



Concatenations with Binary Recurrent Sequences

William D. Banks
Department of Mathematics
University of Missouri
Columbia, MO 65211
USA
bbanks@math.missouri.edu

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180
Morelia, Michoacán
México
fluca@matmor.unam.mx

Abstract

Given positive integers A_1, \dots, A_t and $b \geq 2$, we write $\overline{A_1 \cdots A_t}_{(b)}$ for the integer whose base- b representation is the concatenation of the base- b representations of A_1, \dots, A_t . In this paper, we prove that if $(u_n)_{n \geq 0}$ is a binary recurrent sequence of integers satisfying some mild hypotheses, then for every fixed integer $t \geq 1$, there are at most finitely many nonnegative integers n_1, \dots, n_t such that $\overline{|u_{n_1}| \cdots |u_{n_t}|}_{(b)}$ is a member of the sequence $(|u_n|)_{n \geq 0}$. In particular, we compute all such instances in the special case that $b = 10$, $t = 2$, and $u_n = F_n$ is the sequence of Fibonacci numbers.

1 Introduction

A result of Senge and Straus [24, 25] asserts that if $b_1, b_2 \geq 2$ are multiplicatively independent integers, there are at most finitely many positive integers with the property that the sum of the digits in each of the two bases b_1 and b_2 lies below any prescribed bound. An effective

version of this statement is due to Stewart [28], who gave a lower bound on the overall sum of the digits of n in base b_1 and in base b_2 . A somewhat more general version of Stewart's result has been obtained by Luca [16].

A variety of arithmetical questions about integers whose base- b digits satisfy certain restrictions has been considered by many authors; see, for example, [1, 2, 3, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, 16, 18, 19, 27] and the references contained therein. Here, we consider integers whose base- b digits are formed by concatenating (absolute values of) terms in a binary recurrent sequence.

Let $(u_n)_{n \geq 0}$ be a *binary recurrent sequence* of integers; i.e., a sequence of integers satisfying the recurrence relation

$$u_{n+2} = ru_{n+1} + su_n \quad (n \geq 0), \quad (1)$$

where r and s are nonzero integers with $r^2 + 4s \neq 0$. It is well known that if α and β are the roots of the equation $x^2 - rx - s = 0$, then $u_n = c\alpha^n + d\beta^n$ holds for all $n \geq 0$, where c and d are constants given by

$$c = \frac{-\beta u_0 + u_1}{\alpha - \beta} \quad \text{and} \quad d = \frac{\alpha u_0 - u_1}{\alpha - \beta}.$$

Throughout the paper, we assume that $(u_n)_{n \geq 0}$ is *nondegenerate* (i.e., α/β is not a root of 1, and $\alpha\beta cd \neq 0$). Reordering the roots if necessary, we can further assume that $|\alpha| \geq |\beta|$ and $|\alpha| > 1$.

Let $b \geq 2$ be a fixed integer base. Given positive integers A_1, \dots, A_t , we denote by $\overline{A_1 \cdots A_t}_{(b)}$ the integer whose base- b representation is equal to the concatenation (in order) of the base- b representations of A_1, \dots, A_t . Thus, if l_i is the smallest positive integer such that $A_i < b^{l_i}$, we have

$$\overline{A_1 \cdots A_t}_{(b)} = b^{l_2 + \cdots + l_t} A_1 + b^{l_3 + \cdots + l_t} A_2 + \cdots + b^{l_t} A_{t-1} + A_t.$$

We always assume that $A_1 \neq 0$, and in the special case that $b = 10$, we omit the subscript to simplify the notation.

In this paper, we study the set of positive integers $|u_n|$, where $(u_n)_{n \geq 0}$ is a binary recurrent sequence, that are the base- b concatenations of other numbers of the form $|u_{n_j}|$, $j = 1, \dots, t$. We show that if $t \geq 2$ is fixed, then there are only finitely many instances of the equality

$$|u_n| = \overline{|u_{n_1}| \cdots |u_{n_t}|}_{(b)}$$

provided that the sequence $(u_n)_{n \geq 0}$ satisfies certain mild hypotheses. Note that some assumptions are clearly needed in order to rule out certain obvious counterexamples; for instance, the result does not hold for the sequence $u_n = b^n - 1$, $n \geq 0$, since the concatenation of any two or more terms produces another term of the same sequence.

Theorem 1. *Let $u_n = c\alpha^n + d\beta^n$ be a nondegenerate binary recurrent sequence of integers, and let $b \geq 2$ be a fixed integer base. Assume that $\dim_{\mathbb{Z}} \langle \log \alpha, \log \beta, \log b \rangle \geq$*

2. Then for every fixed integer $t \geq 2$, there are at most finitely many positive integers n for which the equality

$$|u_n| = \overline{|u_{n_1}| \underbrace{0 \cdots 0}_{m_1} |u_{n_2}| \underbrace{0 \cdots 0}_{m_2} \cdots |u_{n_t}| \underbrace{0 \cdots 0}_{m_t}} \quad (b) \quad (2)$$

holds for some nonnegative integers n_1, \dots, n_t and m_1, \dots, m_t with $u_{n_1} \neq 0$.

Here, $\log(\cdot)$ stands for any fixed determination of the natural logarithm function, and $\dim_{\mathbb{Z}} \langle \log \alpha, \log \beta, \log b \rangle$ denotes the rank of (the free part of) the additive subgroup of \mathbb{C} generated by $\{\log \alpha, \log \beta, \log b\}$.

Although our proof of Theorem 1 is ineffective, this result can be seen as an extension of the aforementioned results of Senge and Straus [24, 25].

In some special cases, one can employ effective methods to completely determine all the solutions to an equation such as (2). Perhaps the best known example of a binary recurrent sequence is the *Fibonacci sequence* $(F_n)_{n \geq 0}$, where $F_0 = 0$ and $F_1 = 1$, and (1) holds with $r = s = 1$. In this case, one has $\alpha = (1 + \sqrt{5})/2$, $\beta = -\alpha^{-1}$, $c = 1/(\alpha - \beta)$, and $d = -c$. For this special sequence, we obtain the following computational result:

Theorem 2. *If (m, n, k) is an ordered triple of nonnegative integers with $m > 0$ and $\overline{F_m F_n} = F_k$, then $F_k \in \{13, 21, 55\}$.*

Throughout the paper, we use the Vinogradov symbols \ll and \gg , as well as the Landau symbol O , with the understanding that the implied constants are computable and depend at most on the given data.

2 Preliminaries

Let \mathbb{L} be an algebraic number field of degree D over \mathbb{Q} . Denote by $\mathcal{O}_{\mathbb{L}}$ the ring of algebraic integers and by $\mathcal{M}_{\mathbb{L}}$ the set of places. For a fractional ideal \mathcal{I} of \mathbb{L} , let $\text{Nm}_{\mathbb{L}}(\mathcal{I})$ be the usual norm; we recall that $\text{Nm}_{\mathbb{L}}(\mathcal{I}) = \#(\mathcal{O}_{\mathbb{L}}/\mathcal{I})$ if \mathcal{I} is an ideal of $\mathcal{O}_{\mathbb{L}}$, and the norm map is extended multiplicatively (using unique factorization) to all of the fractional ideals of \mathbb{L} .

For a prime ideal \mathcal{P} , we denote by $\text{ord}_{\mathcal{P}}(x)$ the order at which \mathcal{P} appears in the ideal factorization of the principal ideal $[x]$ generated by x in \mathbb{L} .

