| - n \log|\alpha_2| < C_9 + C_{10} \log m \tag{27}$$

and

$$C_{11}m < n < C_{12}m. \tag{28}$$

For $m > C_6$ we may write

$$|u_m| = |a_1||\alpha_1|^m + \epsilon_1|b_1||\beta_1|^m$$

and

$$|v_n| = |a_2||\alpha_2|^n + \epsilon_2|b_2||\beta_2|^n$$

where $\epsilon_1,\ \epsilon_2 \in \{-1,\ 1\}$. Therefore

$$|Au_m| - |v_n| = \big(A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n\big) + \big(A\epsilon_1|b_1||\beta_1|^m - \epsilon_2|b_2||\beta_2|^n\big) > 0. \tag{29}$$

We now analyse the expression

$$|A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n| = A|a_1||\alpha_1|^m\Big|1 - \Big(\frac{|a_2|}{A|a_1|}\Big)|\alpha_1|^{-m}|\alpha_2|^n\Big| \tag{30}$$

which is non-zero by (23). Let $C_{13} \geq C_6$ be such that if $m > C_{13}$, then

$$\gamma_3(\log m)^{\gamma_4} > \log\left(H\Big(\frac{|a_2|}{|a_1|}\Big)\right).$$

In this case,

$$\max\left(H(A),\ H\Big(\frac{|a_2|}{|a_1|}\Big)\right) < \gamma_3(\log m)^{\gamma_4}.$$

Since $|a_2|/|a_1|$ is algebraic of degree at most 4 and A is rational, it follows that

$$\log H\Big(\frac{|a_2|}{A|a_1|}\Big) \leq 5\cdot\max\left(\log H(A),\ \log\Big(H\Big(\frac{a_2}{|a_1|}\Big)\Big)\right) < 5\gamma_3(\log m)^{\gamma_4} \tag{31}$$

for $m > C_{13}$. Let C_{14} be an upper bound for $\log H(|\alpha_1|)\cdot\log H(|\alpha_2|)$. Let $\Omega = 5\gamma_3 C_{14}(\log m)^{\gamma_4}$. Finally, let $B = \max(m,\ n)$. From now on, assume that $m > C_{15} = \max(C_{12},\ C_{13})$. It follows, by inequality (28), that $n < m^2$. Hence, $\log B < 2\log m$. From formula (30) and Theorem BW, it follows that

$$|A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n| > A|a_1||\alpha_1|^m\cdot\exp\big(-272^{13}\cdot 6\gamma_3\cdot C_{14}(\log m)^{\gamma_4+1}\big). \tag{32}$$

Moreover, since A is rational, it follows that

$$A > \frac{1}{H(A)} > \exp\big(-\gamma_3(\log m)^{\gamma_4}\big) > \exp\big(-\gamma_3(\log m)^{\gamma_4+1}\big). \tag{33}$$

From inequalities (32) and (33), it follows that

$$|A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n| > |a_1||\alpha_1|^m\exp\big(-\gamma_3\cdot(272^{13}\cdot 6\cdot C_{14}+1)\cdot(\log m)^{\gamma_4+1}\big)$$

or

$$|A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n| > |a_1||\alpha_1|^m \exp\bigl(-C_{16}(\log m)^{\gamma_4+1}\bigr) \qquad \text{for } m > C_{15} \tag{34}$$

where $C_{16} = \gamma_3 \cdot (272^{13} \cdot 6 \cdot C_{14} + 1)$. One can show, by using a similar argument, that

$$|A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n| > |a_2||\alpha_2|^n \exp\bigl(-C_{17}(\log m)^{\gamma_4+1}\bigr) \qquad \text{for } m > C_{18}. \tag{35}$$

Now let $C_{19} = \max(C_{18},\ C_{15})$ and let $C_{20} = \max(C_{16},\ C_{17})$. From equations (34) and (35), it follows that

$$|A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n| > \max(|a_1||\alpha_1|^m,\ |a_2||\alpha_2|^n) \cdot \exp\bigl(-C_{20}(\log m)^{\gamma_4+1}\bigr) \tag{36}$$

for $m > C_{19}$. We now show that if

$$A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n < 0, \tag{37}$$

then m is bounded. Indeed, assume that inequality (37) happens. From inequality (29), it follows that

$$|A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n| = -(A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n) < A|b_1||\beta_1|^m + |b_2||\beta_2|^n. \tag{38}$$

Assume, for example, that $A|b_1||\beta_1|^m \geq |b_2||\beta_2|^n$. In this case, from inequalities (36) and (38), it follows that

$$|a_1||\alpha_1|^m \exp\bigl(-C_{20}(\log m)^{\gamma_4+1}\bigr) < 2A|b_1||\beta_1|^m$$

or

$$\left|\frac{\alpha_1}{\beta_1}\right|^m < 2A|b_1||a_1|^{-1} \exp\bigl(C_{20}(\log(m)^{\gamma_4+1}\bigr)$$

or

$$m \log\left|\frac{\alpha_1}{\beta_1}\right| < \log A + C_{21} + C_{20}(\log m)^{\gamma_4+1} \tag{39}$$

for $m > C_{19}$ where $C_{21} = \max(0,\ \log(2|b_1||a_1|^{-1}))$. Since A is rational, it follows that $A \leq H(A)$. Therefore

$$\log A \leq \log H(A) < \gamma_3(\log m)^{\gamma_4}. \tag{40}$$

Inequality (39) implies that

$$m \log\left|\frac{\alpha_1}{\beta_1}\right| < C_{21} + \gamma_3(\log m)^{\gamma_4} + C_{20}(\log m)^{\gamma_4+1}. \tag{41}$$

Inequality (41) implies that $m < C_{22}$. The case $A|b_1||\beta_1|^m < |b_2||\beta_2|^n$ can be treated similarly.