For a place $\mu \in \mathcal{M}_{\mathbb{L}}$ and a number $x \in \mathbb{L}$, we define the absolute value $|x|_{\mu}$ as follows:

- (i) $|x|_{\mu} = |\sigma(x)|^{1/D}$ if μ corresponds to a real embedding $\sigma : \mathbb{L} \rightarrow \mathbb{R}$;
- (ii) $|x|_{\mu} = |\sigma(x)|^{2/D} = |\bar{\sigma}(x)|^{2/D}$ if μ corresponds to some pair of complex conjugate embeddings $\sigma, \bar{\sigma} : \mathbb{L} \rightarrow \mathbb{C}$;
- (iii) $|x|_{\mu} = \text{Nm}_{\mathbb{L}}(\mathcal{P})^{-\text{ord}_{\mathcal{P}}(x)/D}$ if μ corresponds to a nonzero prime ideal \mathcal{P} of $\mathcal{O}_{\mathbb{L}}$.

In the case (i) or (ii), we say that μ is *real infinite* or *complex infinite*, respectively; in the case (iii), we say that μ is *finite*.

The set of absolute values are well known to satisfy the following *product formula*:

$$\prod_{\mu \in \mathcal{M}_{\mathbb{L}}} |x|_{\mu} = 1, \quad \text{for all } x \in \mathbb{L}^*. \quad (3)$$

One of our principal tools is the following simplified version of a result of Schlickewei [22, 23], which is commonly known as the *Subspace Theorem*:

Theorem 3. *Let \mathbb{L} be an algebraic number field of degree D . Let \mathcal{S} be a finite set of places of \mathbb{L} containing all the infinite ones. Let $\{L_{1,\mu}, \dots, L_{N,\mu}\}$ for $\mu \in \mathcal{S}$ be linearly independent sets of linear forms in N variables with coefficients in \mathbb{L} . Then, for every fixed $0 < \varepsilon < 1$, the set of solutions $\mathbf{x} = (x_1, \dots, x_N) \in \mathbb{L}^N \setminus \{\mathbf{0}\}$ to the inequality*

$$\prod_{\mu \in \mathcal{S}} \prod_{i=1}^N |L_{i,\mu}(\mathbf{x})|_{\mu} \leq (\max\{|x_i| : i = 1, \dots, N\})^{-\varepsilon} \quad (4)$$

is contained in finitely many proper linear subspaces of \mathbb{L}^N .

Let \mathcal{S} be a finite subset of $\mathcal{M}_{\mathbb{L}}$ containing all the infinite places. An element $x \in \mathbb{L}$ is called a *\mathcal{S} -unit* if $|x|_{\mu} = 1$ for all $\mu \notin \mathcal{S}$. An equation of the form

$$\sum_{i=1}^N a_i x_i = 0, \quad (5)$$

where each $a_i \in \mathbb{L}^*$, is called an *\mathcal{S} -unit equation* if each x_i is an \mathcal{S} -unit; it is said to be *nondegenerate* if no proper subsum of the left hand side vanishes. It is clear that if $\mathbf{x} = (x_1, \dots, x_N)$ is a solution of the \mathcal{S} -unit equation (5), and ρ is a \mathcal{S} -unit in \mathbb{L}^* , then $\rho\mathbf{x} = (\rho x_1, \dots, \rho x_N)$ is also a solution of (5); in this case, the solutions \mathbf{x} and $\rho\mathbf{x}$ are said to be *equivalent*. We recall the following result of Schlickewei [21] (see also [8]) on \mathcal{S} -unit equations:

Theorem 4. *Let a_1, \dots, a_N be fixed numbers in \mathbb{L}^* . Then the \mathcal{S} -unit equation (5) has only finitely many equivalence classes of nondegenerate solutions (x_1, \dots, x_N) . Moreover, the number of such equivalence classes is bounded by a constant that depends only on N and the cardinality of \mathcal{S} .*

An immediate consequence of Theorem 4 is that if $\mathbf{x} = (x_1, \dots, x_N)$ is a solution of the \mathcal{S} -unit equation (5), then the ratios x_i/x_j for $1 \leq i < j \leq N$ can assume only finitely many values.

We shall also need some estimates from the theory of lower bounds for linear forms in logarithms, both in the complex and the p -adic cases.

Let α_1 and α_2 be algebraic numbers. Put $\mathbb{L} = \mathbb{Q}[\alpha_1, \alpha_2]$, and let D be the degree of \mathbb{L} over \mathbb{Q} . Let A_1 and A_2 be two positive integers such that

$$\log A_i \geq \max \left\{ h(\alpha_i), \frac{|\log \alpha_i|}{D}, \frac{1}{D} \right\} \quad (i = 1, 2). \quad (6)$$

Here, for an algebraic number α whose minimal polynomial over \mathbb{Z} has the form $a \prod_{i=1}^d (X - \alpha^{(i)})$, we write $h(\alpha)$ for the logarithmic height of α , which is given by

$$h(\alpha) = \frac{1}{d} \left(\log |a| + \sum_{i=1}^d \log (\max\{1, |\alpha^{(i)}|\}) \right).$$

Let b_1 and b_2 be positive integers, and put $\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1$. Finally, let

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

The following result is Corollaire 2 on page 288 of [20], which gives an effective lower bound on the size of $\log |\Lambda|$:

Theorem 5. *Assume that α_1 and α_2 are real, positive, and multiplicatively independent. Then*

$$\log |\Lambda| \geq -24.34D^4 \left(\max \left\{ \log b' + 0.14, \frac{21}{D}, \frac{1}{2} \right\} \right)^2 \log A_1 \log A_2.$$

We also need a p -adic lower bound on Λ , that is, an upper bound on the order at which a prime ideal \mathcal{P} can appear in the factorization of the principal ideal generated by $\Lambda_1 = \alpha_1^{b_1} - \alpha_2^{b_2}$ inside $\mathcal{O}_{\mathbb{L}}$. For this, let p be the prime number such that $\mathcal{P} \mid p$ (i.e., $p\mathbb{Z} = \mathcal{P} \cap \mathbb{Z}$), and let f be such that the finite field $\mathcal{O}_{\mathbb{L}}/\mathcal{P}$ has p^f elements. Let g be the smallest positive integer such that \mathcal{P} divides both $\alpha_1^g - 1$ and $\alpha_2^g - 1$. Assume further that A_i satisfies the inequality (6) as well as the inequality $\log A_i \geq f(\log p)/D$, for $i = 1, 2$. The following result is an easy consequence of Corollaire 2 on page 315 of [4]:

Theorem 6. *Assume that α_1 and α_2 are multiplicatively independent. Then*

$$\begin{aligned} \text{ord}_{\mathcal{P}}(\Lambda_1) &\leq \frac{24pgD^5}{f^4(p-1)(\log p)^4} \\ &\times \left(\max \left\{ \log b' + \log \log p + 0.4, \frac{10f \log p}{D}, 10 \right\} \right)^2 \log A_1 \log A_2. \end{aligned}$$

3 Proof of Theorem 1

Our proof of Theorem 1 also treats the (slightly more general) case in which we allow $t = 1$, but in this case we add the additional hypothesis that $m_1 \geq 1$ (clearly, this condition is needed to insure that the number of solutions to (2) is finite).

Since α/β is not a root of unity, at most one element of the sequence $(u_n)_{n \geq 0}$ is equal to 0. Hence, if $u_{n_i} = 0$ for some i in (2), then n_i is uniquely determined. Note that $i \neq 1$. If this happens, then equation (2) can be viewed as an equation of the same form, but with t replaced by $t - 1$ (and with only $2t - 1$ unknowns). Thus, to prove the theorem, it suffices to show that there at most finitely many solutions to (2) with $u_{n_i} \neq 0$, $i = 1, \dots, t$.

Let $\mathbb{L} = \mathbb{Q}[\alpha, \beta]$, and let \mathcal{S} be the set of all infinite places of \mathbb{L} and all finite places that divide $sb = -\alpha\beta b$. For a positive integer m , let $\ell_b(m)$ denote the number of the digits in the base- b representation of m .

Equation (2) is equivalent to

$$|u_n| = \sum_{i=1}^t |u_{n_i}| b^{s_i}, \quad (7)$$

where

$$s_i = \sum_{j=i}^t m_j + \sum_{j=i+1}^t \ell_b(|u_{n_j}|) \quad (i = 1, \dots, t).$$

We remark that, if $n = n_i$ for some i , it follows that $t = 1$ (since each $u_{n_i} \neq 0$) and $s_1 = m_1 = 0$ (since $b \geq 2$), which contradicts our assumption that $m_1 \geq 1$ when $t = 1$. Hence, $n \neq n_i$ for all $i = 1, \dots, t$. Now write (7) in the form

$$\varepsilon_0(c\alpha^n + d\beta^n) = \sum_{i=1}^t \varepsilon_i (c\alpha^{n_i} + d\beta^{n_i}) b^{s_i}, \quad (8)$$

where $\varepsilon_i \in \{\pm 1\}$ for $i = 0, \dots, t$.

Suppose first that $n_i > n - \kappa$ for some $i \in \{1, \dots, t\}$, where $\kappa \geq 0$ is a constant to be specified later. From (7), we have that $|u_n| \geq |u_{n_i}| b^{s_i}$. It is known that the estimate $|u_m| = |\alpha|^{m+O(\log m)}$ holds for all positive integers $m \geq 2$ (see Theorem 3.1 on page 64 in [26]). Moreover, if α is real, then $|\alpha| > |\beta|$, and one has the estimate $|u_m| = |\alpha|^{m+O(1)}$. Therefore, since $|\alpha| > 1$, the following bound holds if $n_i > n - \kappa$:

$$\max\{n_i - n, s_i\} \ll \begin{cases} 1, & \text{if } \alpha \in \mathbb{R}; \\ \log n, & \text{if } \alpha \notin \mathbb{R} \quad (\text{i.e., } \alpha = \bar{\beta}). \end{cases} \quad (9)$$

Next, we show that if $n_i \leq n - \kappa$ for every $i = 1, \dots, t$, then there exists an index $i \in \{1, \dots, t\}$ for which the following bound holds:

$$\max\{n - n_i, s_i\} \ll 1. \quad (10)$$

To do this, we first observe that (8) is an \mathcal{S} -unit equation with $N = 2t + 2$ terms, coefficients $(a_1, \dots, a_N) = (c, d, -c, -d, \dots, -c, -d)$, and the \mathcal{S} -unit unknowns $\mathbf{x} = (x_1, \dots, x_N) = (\varepsilon_0\alpha^n, \varepsilon_0\beta^n, \varepsilon_1\alpha^{n_1}b^{s_1}, \dots, \varepsilon_t\beta^{n_t}b^{s_t})$.

If the \mathcal{S} -unit equation (8) is nondegenerate, then $x_1/x_2 = (\alpha/\beta)^n$ can assume only finitely many values; since α/β is not a root of unity, it follows that n can take at most finitely many values.

On the other hand, if the \mathcal{S} -unit equation (8) is degenerate, let E_1 and E_2 be two (not necessarily distinct) nondegenerate subequations of (8) that contain the unknowns $x_1 = \varepsilon_0\alpha^n$ and $x_2 = \varepsilon_0\beta^n$, respectively. Clearly, E_1 and E_2 can be chosen in at most finitely many ways. The preceding argument shows that n can assume only finitely many values if the unknowns x_1 and x_2 both lie in E_1 or both lie in E_2 . Therefore, we may assume that E_1 does not contain x_2 , and E_2 does not contain x_1 . We now distinguish the following cases:

- (i) E_1 contains an unknown of the form $x_{2i+1} = \varepsilon_i\alpha^{n_i}b^{s_i}$ for some $i \geq 1$ and E_2 contains an unknown of the form $x_{2j} = \varepsilon_j\beta^{n_j}b^{s_j}$ for some $j \geq 2$.

In this case, both $x_1/x_{2i+1} = \pm\alpha^{n-n_i}b^{-s_i}$ and $x_2/x_{2j} = \pm\beta^{n-n_j}b^{-s_j}$ can assume only finitely many values. Since $\dim_{\mathbb{Z}}\langle\log\alpha, \log\beta, \log b\rangle \geq 2$, it follows that either the pair (α, b) or the pair (β, b) is multiplicatively independent. Hence, either $\max\{n-n_i, s_i\} \ll 1$ or $\max\{n-n_j, s_j\} \ll 1$.

- (ii) E_1 contains only unknowns of the form $x_{2i} = \varepsilon_i\beta^{n_i}b^{s_i}$ with $i \geq 2$ (except for x_1) and E_2 contains only unknowns of the form $x_{2j+1} = \varepsilon_j\alpha^{n_j}b^{s_j}$ with $j \geq 1$ (except for x_2).

For each choice of the indices i and j , both $x_1/x_{2i} = \pm\alpha^n\beta^{-n_i}b^{-s_i}$ and $x_2/x_{2j+1} = \pm\beta^n\alpha^{-n_j}b^{-s_j}$ can have at most finitely many values. Since we may assume that n takes infinitely many values (otherwise, there is nothing to prove), it follows that there exist numbers n^* , n_i^* , n_j^* , s_i^* , and s_j^* such that both relations

$$\begin{aligned}\alpha^n\beta^{-n_i}b^{-s_i} &= \alpha^{n^*}\beta^{-n_i^*}b^{-s_i^*}, \\ \beta^n\alpha^{-n_j}b^{-s_j} &= \beta^{n^*}\alpha^{-n_j^*}b^{-s_j^*},\end{aligned}\tag{11}$$

hold for arbitrarily large values of n . Among all possible choices for the quintuple $(n^*, n_i^*, n_j^*, s_i^*, s_j^*)$ of such numbers, we fix one for which n_i^* is as small as possible; thus, $n_i \geq n_i^*$ whenever the relations (11) hold.

Since there are only finitely many possibilities for E_1 and E_2 and (once these are fixed) for the indices i and j , we obtain in this way a finite list of such quintuples $(n^*, n_i^*, n_j^*, s_i^*, s_j^*)$. Hence, the constant κ can be initially chosen such that the inequality $\kappa > \max\{n^* - n_i^*, n^* - n_j^*\}$ holds in all cases.