In conclusion, there exists a constant C_{23} such that, if $m > C_{23}$, then

$$A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n > 0. \tag{42}$$

We now show that

$$|Au_m| - |v_n| > \frac{1}{2}|a_2|\alpha_2|^n \exp\bigl(-C_{20}(\log m)^{\gamma_4+1}\bigr) \tag{43}$$

for m enough large. Indeed, by formula (29) and inequalities (36) and (42) for $m > C_{23}$, it follows that

$$\begin{aligned}|Au_m| - |v_n| &= |A|a_1||\alpha_1|^m - |a_2||\alpha_2|^n| + \bigl(A\epsilon_1|b_1||\beta_1|^m - \epsilon_2|b_2||\beta_2|^n\bigr)\\ &> \ |a_2||\alpha_2|^n \cdot \exp\bigl(-C_{20}(\log m)^{\gamma_4+1}\bigr) + \bigl(A\epsilon_1|b_1||\beta_1|^m - \epsilon_2|b_2||\beta_2|^n\bigr).\end{aligned}$$

Hence, in order to prove that inequality (43) holds when m is large enough, it suffices to show that the inequality

$$\frac{1}{2}|a_2||\alpha_2|^n \cdot \exp\bigl(-C_{20}(\log m)^{\gamma_4+1}\bigr) > |A\epsilon_1|b_1||\beta_1|^m - \epsilon_2|b_2||\beta_2|^n| \tag{44}$$

holds when m is large enough.

Assume, for example, that $A|b_1||\beta_1|^m \leq |b_2||\beta_2|^n$. Then, it suffices to show that

$$\frac{1}{2}|a_2||\alpha_2|^n \cdot \exp\bigl(-C_{20}(\log m)^{\gamma_4+1}\bigr) > 2|b_2||\beta_2|^n$$

or

$$\Bigl|\frac{\alpha_2}{\beta_2}\Bigr|^n > 4|b_2||a_2|^{-1} \exp\bigl(C_{20}(\log m)^{\gamma_4+1}\bigr)$$

or that

$$n \log \Bigl|\frac{\alpha_2}{\beta_2}\Bigr| > C_{24} + C_{20}(\log m)^{\gamma_4+1} \tag{45}$$

for m large enough where $C_{24} = \max(0,\ \log(4|b_2||a_2|^{-1}))$. Using inequality (27), one concludes easily that inequality (45) is satisfied for $m > C_{25}$. It follows that inequality (43) is also satisfied for $m > C_{25}$ in this case.

The case $A|b_1||\beta_1|^m > |b_2||\beta_2|^n$ can be treated using a similar argument.

Assume therefore that inequality (43) holds when $m > C_{25}$.

From inequality (43) and Theorem S, it follows that

$$\begin{aligned}\frac{|Au_m| - |v_n|}{|v_n|} &> \frac{1}{2}|a_2||\alpha_2|^{-C_3 \log n} \exp\bigl(-C_{20}(\log m)^{\gamma_4+1}\bigr)\\ &= \ \exp\Bigl(C_{26} - C_3 \log|\alpha_2| \log n - C_{20}(\log m)^{\gamma_4+1}\Bigr)\end{aligned}$$

for $m > C_{25}$ where $C_{26} = \max(0,\ \log(|a_2|/2))$. Hence, in order to prove that inequality (24) holds when m is large enough, it suffices to show that

$$\exp\Bigl(C_{26} - C_3 \log|\alpha_2| \log n - C_{20}(\log m)^{\gamma_4+1}\Bigr) > \exp(-(\log m)^{\gamma_4+2}) \tag{46}$$

holds when m is large enough. Notice that inequality (46) is equivalent to

$$(\log m)^{\gamma_4+2} > C_{20}(\log m)^{\gamma_4+1} + C_3 \log|\alpha_2| \log n - C_{26}$$

which, by inequality (27), is certainly true for $m > C_{27}$.

The technical lemma is therefore proved. □

For any non-zero integer k and any prime number p, let $\mathrm{ord}_p(k)$ be the power at which p appears in the prime factor decomposition of k.

Lemma 1

Let $(u_n)_{n\geq 0}$ be a nondegenerate binary recurrence sequence. Then, there exist three computable constants C_1, C_2 and C_3 depending only on the sequence $(u_n)_{n\geq 0}$ such that, if p is a prime number and $u_m \neq 0$, then

$$\mathrm{ord}_p(u_m) < \min\Big(C_1 m + C_2,\ C_3 \frac{p^2}{\log p} \log(4m)\Big). \tag{47}$$

Proof of Lemma 1

Assume that u_n is given by formula (1) for all $n \geq 0$. Let $|\alpha| > |\beta|$. Denote $\mu = \mathrm{ord}_p(u_m)$. By Theorem S it follows that

$$2^\mu \leq p^\mu \leq |u_m| < |\alpha|^{m+C_1}$$

where C_1 depends only on a and b. Hence,

$$\mu < (m + C_1)\log_2|\alpha| = m \cdot C_2 + C_3$$

where $C_2 = \log_2|\alpha|$ and $C_3 = C_1 \log_2|\alpha|$.

The fact that

$$\mathrm{ord}_p(u_m) < C_3 \frac{p^2}{\log p} \log(4m)$$

for some computable constant C_3 follows immediately from Theorem Y. □

Lemma 2

Let n be a positive integer and let t be a real number such that $\mathrm{ord}_2(\phi(n)) \leq t$. Then

$$\frac{\phi(n)}{n} \geq \frac{1}{t+2}. \tag{48}$$

Proof of Lemma 2

See, for example, [3]. □

Lemma 3

Let $(v_n)_{n\geq 0}$ be a nondegenerate binary recurrence sequence satisfying either one of the following two conditions:

(1) $(v_n)_{n\geq 0}$ *is a Lucas sequence of the second kind.*
(2) $(v_n)_{n\geq 0}$ *is such that* $(r,\ s)$ *is odd and* s *is even.*

In this case, there exist two computable constants C_1 *and* C_2 *such that*

$$\operatorname{ord}_2(v_n) < C_1 \qquad \text{for all } n > C_2. \tag{49}$$

Proof of Lemma 3

Throughout this proof, we assume that $(v_n)_{n\geq 0}$ is given by the recurrence relation

$$v_{n+2} = rv_{n+1} + sv_n \qquad \text{for } n = 0,\ 1,\ ...$$

Assume first that $(v_n)_{n\geq 0}$ is a Lucas sequence of the second kind and that s is odd. We distinguish 2 cases.