Now let E_1 , E_2 , i , and j be fixed, and suppose that the relations (11) hold with $n > n^*$. Taking logarithms, we obtain that

$$\begin{aligned}(n - n^*)\log\alpha &= (n_i - n_i^*)\log\beta + (s_i - s_i^*)\log b, \\ (n - n^*)\log\beta &= (n_j - n_j^*)\log\alpha + (s_j - s_j^*)\log b.\end{aligned}$$

Let $v_1 = (n_i - n_i^*)/(n - n^*)$ and $v_2 = (n_j - n_j^*)/(n - n^*)$, and note that both numbers are rational. Since we are assuming that $n_i \leq n - \kappa$ for $i = 1, \dots, t$, it follows that

$$n^* - n_i^* < \kappa \leq n - n_i,$$

which implies that $v_1 < 1$. Similarly, $v_2 < 1$. Since $n_i \geq n_i^*$ by our choice of the quintuple $(n^*, n_i^*, n_j^*, s_i^*, s_j^*)$, we also see that $v_1 \geq 0$. These statements together imply that $v_1v_2 \neq 1$, which is all we need. From the preceding relations, we obtain that

$$\log\alpha = v_1\log\beta + w_1\log b = v_1(v_2\log\alpha + w_2\log b) + w_1\log b,$$

where $w_1 = (s_i - s_i^*)/(n - n^*)$ and $w_2 = (s_j - s_j^*)/(n - n^*)$ are rational numbers. Since $v_1v_2 \neq 1$, this implies that $\log\alpha/\log b$ is rational. Similarly, we see that $\log\beta/\log b$ is rational. But these statements contradict our hypothesis that $\dim_{\mathbb{Z}}\langle\log\alpha, \log\beta, \log b\rangle \geq 2$; therefore, n is bounded, and it follows that n_i , n_j , s_i , and s_j are bounded as well.

(iii) *The remaining cases.*

For the remaining cases, there are only two possibilities:

- E_1 contains an unknown of the form $x_{2i+1} = \varepsilon_i \alpha^{n_i} b^{s_i}$ for some $i \geq 1$ and E_2 contains only unknowns of the form $x_{2j+1} = \varepsilon_j \alpha^{n_j} b^{s_j}$ with $j \geq 1$ (except for x_2).
- E_1 contains only unknowns of the form $x_{2i} = \varepsilon_i \beta^{n_i} b^{s_i}$ with $i \geq 2$ (except for x_1) and E_2 contains an unknown of the form $x_{2j} = \varepsilon_j \beta^{n_j} b^{s_j}$ for some $j \geq 2$.

We treat only the first case, as the second case is similar.

We note that the ratio $x_1/x_{2i+1} = \pm \alpha^{n-n_i} b^{-s_i}$ assumes only finitely many values. If α and b are multiplicatively independent, it follows that both $n - n_i$ and s_i are bounded, and we are done. On the other hand, if $n - n_i$ is not bounded, it follows that $\log \alpha / \log b$ is rational. If j is such that $x_{2j+1} \in E_2$, then $x_2/x_{2j+1} = \pm \beta^n \alpha^{-n_j} b^{-s_j}$ can take at most finitely many values. Since α and b are multiplicatively dependent, β and b must be multiplicatively independent, and it follows that n can take only finitely many values. But this is impossible if $n - n_i$ is unbounded.

The analysis above completes our proof that (10) holds for some i in the case that $n_i \leq n - \kappa$ for all $i = 1, \dots, t$. Combining (9) and (10), we see that the bound

$$\max\{|n - n_i|, s_i\} \ll \begin{cases} 1, & \text{if } \alpha \in \mathbb{R}; \\ \log n, & \text{if } \alpha \notin \mathbb{R} \quad (\text{i.e., } \alpha = \bar{\beta}) \end{cases} \quad (12)$$

holds for some $i \in \{1, \dots, t\}$ in every case.

We now select i such that (12) holds and rewrite (8) in the form

$$c\alpha^n + d\beta^n + Ab^{s_i-1} + c_1\alpha^{n_i}b^{s_i} + d_1\beta^{n_i}b^{s_i} + B = 0, \quad (13)$$

where $c_1 = -\varepsilon_i \varepsilon_0 c$, $d_1 = -\varepsilon_i \varepsilon_0 d$,

$$A = -\sum_{j=1}^{i-1} \varepsilon_j \varepsilon_0 u_{n_j} b^{s_j - s_i - 1} \quad \text{and} \quad B = -\sum_{j=i+1}^t \varepsilon_j \varepsilon_0 u_{n_j} b^{s_j}.$$

Since

$$b^{s_i-1} \geq |u_{n_i}| \geq |\alpha|^{n_i + O(\log n_i)} = |\alpha|^{n + O(\log n)},$$

we see that $A = \exp(O(\log n))$. Similarly, since $b^{s_i} \geq B$, it follows that $B = \exp(O(\log n))$.

Assume first that both $n - n_i$ and s_i are bounded (this is the case, for instance, if \mathbb{L} is real). In this case, A and B are bounded as well; hence, we can assume that they are fixed. Here, (13) becomes

$$C_1\alpha^n + D_1\beta^n + Ab^{s_i-1} + B = 0, \quad (14)$$

where $C_1 = c + c_1\alpha^{n_i-n}$ and $D_1 = d + d_1\beta^{n_i-n}$ can also be regarded as fixed numbers. The case $A = B = C_1 = D_1 = 0$ leads to $i = t = 1$, $\alpha^{n-n_i} = -cc_1^{-1} = \pm 1$ and $\beta^{n-n_i} = -dd_1^{-1} = \pm 1$; therefore, $t = 1$, $n = n_1$, and $m_1 = 0$, which contradicts our assumption that $m_1 \geq 1$ when $t = 1$. Consequently, the equation (14) is nontrivial. If any two of the coefficients

A, B, C_1, D_1 are zero, then either n or s_{i-1} is bounded, and this leads to at most finitely many possibilities for n . A similar argument based on Theorem 4 can be used if one of the coefficients A, B, C_1, D_1 is zero, or if $ABC_1D_1 \neq 0$, to show that there are at most finitely many possibilities for n .

Thus, from now on, we can suppose that either $n - n_i$ or s_i is unbounded over the set of solutions to (13). In this case, α and β are complex conjugates.

Assume first that $B \neq 0$ in equation (13). Suppose also that $A \neq 0$. We apply Theorem 3 with $N = 5$, the linear forms $L_{j,\mu}(\mathbf{x}) = x_j$ for each $j = 1, \dots, 5$, and $\mu \in \mathcal{S}$, except when $j = 1$ and μ is infinite, in which case we take $L_{1,\mu}(\mathbf{x}) = cx_1 + dx_2 + x_3 + c_1x_4 + d_1x_5$ (note that, as \mathbb{L} is complex quadratic, there is only one infinite place). We evaluate the double product appearing in Theorem 3 for our system of forms and the points $\mathbf{x} = (\alpha^n, \beta^n, Ab^{s_{i-1}}, \alpha^{n_i}b^{s_i}, \beta^{n_i}b^{s_i})$. Clearly,

$$\prod_{\mu \in \mathcal{S}} |L_{j,\mu}(\mathbf{x})| = 1 \quad (15)$$

if $j \in \{2, 4, 5\}$, since x_2, x_4 and x_5 are \mathcal{S} -units. Moreover,

$$\prod_{\mu \in \mathcal{S}} |L_{3,\mu}(\mathbf{x})| \leq A = \exp(O(\log n)). \quad (16)$$

Finally, since x_1 is an \mathcal{S} -unit, it follows from the product formula (3) that

$$\prod_{\substack{\mu \in \mathcal{S} \\ \mu \text{ finite}}} |L_{1,\mu}(\mathbf{x})|_{\mu} = \frac{1}{|\mathrm{Nm}_{\mathbb{L}}(\alpha^n)|} \leq \frac{1}{|\alpha|^n}, \quad (17)$$

while by equation (13), we have

$$\prod_{\substack{\mu \in \mathcal{S} \\ \mu \text{ is infinite}}} |L_{1,\mu}(\mathbf{x})|_{\mu} = B^2 \leq \exp(O(\log n)). \quad (18)$$

Multiplying the estimates (15), (16), (17) and (18), we derive that

$$\prod_{j=1}^N \prod_{\mu \in \mathcal{S}} |L_{j,\mu}(\mathbf{x})| \leq \frac{AB^2}{\alpha^n} \leq \exp(-n \log \alpha + O(\log n)). \quad (19)$$

Since $\max\{|x_j| : j = 1, \dots, N\} = |\alpha|^n$, the inequality (19) together with Theorem 3 (for example, with $\varepsilon = 1/2$ and $n > n_{\varepsilon}$), imply that there exist finitely many proper subspaces of \mathbb{L}^N containing all solutions \mathbf{x} . Thus, the relation

$$C_2\alpha^n + D_2\beta^n + C_3\alpha^{n_i}b^{s_i} + D_3\beta^{n_i}b^{s_i} + EAb^{s_{i-1}} = 0 \quad (20)$$

holds for some fixed coefficients C_2, D_2, C_3, D_3 and E in \mathbb{L} , which are not all equal to zero. If $A = 0$, then the same argument with $N = 4$ also yields an identity of the shape (20). Finally, if $B = 0$, then (13) is the same as (20) with $C_2 = c, D_2 = d, C_3 = c_1, D_3 = d_1$,

and $E = 1$. Clearly, we may assume that C_2 and D_2 are conjugate (over \mathbb{L}), that C_3 and D_3 are conjugate (over \mathbb{L}), and that $E \in \mathbb{Z}$ (if not, we can conjugate (20) and subtract the result from (20) to obtain a “shorter” nontrivial equation of the same type with the desired properties).

If $E = 0$, then (20) is a \mathcal{S} -unit equation. If it is nondegenerate, we see that $\alpha^n \beta^{-n}$ can take only finitely many values; since α/β is not a root of unity, there are at most finitely many possibilities for n . If the \mathcal{S} -unit equation is degenerate, then either $C_2 = D_2 = 0$, in which case n_i can take only finitely many values (and since $|n - n_i| \ll \log n$, it follows that n is bounded as well), or $C_2 D_2 \neq 0$ but $C_3 = D_3 = 0$, in which case n can again take only finitely many values, or $C_2 C_3 D_2 D_3 \neq 0$. In the last case, either $\alpha^{n-n_i} b^{-s_i}$ and $\beta^{n-n_i} b^{-s_i}$ can take only finitely many values, or $\alpha^n \beta^{-n_i} b^{-s_i}$ and $\beta^n \alpha^{-n_i} b^{-s_i}$ can take only finitely many values; but these are cases that have already been considered.

Finally, we are left with the possibility that $E \neq 0$, in which case we can assume that $E = 1$. We now rewrite (20) in the form

$$C_4 \alpha^n + D_4 \beta^n = -A b^{s_i-1}, \quad (21)$$

where $C_4 = C_2 + C_3 \alpha^{n_i-n} b^{s_i}$ and $D_4 = D_2 + D_3 \beta^{n_i-n} b^{s_i}$. Since C_4 and D_4 are conjugated in \mathbb{L} , it follows that they are simultaneously zero or nonzero.

Assume first that $C_4 = D_4 = 0$. Then both relations

$$C_2 = -C_3 \alpha^{n-n_i} b^{s_i} \quad \text{and} \quad D_2 = -D_3 \beta^{n-n_i} b^{s_i} \quad (22)$$

hold. If $C_2 = 0$ then $C_3 = 0$ (by (22)), $D_2 = 0$ (because C_2 and D_2 are conjugated), and therefore $D_3 = 0$ (by (22)); together with equation (20), these lead to $E = 0$, which is a contradiction. Thus, $C_2 \neq 0$, and the preceding argument implies that $C_2 C_3 D_2 D_3 \neq 0$. Now, equation (22) together with our hypothesis that $\dim_{\mathbb{Q}} \langle \log \alpha, \log \beta, \log b \rangle \geq 2$ lead to the conclusion that both $n - n_i$ and s_i are bounded, which is a case already treated.

We now assume that $C_4 D_4 \neq 0$. Let $\ell = \gcd(r^2, s)$, where r and s are the coefficients of the recurrence (1). Set $\alpha_1 = \alpha^2/\ell$, $\beta_1 = \beta^2/\ell$. Applying Lemma A.10 on page 20 in [26], we see that α_1 and β_1 are algebraic integers and that the principal ideals they generate in \mathbb{L} are coprime. Clearly, α_1 and β_1 are complex conjugates, and $|\alpha_1| > 1$. Write $n = 2m + \delta$, where $\delta \in \{0, 1\}$. Put $(C_5, D_5) = (C_4, D_4)$ if $\delta = 0$ and $(C_5, D_5) = (\alpha C_4, \beta D_4)$ if $\delta = 1$. Dividing both sides of equation (21) by ℓ^m , we see that the expression

$$C_5 \alpha_1^m + D_5 \beta_1^m$$

is a rational number such that every prime factor of its numerator or denominator divides either $Ab\alpha\beta$ or one of the denominators of C_2 , D_2 , C_3 , or D_3 . Let $\mathcal{P} = \{p_1, \dots, p_v\}$ be the set consisting of all of these primes, and write

$$C_5 \alpha_1^m + D_5 \beta_1^m = \prod_{i=1}^v p_i^{r_i}.$$

We now bound the order r_i of p_i . Let π_i be some prime ideal of \mathbb{L} lying above p_i . If $\pi_i | \alpha_1$, then $\text{ord}_{\pi_i}(\alpha_1^m) \geq m \geq n/2 - 1$. On the other hand, it is clear that

$$\max\{|\text{ord}_{\pi_i}(C_5)|, |\text{ord}_{\pi_i}(D_5)|\} \ll \max\{|n - n_i|, s_i\} \ll \log n.$$

Thus, for large n , we get that

$$\text{ord}_{\pi_i}(C_5\alpha_1^m + D_5\beta_1^m) = \text{ord}_{\pi_i}(D_5\beta_1^m) = \text{ord}_{\pi_i}(D_5) \ll \log n, \quad (23)$$

since α_1 and β_1 are coprime. A similar analysis can be used if $\pi_i|\beta_1$. Assume now that π_i does not divide $\alpha_1\beta_1$. Then

$$r_i = \text{ord}_{\pi_i}(C_5\alpha_1^m + D_5\beta_1^m) = \text{ord}_{\pi_i}(C_5\beta_1^m) + \text{ord}_{\pi_i}((\alpha_1/\beta_1)^m - (-D_5/C_5)).$$

Certainly,

$$\text{ord}_{\pi_i}(C_5\beta_1^m) = \text{ord}_{\pi_i}(C_5) \ll \log n,$$

while from Theorem 6, we deduce that

$$\text{ord}_{\pi_i}((\alpha_1/\beta_1)^m - (-D_5/C_5)) \ll (\log n)^2 |\log |C_5|| \ll (\log n)^3.$$

Thus,

$$\text{ord}_{\pi_i}(C_5\alpha_1^m + D_5\beta_1^m) \ll (\log n)^3 \quad (24)$$

in this case. Comparing inequalities (23) and (24), we see that inequality (24) always holds. Since this is true for all $i = 1, \dots, v$, we conclude that

$$\log |C_5\alpha_1^m + D_5\beta_1^m| \leq \sum_{i=1}^v r_i \log p_i \ll (\log n)^3. \quad (25)$$

On the other hand, we have

$$\log |C_5\alpha_1^m + D_5\beta_1^m| = \log |C_5| + m \log |\alpha_1| + \log |1 + (D_5C_5^{-1}(\beta_1\alpha_1^{-1})^m)|.$$

Clearly,

$$\log |C_5| \gg -\log n, \quad (26)$$

and using Theorem 5, we get that

$$\log |1 + (D_5C_5^{-1}(\beta_1\alpha_1^{-1})^m)| \gg -(\log n)^2 |\log |C_5||. \quad (27)$$

Putting together inequalities (25), (26), (27), and using the fact that $m \gg n$ and $|\alpha_1| > 1$, we obtain that

$$n \ll (\log n)^3,$$

which shows that n can take only finitely many values.