Case 1. r is even. We first show that u_n is even for all $n \geq 0$. Indeed this follows easily by induction using the recurrence formula and the fact that both $v_0 = 2$ and $v_1 = r$ are even. We now show that

$$\operatorname{ord}_2(v_n) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod 2, \\ \operatorname{ord}_2(r) & \text{if } n \equiv 1 \pmod 2. \end{cases}$$

Assume, for example, that $2 \mid n$. Then,

$$v_n = \alpha^n + \beta^n = (\alpha^{n/2} + \beta^{n/2})^2 - 2\alpha^{n/2}\beta^{n/2} = v_{n/2}^2 \pm 2s^{n/2} \equiv 2 \pmod 4$$

because s is odd and $u_{n/2}$ is even. Hence, $\operatorname{ord}_2(v_n) = 1$ if n is even. Now write $r = 2^\mu r'$ where $\mu \geq 1$ and $r' \equiv 1 \pmod 2$. We prove, by induction, that $\operatorname{ord}(v_{2k+1}) = \mu$ for all $k \geq 0$. This is certainly true for $k = 0$. Assume that this is true for k. From the recurrence relation, we conclude that

$$v_{2(k+1)+1} = rv_{2(k+1)} + sv_{2k+1} = 2^{\mu+1}r'\frac{v_{2(k+1)}}{2} + 2^\mu s\frac{v_{2k+1}}{2^{mu}}. \tag{50}$$

By the previous arguments and the induction hypothesis both numbers

$$r'\frac{v_{2(k+1)}}{2} \quad \text{and} \quad s\frac{v_{2k+1}}{2^{mu}}$$

are odd integers. From formula (50) it follows that $\operatorname{ord}_2(v_{2(k+1)+1}) = \mu$. The induction is therefore complete.

Case 2. r is odd. Reducing the recurrence formula of $(v_n)_{n\geq 0}$ modulo 2, it follows that

$$v_{n+2} \equiv v_{n+1} + v_n \pmod 2.$$

Since $v_0 = 2 \equiv 0 \pmod 2$ and $v_1 = r \equiv 1 \pmod 2$, it follows that $v_n \equiv F_n \pmod 2$ where F_n is the n'th term of the Fibonacci sequence. It is well known that $2 \mid F_n$ if and only if $3 \mid n$. Hence, $\operatorname{ord}_2(v_n) = 0$ if $3 \not\mid n$. Assume now that $n = 3k$. Let

$w_k = (\alpha^3)^k + (\beta^3)^k$. Notice that $(w_n)_{n\geq 0}$ is a Lucas sequence of the second kind satisfying the recurrence

$$w_{n+2} = (r^3 + 3rs)w_{n+1} + s^3 w_n \qquad \text{for all } n > 0.$$

Since $r^3 + 3rs \equiv 0 \pmod 2$, it follows, by Case 1, that

$$\mathrm{ord}_2(v_{3k}) = \begin{cases} 1 & \text{if } k \equiv 0 \pmod 2, \\ \mathrm{ord}_2(r^2 + 3s) & \text{if } k \equiv 1 \pmod 2. \end{cases}$$

Assume now that $(v_n)_{n\geq 0}$ is such that $(r,\ s)$ is odd and s is even. Let $\mathbb{F} = \mathbb{Q}(\alpha)$ and let π be a prime ideal of $\mathbb{F}$ lying above the prime number 2. Since π divides s but π does not divide r, it follows that π divides exactly one of the ideals $[\alpha]$ and $[\beta]$. Assume that $\pi \mid [\alpha]$. Let γ be an upper bound for $\mathrm{ord}_\pi(b)$. Finally, let $C_1 > \gamma$ be such that $v_n \neq 0$ for $n > C_1$ (the existence of such a constant is guaranteed by Theorem S). If $n > C_1$, then

$$\mathrm{ord}_\pi(v_n) = \mathrm{ord}_\pi(a\alpha^n + b\beta^n) = \mathrm{ord}_\pi(b\beta^n) = \mathrm{ord}_\pi(b) < \gamma.$$

Hence, $\mathrm{ord}_2(v_n) \leq 2\mathrm{ord}_\pi(v_n) < 2\gamma$ for $n > C_1$. The lemma is, therefore, completely proved. $\square$

Lemma 4

Let $0 < x_i < 1$ *for* $i = 1,\ ...,\ s$ *be real numbers. Then,*

$$1 - (1 - x_1)(1 - x_2)...(1 - x_s) \leq x_1 + x_2 + ... + x_s. \tag{51}$$

Proof of Lemma 4

We proceed by induction on s. If $s = 1$, then inequality (51) becomes equality. Assume that inequality (51) holds for some $s \geq 1$. Then,

$$\begin{aligned} 1 - (1 - x_1)...(1 - x_s)(1 - x_{s+1}) &= \big(1 - (1 - x_1)...(1 - x_s)\big) + x_{s+1}(1 - x_1)\dots(1 - x_s) \\ &< x_1 + ... + x_s + x_{s+1}. \ \square \end{aligned}$$

3. The proofs

We are now ready to prove the theorem.

Proof of the Theorem

By $C_1,\ C_2,...$ we denote computable positive constants depending only on a, b and the sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$. Let $(m,\ n)$ be a pair of positive integers satisfying equation (6). We may replace the sequence $(u_n)_{n\geq 0}$ by $(au_n)_{n\geq 0}$ and the sequence $(v_n)_{n\geq 0}$ by $(bv_n)_{n\geq 0}$. From Theorem S, it follows that $|u_m| > 1$ for $m > C_1$. From Lemma 3, it follows that there exist two constants C_2 and C_3 such that

$$\operatorname{ord}_2(v_n) < C_2 \qquad \text{for } n > C_3. \tag{52}$$

We may assume that C_2 is an integer. Let $C_4 > C_1$ be such that if $m > C_4$, then $n > C_3$. Assume that $m > C_4$. Write

$$|u_m| = p_1^{\mu_1} p_2^{\mu_2} ... p_t^{\mu_t} \tag{53}$$

where $p_1 < p_2 < \ldots < p_t$ are prime numbers. Since at least $t-1$ of the above primes are odd, it follows that

$$t - 1 \leq \operatorname{ord}_2\big(\phi(|u_m|)\big) = \operatorname{ord}_2\big(|v_n|\big) < C_2.$$