This completes the proof of Theorem 1.

4 Proof of Theorem 2

Before proceeding to the proof of Theorem 2, we gather a few useful facts about the Fibonacci sequence.

We first recall the following special case of the *Primitive Divisor Theorem*, which is due to Carmichael [5]:

Lemma 7. *For all $n \geq 13$, there exists a prime factor p of F_n such that p does not divide F_m for any positive integer $m < n$. Furthermore, any such prime p satisfies $p \equiv \pm 1 \pmod{n}$.*

Next, we record the following estimate for the function $\ell(n) = \ell_{10}(F_n)$, which gives the number of digits in the decimal expansion of F_n :

Lemma 8. *For all $n \geq 1$, we have*

$$\frac{(n-2)\log \alpha}{\log 10} < \ell(n) \leq \frac{(n-1)\log \alpha}{\log 10} + 1.$$

Proof. By induction on k , it is easy to see that $\alpha^{k-2} \leq F_k \leq \alpha^{k-1}$ holds for all $k \geq 1$. Since $\ell(k)$ is the unique integer for which $10^{\ell(k)-1} \leq F_k < 10^{\ell(k)}$, the result follows. \square

We keep the notation used in the proof of Theorem 1. In particular, $\mathbb{L} = \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_{\mathbb{L}} = \mathbb{Z}[\alpha]$, and $D = 2$ is the degree of \mathbb{L} over \mathbb{Q} . Notice that $\mathcal{O}_{\mathbb{L}}$ is a UFD. We also put $\varpi = \sqrt{5}$ and $\mathcal{P} = [\varpi]$; then $[p] = [5] = \mathcal{P}^2$, and $f = 1$. We need the following elementary lemma:

Lemma 9. *If $r \geq 2$, we have*

$$\text{ord}_{\mathcal{P}}(\alpha^r - 1) \leq \frac{2\log(r/4)}{\log 5} + 1.$$

The same inequality holds with α replaced by β .

Proof. The inequality for β follows from the one for α by conjugation. Note that the right hand side of the stated inequality is positive for all $r \geq 2$. Since

$$\alpha = \frac{1 + \sqrt{5}}{2} \equiv 2^{-1} \pmod{\varpi},$$

it follows that $\text{ord}_{\mathcal{P}}(\alpha^r - 1) = 0$ if $4 \nmid r$; hence, it suffices to assume that $4 \mid r$ in what follows. Since

$$\alpha^4 - 1 = \frac{5 + 3\sqrt{5}}{2},$$

it follows that $\text{ord}_{\mathcal{P}}(\alpha^4 - 1) = 1$. Thus, we may write $\alpha^4 = 1 + \varpi u$, where u is coprime to ϖ . If $s \geq 1$ is an integer and $5 \nmid s$, then

$$\alpha^{4s} - 1 = (\alpha^4 - 1) \sum_{j=0}^{s-1} \alpha^{4j} = \varpi u \sum_{j=0}^{s-1} (1 + \varpi u)^j \equiv \varpi u s \pmod{\varpi},$$

which shows that $\text{ord}_{\mathcal{P}}(\alpha^{4s} - 1) = 1$ as well. One checks similarly that if $s \geq 1$ and $5 \nmid s$, then $\text{ord}_{\mathcal{P}}(\alpha^{20s} - 1) = 3$.

We now claim that, for all $t \geq 0$ and $s \geq 1$ such that $5 \nmid s$, we have

$$\text{ord}_{\mathcal{P}}(\alpha^{4s \cdot 5^t} - 1) = 2t + 1. \tag{28}$$

To prove this, we use induction on the parameter t . Since the claim is true for $t = 0$ or 1 , let us suppose that $t \geq 2$. Then,

$$\begin{aligned}\alpha^{4s \cdot 5^t} - 1 &= (\alpha^{4s \cdot 5^{t-1}} - 1) \sum_{j=0}^4 \alpha^{4sj \cdot 5^{t-1}} \\ &= 5(\alpha^{4s \cdot 5^{t-1}} - 1) + (\alpha^{4s \cdot 5^{t-1}} - 1) \sum_{j=1}^4 (\alpha^{4sj \cdot 5^{t-1}} - 1).\end{aligned}$$

By the induction hypothesis, we have

$$\text{ord}_{\mathcal{P}} \left(5(\alpha^{4s \cdot 5^{t-1}} - 1) \right) = 2 + (2(t-1) + 1) = 2t + 1,$$

while

$$\text{ord}_{\mathcal{P}} \left((\alpha^{4s \cdot 5^{t-1}} - 1) \sum_{j=1}^4 (\alpha^{4sj \cdot 5^{t-1}} - 1) \right) \geq 2(2(t-1) + 1) = 4t - 2 > 2t + 1,$$

and (28) follows.

Finally, writing r in the form $r = 4s \cdot 5^t$, where $t \geq 0$, $s \geq 1$, and $5 \nmid s$, we have

$$\text{ord}_{\mathcal{P}}(\alpha^r - 1) = 2t + 1 = \frac{2 \log(r/4s)}{\log 5} + 1 \leq \frac{2 \log(r/4)}{\log 5} + 1,$$

which finishes the proof. \square

Lemma 10. *If (m, n, k) is an ordered triple of positive integers such that $\overline{F_m F_n} = F_k$, and $(m, n, k) \neq (1, 4, 7)$ or $(2, 4, 7)$, then $m \geq 3$ and $k - n \geq 4$.*

Proof. Suppose that $n \geq 13$. First, suppose that $m = 1$ or $m = 2$. Then $10^{\ell(n)} + F_n = F_k$; hence, $2F_n \leq F_k \leq 11F_n$, which (by simple estimates) implies that $n + 2 \leq k \leq n + 5$. Since $n \geq 13$, we have that $\ell(n) \geq 3$, and thus,

$$F_n \equiv F_k \pmod{8}.$$

An analysis of the sequence of Fibonacci numbers modulo 8 shows that this congruence is not possible when $k = n + 4$ or $k = n + 5$; therefore, $k = n + 2$ or $k = n + 3$. If $k = n + 2$, then $10^{\ell(n)} = F_{n+1}$, while for $k = n + 3$, we have $10^{\ell(n)} = 2F_{n+1}$. However, by Lemma 7, there exists a prime $p \geq n$ dividing F_{n+1} , which is not possible in our cases. Consequently, if $m \leq 2$, we must have $n \leq 12$. Checking the remaining possibilities, the only solutions found are $(1, 4, 7)$ and $(2, 4, 7)$.