Hence,

$$t \leq C_2. \tag{54}$$

From Lemma 2, it follows that

$$1 > \frac{\phi(|u_m|)}{|u_m|} \geq \frac{1}{C_2 + 2}.$$

Hence,

$$1 < \frac{|u_m|}{|v_n|} \leq C_2 + 2 < C_2 + 3 = C_5 \qquad \text{for } m > C_4. \tag{55}$$

We now find upper bounds for the primes p_i for $i = 1, \ ..., \ t$. We use induction to prove that there exists a constant C_6 such that, if $m > C_6$, then

$$p_i < 2(\log m)^{2i}. \tag{56}$$

Let $i = 1$. Write

$$\frac{|v_n|}{|u_m|} = \frac{\phi(|u_m|)}{|u_m|} = \prod_{i=1}^{t} \frac{(p_i - 1)}{p_i}. \tag{57}$$

Hence,

$$1 - \prod_{i=1}^{t}\Big(1 - \frac{1}{p_i}\Big) = 1 - \frac{|v_n|}{|u_m|} = \frac{|u_m| - |v_n|}{|v_n|}. \tag{58}$$

From Lemma 4, it follows that

$$\frac{C_2}{p_1} \geq \frac{t}{p_1} \geq \frac{1}{p_1} + ... + \frac{1}{p_t} \geq 1 - \prod_{i=1}^{t}\Big(1 - \frac{1}{p_i}\Big) = \frac{|u_m| - |v_n|}{|u_m|}. \tag{59}$$

We first assume that:

$$|a_1||\alpha_1|^m \neq |a_2||\alpha_2|^n. \tag{60}$$

We shall return later on and prove that inequality (60) holds when m is large enough. From inequalities (60) and (55), it follows that the hypothesis of the Technical Lemma are satisfied for $\gamma_1 = 1$, $\gamma_2 = C_5$, $A = 1$, $\gamma_3 = 1$ and $\gamma_4 = 0$. By the Technical Lemma and inequality (59), it follows that

$$\frac{C_2}{p_1} \geq \frac{|u_m| - |v_n|}{|u_m|} > \exp\bigl(-(\log m)^2\bigr) \qquad \text{for } m > C_4.$$

Hence,

$$\log p_1 < (\log m)^2 + \log C_2 < 2(\log m)^2 \qquad \text{for } m > C_6. \tag{61}$$

Assume now that there exists i with $1 \leq i < t$ and a computable constant C_7 such that

$$\log p_j < 2(\log m)^{2j} \qquad \text{for } j = 1,\ ...,\ i \text{ and } m > C_7. \tag{62}$$

Let

$$A_i = \prod_{j=1}^{i} \frac{(p_j - 1)}{p_j}. \tag{63}$$

Formula (57) may be rewritten as

$$\frac{|v_n|}{|u_m|} = A_i \prod_{j=i+1}^{t} \frac{(p_j - 1)}{p_j}$$

or

$$1 - \prod_{j=i+1}^{t} \Bigl(1 - \frac{1}{p_j}\Bigr) = 1 - \frac{|v_n|}{A_i|u_m|} = \frac{A_i|u_m| - |v_n|}{A_i|u_m|}. \tag{64}$$

From Lemma 4, it follows that

$$\begin{aligned} \frac{C_2}{p_{i+1}} > \frac{t-i}{p_{i+1}} \geq \frac{1}{p_{i+1}} + \ldots + \frac{1}{p_t} > 1 - \prod_{j=i+1}^{t} \Bigl(1 - \frac{1}{p_j}\Bigr) \\ = \frac{A_i|u_m| - |v_n|}{A_i|u_m|}. \end{aligned} \tag{65}$$

Assume, for the time being, that

$$A_i|a_1||\alpha_1|^m \neq |a_2||\alpha_2|^n. \tag{66}$$

We shall return later on and prove that inequality (66) holds when m is large enough. We apply the Technical Lemma with $\gamma_1 = 1$, $\gamma_2 = C_5$ and $A = A_i$. From the induction hypothesis and the formula of A_i, it follows that

$$\log H(A_i) = \log \prod_{j=1}^{i} p_j = \sum_{j=1}^{i} p_j < \sum_{j=1}^{i} 2(\log m)^{2j} = 2(\log m)^2 \cdot \frac{(\log m)^{2i} - 1}{(\log m)^2 - 1}$$
$$= \frac{2(\log m)^2}{(\log m)^2 - 1} \cdot \Big((\log m)^{2i} - 1\Big) < 3(\log m)^{2i} \qquad \text{for } m > C_8.$$

Thus, we may take $\gamma_3 = 3$ and $\gamma_4 = 2i$. Since

$$\frac{1}{A_i} = \prod_{j=1}^{i} \frac{p_j}{p_j - 1} > 1,$$

it follows, by inequality (65) and the Technical Lemma, that

$$\frac{C_2}{p_{i+1}} > \frac{A_i|u_m| - |v_n|}{A_i|u_m|} > \exp\big(-(\log m)^{2i+2}\big)$$

or

$$\log p_{i+1} < (\log m)^{2(i+1)} + \log C_2 < 2(\log m)^{2(i+1)} \qquad \text{for } m > C_9.$$

The induction is, therefore, complete.

We now use Theorem BW to show that m is bounded. Rewrite equation (53) as

$$a_1\alpha_1^m + b_1\beta_1^m = p_1^{\mu_1} ... p_t^{\mu_t}$$

or

$$\left|\frac{b_1}{a_1}\right|\left|\frac{\beta_1}{\alpha_1}\right|^m = \left|1 - \frac{1}{a_1}\alpha_1^{-m}p_1^{\mu_1}...p_t^{\mu_t}\right|. \tag{67}$$

Let C_9 be such that inequalities (56) hold for $i = 1, \ ..., \ t$ and $m > C_9$. Let C_{10} be an upper bound for both $H(a_1)$ and $H(\alpha_1)$. Let

$$\Omega = H(a_1)H(\alpha_1)\prod_{i=1}^{t} \log p_i.$$

From inequalities (56), it follows that

$$\Omega < C_{10}^2 \prod_{i=1}^{t} 2(\log m)^{2i} = 2^t C_{10}^2 (\log m)^{t(t-1)} < C_{11}(\log m)^{C_{12}} \tag{68}$$

where $C_{11} = 2^{C_2}C_{10}^2$ and $C_{12} = C_2(C_2 - 1)$. Let B be an upper bound for m and μ_i for $i = 1, \ ..., \ t$. From Lemma 1, it follows that $B < C_{13}m + C_{14}$. From equation (67), Theorem BW and inequality (68), it follows that

$$\log\left|\frac{b_1}{a_1}\right| + m\log\left|\frac{\beta_1}{\alpha_1}\right| > -\big(17(t+3)\big)^{2(t+2)+7}\Omega\log B$$

or

$$m \log \left| \frac{\alpha_1}{\beta_1} \right| + \log \left| \frac{a_1}{b_1} \right| < C_{15} \cdot C_{11} (\log m)^{C_{12}} \log(C_{13} m + C_{14}) \tag{69}$$

where $C_{15} = (17(C_2+3))^{2(C_2+2)+7}$. Inequality (69) shows that m is bounded.

Hence, the theorem is proved once we show that both inequalities (60) and (66) hold when m is large enough. Denote $A_0 = 1$. Assume that

$$A_i |a_1| |\alpha_1|^m = |a_2| |\alpha_2|^n \qquad \text{for some } i = 0,\ \ldots,\ t-1. \tag{70}$$

We first show that if equation (70) holds, then the rational numbers A_i can take only finitely many values. Let $\mathbb{F} = \mathbb{Q}(\alpha_1,\ \alpha_2)$ and let $d_{\mathbb{F}} = [\mathbb{F} : \mathbb{Q}]$. Clearly, $d_{\mathbb{F}} \leq 2$. Let Δ be a common denominator of a_1 and a_2; that is, a positive integer such that both Δa_1 and Δa_2 are algebraic integers. Let $a_1' = \Delta a_1$ and $a_2' = \Delta a_2$. Rewrite equality (70) as

$$A_i |a_1'| |\alpha_1|^m = |a_2'| |\alpha_2|^n. \tag{71}$$

Taking norms in (71) we get

$$A_i^{d_{\mathbb{F}}} N_{\mathbb{F}}(|a_1'|) N_{\mathbb{F}}(|\alpha_1|)^m = N_{\mathbb{F}}(|a_2'|) N_{\mathbb{F}}(|\alpha_2|)^n. \tag{72}$$

Using formula (63), one concludes easily that equation (72) forces

$$p_i \mid N_{\mathbb{F}}(|a_1'|) N_{\mathbb{F}}(|\alpha_1|).$$

Hence, $p_i < C_{16}$. From formula (63) and the fact that $p_1 < \ldots < p_i < C_{16}$, it follows that A_i can take only finitely many rational values. For simplicity, denote $A = A_i$.

In order to show that m is bounded, we use the fact that the pair of sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ satisfies one of the assumptions A1-A3.

Case 1. *The pair of sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq)}$ satisfies A1.*

Assume that $\alpha_1 \notin \mathbb{Z}$. If $|a_1||\alpha_1|^m \in \mathbb{Q}$, it follows that $|a_1||\alpha_1|^m$ is invariant under the action of the Galois group $G = \mathrm{Gal}(\mathbb{F}/\mathbb{Q})$. Hence,

$$|a_1||\alpha_1|^m = |b_1||\beta_1|^m$$

or

$$\left| \frac{\alpha_1}{\beta_1} \right|^m = \left| \frac{b_1}{a_1} \right|. \tag{73}$$

Equation (73) has a unique solution m. In particular, m is bounded.

Assume now that $|a_1||\alpha_1|^m \notin \mathbb{Q}$. From equation (70), we conclude that $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$. Moreover, by conjugating equation (70), we get

$$A |b_1| |\beta_1|^m = |b_2| |\beta_2|^n. \tag{74}$$

From formula (29), we get

$$|Au_m| - |v_n| = A|b_1||\beta_1|^m(\epsilon_1 - \epsilon_2). \tag{75}$$

If $\epsilon_1 = \epsilon_2$, we get $|Au_m| = |v_n|$ which contradicts the fact that $i < t$. Hence, $\epsilon_1 - \epsilon_2 = 2$ and formula (75) becomes

$$|Au_m| - |v_n| = 2A|b_1||\beta_1|^m. \tag{76}$$

Equation (26) shows that $|b_1||\beta_1|^m \in \mathbb{Q}$. In particular, $|a_1||\alpha_1|^m \in \mathbb{Q}$ which is a case already treated.

Case 2. *The pair of sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ satisfies A2.*

Assume that both α_1 and α_2 are integers. Rewrite equation (70) as

$$|\alpha_1|^m|\alpha_2|^{-n} = |a_2||a_1|^{-1}A^{-1}. \tag{77}$$

Since $a_1,\ a_2 \in \mathbb{Q}$ and A can take only finitely many rational values, it follows that the right-hand side of equation (77) can take only finitely many rational values. Let C_{17} be such that

$$\Big|\mathrm{ord}_p\big(|a_2||a_1|^{-1}A^{-1}\big)\Big| < C_{17} \tag{78}$$

for all the prime numbers p. Write

$$|\alpha_1| = q_1^{\lambda_1}\dots q_l^{\lambda_l}$$

and

$$|\alpha_2| = q_1^{\nu_1}\dots q_l^{\nu_l}$$

where $q_1 < \ldots < q_l$ are primes and $\lambda_i \geq 0,\ \nu_i \geq 0$ for $i = 1,\ \ldots,\ l$. Equation (77) and inequality (78) imply

$$|\lambda_i m - \nu_i n| < C_{17} \tag{79}$$

for $i = 1,\ \ldots,\ l$. Since $\log|\alpha_1|$ and $\log|\alpha_2|$ are linearly independent over $\mathbb{Q}$, it follows that the set

$$\big\{(x,\ y)\mid |\lambda_i x - \nu_i y| < C_{17} \text{ for } i = 1,\ \ldots,\ l\big\}$$

is a bounded set in the xy-plane. This shows that m is bounded.