Assuming now that $\overline{F_m F_n} = F_k$, $n \geq 15$, and $k \leq n + 3$, we then have

$$F_m \cdot 10^{\ell(n)} = F_k - F_n = \begin{cases} F_{n-1}, & \text{if } k = n + 1; \\ F_{n+1}, & \text{if } k = n + 2; \\ 2F_{n+1}, & \text{if } k = n + 3. \end{cases} \quad (29)$$

Moreover, $m < n - 1$, for otherwise

$$F_k = F_m \cdot 10^{\ell(n)} + F_n > 1000F_{n-1} > F_{n+3},$$

contradicting our assumption that $k \leq n + 3$. Using Lemma 7 again, we see that there exist primes $p \mid F_{n-1}$ and $q \mid F_{n+1}$ with $\gcd(pq, F_m) = 1$ and $\min\{p, q\} \geq 13$, which is not possible in view of (29). Hence, if $k \leq n + 3$, we must have $n \leq 14$, and thus $k \leq 17$. Examining these possibilities reveals no solutions other than the two found in the previous case. \square

Lemma 11. *If $r \geq 1$ is even, then*

$$\frac{\alpha^r - 1}{\beta^r - 1} = -\alpha^r,$$

while if $r \geq 5$ is odd, then the numbers $(\alpha^r - 1)/(\beta^r - 1)$ and α are multiplicatively independent.

Proof. The first statement is trivial since $\alpha\beta = -1$. For the second statement, we note that if r is odd then

$$\frac{\alpha^r - 1}{\beta^r - 1} = -\alpha^r \left(\frac{\alpha^r - 1}{\alpha^r + 1} \right).$$

We now observe that if \mathcal{D} is the common divisor in $\mathcal{O}_{\mathbb{L}}$ of $\alpha^r - 1$ and $\alpha^r + 1$, then $\mathcal{D} \mid 2$. Since 2 is inert in $\mathcal{O}_{\mathbb{L}}$, it follows that $\mathcal{D} \in \{1, 2\}$. The above arguments show that if $(\alpha^r - 1)/(\beta^r - 1)$ and α are multiplicatively dependent, then so are $(\alpha^r - 1)/(\alpha^r + 1)$ and α . Using the fact that $\mathcal{O}_{\mathbb{L}}$ is a UFD and the computation of \mathcal{D} , it follows that $\alpha^r - 1$ is either a unit, or it is an associate of 2. Hence, we get an equation of the form

$$\alpha^r - 1 = \pm 2^\lambda \alpha^t$$

with integers $\lambda \in \{0, 1\}$ and t . Since $r > 3$, it follows that $\alpha^r - 1 > \alpha^3 - 1 > 2$; hence, the sign in this equation is positive, and $t \geq 1$. Clearly, $t < r$. Thus, $\alpha^r - 1 = 2^\lambda \alpha^t$. By conjugation, we also have $\beta^r - 1 = 2^\lambda \beta^t$. Subtracting these two equations and dividing the result by $\alpha - \beta$, we obtain that $F_r = 2^\lambda F_t$. If $r \geq 13$, this equation is impossible in view of Lemma 7. The fact that $F_r = 2^\lambda F_t$ is also impossible for $5 \leq r \leq 13$ can be checked by hand, and the result follows. \square

We are now ready to embark on the proof of Theorem 2. For this, let (m, n, k) be a fixed triple of nonnegative integers for which $\overline{F_m F_n} = F_k$ holds. We note that $n > 0$, since for $n = 0$ we have $10F_m = F_k$, which has no positive integer solutions (m, k) (by Lemma 7, for example). Put $r = k - n$, and assume that $k > 10^6$. By Lemma 10, we can further suppose that $m \geq 3$ and $r \geq 4$. Since $\beta = -1/\alpha$, we have

$$\begin{aligned} F_m \cdot 10^{\ell(n)} = F_k - F_n &= \varpi^{-1}(\alpha^k - \beta^k - \alpha^n + \beta^n) \\ &= \varpi^{-1}(\alpha^n(\alpha^r - 1) - \beta^n(\beta^r - 1)) \\ &= \varpi^{-1}\alpha^n(\beta^r - 1) \left(\left(\frac{\alpha^r - 1}{\beta^r - 1} \right) - (-\alpha^{-2})^n \right). \end{aligned}$$

Consequently,

$$\text{ord}_{\mathcal{P}}(F_m) + 2\ell(n) = -1 + \text{ord}_{\mathcal{P}}(\beta^r - 1) + \text{ord}_{\mathcal{P}}\left(\left(\frac{\alpha^r - 1}{\beta^r - 1}\right) - (-\alpha^{-2})^n\right). \quad (30)$$

Assume first that r is odd. We shall apply Theorem 6 with the choices $\alpha_1 = (\alpha^r - 1)/(\beta^r - 1)$, $\alpha_2 = -\alpha^{-2}$, $b_1 = 1$, and $b_2 = n$. The condition that α_1 and α_2 are multiplicatively independent is satisfied by Lemma 11 because $r \geq 5$. Furthermore, note that

$$h(\alpha_1) \leq \frac{1}{2} (\log |(\alpha^r - 1)(\beta^r - 1)| + \log |\alpha_1|) \leq \frac{1}{2} \log \alpha^{2r} = r \log \alpha,$$

and $h(\alpha_2) = \log \alpha$. Since $r \geq 5$, we can choose $A_1 = \alpha^r$ and $A_2 = \varpi$; hence,

$$b' = \frac{1}{\log 5} + \frac{n}{2r \log \alpha} \leq \frac{1}{2 \log \alpha} + \frac{n}{10 \log \alpha} \leq \frac{3n}{4 \log \alpha}.$$

Finally, as $\alpha \equiv \beta \pmod{\varpi}$, and $\text{ord}_{\mathcal{P}}(\alpha^r - 1) = \text{ord}_{\mathcal{P}}(\beta^r - 1) = 0$ (by Lemma 9), it follows that \mathcal{P} divides $\alpha_1 - 1$. Moreover, noting that $-\alpha^{-2} \equiv 1 \pmod{\varpi}$, it follows that \mathcal{P} also divides $\alpha_2 - 1$. Thus, we can take $g = 1$. By Theorem 6, we obtain the bound

$$\begin{aligned} \text{ord}_{\mathcal{P}}\left(\left(\frac{\alpha^r - 1}{\beta^r - 1}\right) - (-\alpha^{-2})^n\right) &\leq \frac{480r \log \alpha}{(\log 5)^3} \left(\max\left\{\log n + \log\left(\frac{3 \log 5}{4 \log \alpha}\right) + 0.4, 10\right\}\right)^2 \\ &\leq 56r (\max\{\log n + 2, 10\})^2. \end{aligned}$$

Next, consider the case that r is even; then

$$\frac{\alpha^r - 1}{\beta^r - 1} - (\alpha^{-2})^n = -\alpha^r - (-\alpha^2)^n = (-1)^{n+1} \alpha^{-2n} (\alpha^{k+n} \pm 1),$$

and the last expression divides $\alpha^{2k+2n} - 1$ in $\mathcal{O}_{\mathbb{L}}$; hence, by Lemma 9, we obtain that

$$\text{ord}_{\mathcal{P}}\left(\left(\frac{\alpha^r - 1}{\beta^r - 1}\right) - (-\alpha^{-2})^n\right) \leq \frac{2 \log((k+n)/2)}{\log 5} + 1.$$

Substituting the estimates above into (30), and applying Lemmas 8 and 9, we derive that

$$2 \frac{(n-2) \log \alpha}{\log 10} < \ell(n) \leq \frac{2 \log(r/4)}{\log 5} + 56r (\max\{\log n + 2, 10\})^2, \quad (31)$$

if r is odd, and

$$2 \frac{(n-2) \log \alpha}{\log 10} < \ell(n) \leq \frac{2 \log(r/4)}{\log 5} + \frac{2 \log((k+n)/2)}{\log 5} + 1, \quad (32)$$

if r is even.