Case 3. *The pair of sequences $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ satisfies A3.*

From formula (29), we get

$$A|u_m| - |u_n| = A\epsilon_1|b_1||\beta_1|^m - \epsilon_2|b_2||\beta_2|^n. \tag{80}$$

Let

$$w_m = \prod_{j=i+1}^{t} p_j^{\mu_j}.$$

We first show that w_m is a prime when m is large enough. Indeed notice that

$$\begin{aligned} A|u_m| - |v_n| &= \prod_{j=1}^{i}\Big(\frac{p_j-1}{p_j}\Big)\cdot\prod_{j=1}^{t} p_j^{\mu_j} - \phi(|u_m|) \\ &= \prod_{j=1}^{i} p_j^{\mu_j-1}(p_j-1)\big(w_m-\phi(w_m)\big) \\ &= A\epsilon_1|b_1||\beta_1|^m - \epsilon_2|b_2||\beta_2|^n. \end{aligned} \tag{81}$$

Assume now that w_m is not a prime. It is clear that if k is any positive integer which is not a prime, then

$$k-\phi(k) > \frac{k}{d}$$

for any proper divisor d of k. Indeed, this follows, for example, by noticing that the k/d integers

$$d,\ 2d,\ \ldots,\ \frac{k}{d}\cdot d$$

are less than or equal to k and are not coprime to k. In particular,

$$w_m - \phi(w_m) > \frac{w_m}{p_{i+1}}.$$

Hence,

$$\begin{aligned} A\epsilon_1|b_1||\beta_1|^m - \epsilon_2|b_2||\beta_2|^n &= \prod_{j=1}^{i} p_j^{\mu_j-1}(p_j-1)(w_m-\phi(w_m)) \\ &\geq \prod_{j=1}^{i} p_j^{\mu_j-1}(p_j-1)\frac{w_m}{p_{i+1}} = \frac{A|u_m|}{p_{i+1}}. \end{aligned} \tag{82}$$

Assume, for example, that $A|b_1||\beta_1|^m \geq |b_2||\beta_2|^n$. From inequality (82), it follows that

$$2A|b_1||\beta_1|^m \geq A\epsilon_1|b_1||\beta_1|^m - \epsilon_2|b_2||\beta_2|^n \geq \frac{A|u_m|}{p_{i+1}}. \tag{83}$$

Hence,

$$p_{i+1} \geq \frac{|u_m|}{|b_1||\beta_1|^m}. \tag{84}$$

From Theorem S, it follows that there exist three constants C_{18}, C_{19} and C_{20} such that

$$|\alpha_1|^{m+C_{18}} > |u_m| > |\alpha_1|^{m-C_{19}\log m} \qquad \text{for } m > C_{20}. \tag{85}$$

From inequalities (84) and (85), it follows that

$$p_{i+1} > \left|\frac{\alpha_1}{\beta_1}\right|^{m-C_{21}\log m - C_{22}} \qquad \text{for } m > C_{20}. \tag{86}$$

On the other hand, since w_m is not prime and p_{i+1} is the smallest prime divisor of w_m, it follows that $w_m \geq p_{i+1}^2$. Hence,

$$|\alpha_1|^{m+C_{18}} > |u_m| \geq |w_m| \geq p_{i+1}^2 > \left|\frac{\alpha_1}{\beta_1}\right|^{2m-2C_{21}\log m-2C_{22}} \qquad \text{for } m > C_{20}. \tag{87}$$

By taking logarithms in inequality (87), we conclude that

$$(m + C_{18})\log|\alpha_1| > (m - C_{21}\log m - C_{22})\log\left|\frac{\alpha_1^2}{\beta_1^2}\right|$$

or

$$m\log\left|\frac{\alpha_1}{\beta_1^2}\right| < C_{18}\log|\alpha_1| + (C_{21}\log m + C_{22})\log\left|\frac{\alpha_1^2}{\beta_1^2}\right|. \tag{88}$$

Since $|\alpha_1| > |\beta_1|^2$, it follows that inequality (88) holds only for finitely many values of m.

The case $A|b_1||\beta_1|^m < |b_2||\beta_2|^n$ can be treated using similar arguments together with inequality (27) and the fact that A can take only finitely many values.

Hence, if $m > C_{23}$, then $w_m = p_{i+1}$. In this case, equation (81) becomes

$$A\epsilon_1|b_1||\beta_1|^m - \epsilon_2|b_2||\beta_2|^n = \prod_{j=1}^{i} p_j^{\mu_j-1}(p_j-1)(w_m - \phi(w_m)) = \prod_{j=1}^{i} p_j^{\mu_j-1}(p_j-1). \tag{89}$$

Since max $(|\beta_1|,\ |\beta_2|) > 1$, we may assume that $|\beta_1| > 1$. Rewrite equation (89) as

$$A|b_1||\beta_1|^m\left|1 - \epsilon_2\epsilon_1|b_1|^{-1}A^{-1}|b_2||\beta_2|^n|\beta_1|^{-m}\right| = \prod_{j=1}^{i} p_j^{\mu_j-1}(p_j-1). \tag{90}$$

We know that $p_j \leq p_i < C_{16}$ for $j = 1,\ \ldots,\ i$. From Lemma 1, it follows that there exists C_{24} such that

$$\mu_j < C_{24}\log(4m) \qquad \text{for } j = 1,\ \ldots,\ i. \tag{91}$$

In particular,

$$\begin{aligned} A|b_1||\beta_1|^m\left|1 - \epsilon_2\epsilon_1|b_1|^{-1}|b_2||\beta_2|^n|\beta_1|^{-m}\right| &= \prod_{j=1}^{i} p_j^{\mu_j-1}(p_j-1) \\ &< C_{16}^{tC_{24}\log(4m)} = C_{16}^{C_{25}\log(4m)} \end{aligned} \tag{92}$$

where $C_{25} = C_2 \cdot C_{24} \geq tC_{24}$. On the other hand, let C_{26} be an upper bound for $\log(|b_1|^{-1}A^{-1}|b_2|) \cdot \log|\beta_1| \cdot \log|\beta_2|$ and let B be an upper bound for max $(m,\ n)$. From inequality (28), we know that $B < C_{27}m$. By Theorem BW, it follows that

$$\begin{aligned}\left|1 - \epsilon_2\epsilon_1|b_1|^{-1}|b_2||\beta_2|^n|\beta_1|^{-m}\right| &> \exp\bigl(-68^{13}C_{26}\log B\bigr)\\ &> \exp\bigl(-68^{13}C_{26}\log(C_{27}m)\bigr).\end{aligned} \tag{93}$$

By combining equation (90), inequalities (92) and (93), and by taking logarithms, we get

$$\log(A|b_1|) + m\log|\beta_1| - 68^{13}C_{26}\log(C_{27}m) < C_{25}\log C_{16} \cdot \log(4m). \tag{94}$$

Inequality (94) shows that m is bounded.

This finishes the proof of the Theorem. □

Proof of Proposition 1

Let $(u_n)_{n\geq 0}$ be the sequence

$$u_n = \frac{10^n - 1}{9}. \tag{95}$$

Assume that the equation

$$\phi(au_m) = bu_n \tag{96}$$

has a solution $(a,\ b,\ m,\ n)$ with $m > 1$ and $a,\ b \in \{1,\ \ldots,\ 9\}$.

We first show that $n = m - 1$. Indeed, on the one hand, one has

$$10^m - 1 \geq au_m > \phi(au_m) = bu_n \geq u_n = \frac{10^n - 1}{9}.$$

Hence, $m \geq n$. We now show that $m > n$. Let P be the largest prime dividing u_m. From a result of Carmichael (see [2]), it follows that $P > m$ if $m \geq 12$. In particular, $P > 10$ for $m \geq 12$. One can check that $P > 10$ for $2 \leq m \leq 12$ as well. In particular, $P \not| ab$. If $\mu = \mathrm{ord}_P(u_m)$, it follows that

$$\mu = \mathrm{ord}_P(bu_m) \tag{97}$$

and

$$\mu - 1 = \mathrm{ord}_P\bigl(\phi(au_m)\bigr). \tag{98}$$

Equations (97) and (98) show that the equation $\phi(au_m) = bu_m$ is impossible. Hence, $m > n$.

We now show that $m = n + 1$. Indeed, since

$$\mathrm{ord}_2\bigl(\phi(au_m)\bigr) = \mathrm{ord}_2(bu_n) = \mathrm{ord}_2(b) \leq 3, \tag{99}$$

it follows, by Lemma 2, that

$$\frac{9(10^n-1)}{10^m-1} \geq \frac{bu_n}{au_m} = \frac{\phi(au_m)}{au_m} \geq \frac{1}{5}$$

or

$$45 \cdot 10^n - 45 > 10^m - 1. \tag{100}$$

Inequality (100) shows that $n \geq m-1$. Hence, $n = m-1$.

Let p_1 be the smallest prime divisor of u_m. We show that $p_1 > 13$.

Assume $p_1 = 3$. Since $3 \mid u_m$, it follows that $3 \mid m$. Hence, $37 \mid u_3 \mid u_m$. It follows that $36 \mid \phi(au_m) = bu_n$. Since u_n is odd and $b < 10$, it follows that $3 \mid u_n$. Hence, $2 \mid n$. This contradicts the fact that m is even and $n = m-1$.

Clearly, $p_1 \neq 5$.

If $p_1 = 7$, then $7 \mid u_m$; hence, $6 \mid m$. In particular, $3 \mid u_m$ which is a case already treated.

If $p_1 = 11$, then $10 \mid \phi(au_m) = bu_n$. This is impossible because $(10,\ u_n) = 1$ and $b < 10$.

Finally, if $p_1 = 13$, then $13 \mid u_m$; hence, $6 \mid m$. In particular, $3 \mid u_m$ which is a case already treated.

Since $p_1 > 13$, it follows that $(u_m,\ ab) = 1$. Since $n = m-1$, it follows that $(u_m,\ u_n) = 1$. In particular, $(u_m,\ bu_n) = 1$. This shows that u_m is square free. From inequality (99), it follows that u_m is a product of at most 3 primes.

We show that u_m cannot be prime. Indeed if $p = u_m$, then $p \equiv 1 \pmod 5$. This shows that $5 \mid \phi(au_m) = bu_n$. Since $5 \nmid u_n$, it follows that $5 \mid b$. Hence, $b = 5$. In this case bu_n is odd. However, the only positive integers k such that $\phi(k)$ is odd are 1 and 2. This contradicts the fact that $m > 1$.

We now show that b is 8. This is certainly true if u_m is a product of 3 different primes. On the other hand, if $u_m = p_1p_2$, then $p_1p_2 = u_m \equiv -1 \pmod 4$. This shows that at least one of the two primes p_1 and p_2 is congruent to 1 modulo 4. This implies that $b = 8$. Since $(a,\ u_m) = 1$, it follows that

$$8u_{m-1} = bu_n = \phi(au_m) = \phi(a)\phi(u_m). \tag{101}$$

Since $\phi(u_m)$ is divisible by 8 and u_{m-1} is odd, it follows that $\phi(a)$ is odd. Hence, $\phi(a) = 1$. We may suppose that $a = 1$. Equation (101) becomes

$$\phi(u_m) = 8u_{m-1}. \tag{102}$$

Suppose now that $u_m = p_1p_2$ where $p_1 < p_2$. Then,

$$\begin{aligned} \frac{2 \cdot 10^{m-1}+7}{9} &= \frac{10^m-1}{9} - 8 \cdot \frac{10^{m-1}-1}{9} \\ &= u_m - 8u_{m-1} = p_1p_2 - (p_1-1)(p_2-1) \\ &= p_1 + p_2 - 1 < 2p_2. \end{aligned} \tag{103}$$

Hence,

$$p_2 > \frac{10^{m-1}+3.5}{9}. \tag{104}$$

It follows that

$$p_1 = \frac{u_m}{9p_2} < \frac{10^m-1}{10^{m-1}+3.5} < 10$$

which contradicts the fact that $p_1 > 13$.

Finally, assume that $u_m = p_1p_2p_3$ where $p_1 < p_2 < p_3$. Then,

$$\begin{aligned}\frac{2\cdot 10^{m-1}+7}{9} &= \frac{10^m-1}{9} - 8\cdot\frac{10^{m-1}-1}{9} = u_m - 8u_{m-1}\\ &= p_1p_2p_3 - (p_1-1)(p_2-1)(p_3-1)\\ &= p_1p_2+p_1p_3+p_2p_3-p_1-p_2-p_3+1 < 3p_2p_3. \qquad (105)\end{aligned}$$

Hence,

$$p_2p_3 > \frac{2\cdot 10^{m-1}+7}{27}.$$

It follows that

$$p_1 = \frac{u_m}{9p_2p_3} < \frac{3\cdot 10^m-3}{2\cdot 10^{m-1}+7} < 15$$

which contradicts the fact that $p_1 > 13$. □

Proof of Proposition 2

The proof is very similar to the proof of Proposition 1. We shall treat only equation (9) and leave equation (10) as an exercise to the reader.

One can check that the given solutions are the only ones for $m \le 8$. From now on, assume that $m > 8$. Since

$$L_m > \phi(L_m) = L_n,$$

it follows that $m > n$.

We now show that $\mathrm{ord}_2(L_n) \le 2$. Indeed, the sequence $(L_k)_{k\ge 0}$ is periodic modulo 8 with period 12. Moreover, by investigating the values L_k for $k = 0,\ 1,\ \ldots,\ 11$, one concludes easily that L_k is never a multiple of 8. Since

$$\mathrm{ord}_2(\phi(L_m)) = \mathrm{ord}_2(L_n) \le 2,$$

it follows, by Lemma 2, that

$$\frac{L_n}{L_m} = \frac{\phi(L_m)}{L_m} \ge \frac{1}{4}$$

or

$$4L_n \ge L_m. \tag{106}$$

From equation (106), we conclude easily that $n \geq m-2$. Indeed assume that $n \leq m-3$. From inequality (106), we get

$$4L_{m-3} \geq 4L_n \geq L_m = L_{m-1} + L_{m-2} = 2L_{m-2} + L_{m-3} = 3L_{m-3} + 2L_{m-4}$$

or

$$L_{m-3} \geq 2L_{m-4}$$

or

$$L_{m-4} + L_{m-5} \geq 2L_{m-4}$$

or

$$L_{m-5} \geq L_{m-4}$$

which is certainly false for $m \geq 8$. Hence, $n \in \{m-1,\ m-2\}$. In particular, $(L_m,\ L_n) = 1$. Hence, L_m is odd and squarefree. Since $\text{ord}_2(\phi(L_m)) = \text{ord}_2(L_n) \leq 2$, it follows that L_m is either a prime or a product of two distinct primes.

If $L_m = p_1$, then

$$L_m - L_n = L_m - \phi(L_m) = p_1 - (p_1 - 1) = 1$$

or

$$1 = L_m - L_n \geq L_m - L_{m-1} = L_{m-2}$$

which is certainly false for $m \geq 8$.

Finally, if $L_m = p_1 p_2$ with $p_1 < p_2$, then

$$L_m - L_n = L_m - \phi(L_m) = p_1 p_2 - (p_1 - 1)(p_2 - 1) = p_1 + p_2 - 1 < 2p_2$$

or

$$2p_2 > L_m - L_n \geq L_m - L_{m-1} = L_{m-2}.$$

Hence,

$$p_1 = \frac{L_m}{p_2} < \frac{2L_m}{L_{m-2}} = \frac{2(L_{m-1} + L_{m-2})}{L_{m-2}} = \frac{2(2L_{m-2} + L_{m-3})}{L_{m-2}} < 6.$$

Since

$$L_k^2 - 5F_k^2 = 4(-1)^k \qquad \text{for } k = 0,\ 1,\ \ldots,$$

it follows that $p_1 \neq 5$. Since p_1 is odd, it follows that $p_1 = 3$. Hence,

$$L_m - L_n = L_m - \phi(L_m) = 3p_2 - 2(p_2 - 1) = p_2 + 2 = \frac{L_m}{3} + 2$$

or

$$\begin{aligned} 6 = 2L_m - 3L_n \geq 2L_m - 3L_{m-1} &= 2L_{m-1} + 2L_{m-2} - 3L_{m-1} = 2L_{m-2} - L_{m-1} \\ &= 2L_{m-2} - (L_{m-2} + L_{m-3}) = L_{m-2} - L_{m-3} = L_{m-4}. \end{aligned}$$

Hence,

$$L_{m-4} \leq 6 < 7 = L_4$$

which contradicts the fact that $m \geq 8$. $\square$

Acknowledgements. This work was done while the author was visiting the University of Bielefeld. He would like to thank Professor A. Dress and his research group for their hospitality during his visit and the Alexander von Humboldt Foundation for support.

References

1. A. Baker and G. Wüstholz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993), 19–62.
2. R.D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. Math.* **15** (1913), 30–70.
3. F. Luca, On the equation $\phi(|x^m+y^m|)=|x^n+y^n|$, *Indian J. Pure Appl. Math.* **30** (1999), 183–197.
4. F. Luca, On the equation $\phi(x^m-y^m)=x^n+y^n$, *Irish Math. Soc. Bull.* **40** (1998) 46–55.
5. F. Luca, Equations involving arithmetic functions of Fibonacci and Lucas numbers, *Fibonacci Quart.* **38** (2000), 49–55.
6. F. Luca, Pascal's triangle and constructible polygons, *Util. Math.* **58** (2000), 209–214.
7. T.N. Shorey, A.J. Van der Poorten, R. Tijdeman, and A. Schinzel, Applications of the Gel'fond-Baker method to diophantine equations, *Transcendence theory: advances and applications*, 59–77, Academic Press, London, 1977.
8. C.L. Stewart, On divisors of terms of linear recurrence sequences, *J. Reine Angew. Math.* **333** (1982), 12–31.
9. K.R. Yu, Linear forms in p-adic logarithms III, *Compositio Math.* **91** (1994), 241–276.