From the equality $\overline{F_m F_n} = F_k$, we also see that

$$\alpha^m \cdot 10^{\ell(n)} - \alpha^k = \beta^m \cdot 10^{\ell(n)} - \alpha^n + \beta^n - \beta^k, \quad (33)$$

and, since $10^{\ell(n)} < 10F_n$ and $m \geq 3$, we have

$$\begin{aligned} |\alpha^{m-k} \cdot 10^{\ell(n)} - 1| &= \alpha^{-k} |\beta^m \cdot 10^{\ell(n)} - \alpha^n + \beta^n - \beta^k| \\ &\leq \alpha^{-k} (10|\beta|^3 F_n + \alpha^n + 2) < 4\alpha^{-r}. \end{aligned} \quad (34)$$

Since $m \geq 3$, both sides of (33) are *negative*, and since $r \geq 4$, we have $4\alpha^{-r} < \frac{3}{5}$; thus,

$$\frac{2}{5} < \alpha^{m-k} \cdot 10^{\ell(n)} < 1.$$

It follows that

$$|\alpha^{m-k} \cdot 10^{\ell(n)} - 1| > \frac{2}{5} |(k-m) \log \alpha - \ell(n) \log 10|. \quad (35)$$

We now apply Theorem 5 with the choices $\Lambda = (k-m) \log \alpha - \ell(n) \log 10$, $\alpha_1 = 10$, $\alpha_2 = \alpha$, $b_1 = \ell(n)$, and $b_2 = k-m$. Here, $h(\alpha_1) = \log 10$ and $h(\alpha_2) = \frac{1}{2} \log \alpha$; hence, we can choose $A_1 = 10$, and $A_2 = \alpha^2$, and

$$b' = \frac{\ell(n)}{4 \log \alpha} + \frac{k-m}{20} < b'' = \frac{\ell(n)}{4 \log \alpha} + \frac{k}{20}.$$

Using Theorem 5, we get that

$$|(k-m) \log \alpha - \ell(n) \log 10| \geq \exp \left(-864 (\max\{\log b'' + 0.14, 10.5\})^2 \right).$$

Combining the above estimates, we derive the bound

$$r < \frac{\log 10}{\log \alpha} + \frac{864}{\log \alpha} (\max\{\log b'' + 0.14, 10.5\})^2. \quad (36)$$

Now, if $k > 2n$, then, by Lemma 8, we have

$$b'' = \frac{\ell(n)}{4 \log \alpha} + \frac{k}{20} \leq \frac{n-1}{4 \log 10} + \frac{1}{4 \log \alpha} + \frac{k}{20} < \frac{(k/2) - 1}{4 \log 10} + \frac{1}{4 \log \alpha} + \frac{k}{20},$$

and $r = k - n > k/2$; hence, the inequality (36) is not possible for $k > 500000$. On the other hand, if $k \leq 2n$, then

$$b'' = \frac{\ell(n)}{4 \log \alpha} + \frac{k}{20} \leq \frac{n-1}{4 \log 10} + \frac{1}{4 \log \alpha} + \frac{n}{10}.$$

When r is even, estimate (32) gives

$$\frac{(n-2) \log \alpha}{\log 10} < \frac{\log(n/4)}{\log 5} + \frac{\log(3n/2)}{\log 5} + \frac{1}{2},$$

which implies that $n < 20$; hence, $k < 40$. When r is odd, by combining the inequalities (31), and (36), we obtain a contradiction unless $n \leq 1.1 \times 10^{11}$ and $k \leq 2n \leq 2.2 \times 10^{11}$.

Although the preceding argument shows that there are only finitely many solutions (m, n, k) to the equation $\overline{F_m F_n} = F_k$, it would be computationally infeasible to search for

solutions over the entire range $k \leq 2.2 \times 10^{11}$. In order to reduce the range further, we use a standard technique involving the continued fraction expansion of $(\log 10)/(\log \alpha)$.

Suppose that $n \leq 1.1 \times 10^{11}$ and $r \geq 56$. By (34) and (35), we have

$$\left| \frac{\log 10}{\log \alpha} - \frac{(k-m)}{\ell(n)} \right| < \frac{10}{\alpha^r \ell(n)} \leq \frac{1}{2\ell(n)^2}.$$

Here, the last inequality is equivalent to $20\ell(n) \leq \alpha^r$, which holds (by Lemma 8) for this choice of parameters. By well known properties of continued fractions, it follows that $(k-m)/\ell(n)$ is a convergent of $(\log 10)/(\log \alpha)$. Writing $(k-m)/\ell(n) = p_j/q_j$ for some $j \geq 0$, where p_j/q_j denotes the j th convergent to $(\log 10)/(\log \alpha)$, and using Lemma 8 again to bound $\ell(n)$ for n in our range, we see that $q_j \leq \ell(n) \leq 2.3 \times 10^{10}$, which implies that $j \leq 23$. Noting that

$$10\alpha^{-r} > |\ell(n) \log 10 - (k-m) \log \alpha| \geq \min_{1 \leq j \leq 23} |q_j \log 10 - p_j \log \alpha| > 1.6 \times 10^{-11},$$

we conclude that $r \leq 57$. Substituting this estimate into (31), we derive the more tractable upper bound $n \leq 2.1 \times 10^6$.

At this point, we turn to the computer. Note that if $n \geq 74$, one has $\ell(n) \geq 15$; therefore, if $\overline{F_m F_n} = F_k$, it follows that $F_n \equiv F_k \pmod{10^{15}}$. However, a computer search quickly reveals that there is no solution to this congruence with $74 \leq n \leq 2.1 \times 10^6$ and $k \leq n+57$. Thus, it remains only to search for solutions (m, n, k) with $n \leq 73$ and $k \leq n+57$, and one obtains only solutions with $k = 7, 8$ or 10 ; that is $F_k \in \{13, 21, 55\}$.

This completes the proof of Theorem 2.

5 Acknowledgements

This work was done during a visit by the second author to the University of Missouri, Columbia; the hospitality and support of this institution are gratefully acknowledged. During the preparation of this paper, W. B. was supported in part by NSF grant DMS-0070628, and F. L. was supported in part by grants SEP-CONACYT 37259-E and 37260-E.

References

- [1] W. Banks, A. Conflitti and I. E. Shparlinski, Character sums over integers with restricted g -ary digits, *Illinois J. Math.* **46** (2002), 819–836.
- [2] W. Banks, D. Hart and M. Sakata, Almost all palindromes are composite, *Math. Res. Lett.* **11** (2004), 853–868.
- [3] W. Banks and I. E. Shparlinski, On the number of sparse RSA exponents, *J. Number Theory* **95** (2002), 340–350.
- [4] Y. Bugeaud and M. Laurent, Minoration effective de la distance p -adique entre puissances de nombres algébriques, *J. Number Theory* **61** (1996), 311–342.

- [5] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n 1 \beta^n$, *Ann. of Math. (2)* **15** (1913/14), 30–70.
- [6] P. Erdős, C. Mauduit and A. Sárközy, On arithmetic properties of integers with missing digits, I, *J. Number Theory* **70** (1998), 99–120.
- [7] P. Erdős, C. Mauduit and A. Sárközy, On arithmetic properties of integers with missing digits, II, *Discrete Math.* **200** (1999), 149–164.
- [8] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, Linear equations with variables which lie in a multiplicative group, *Ann. of Math. (2)* **155** (2002), 807–836.
- [9] M. Filaseta and S. V. Konyagin, Squarefree values of polynomials all of whose coefficients are 0 and 1, *Acta Arith.* **74** (1996), 191–205.
- [10] E. Fouvry and C. Mauduit, Méthodes des crible et fonctions sommes des chiffres, *Acta Arith.* **77** (1996), 339–351.
- [11] E. Fouvry and C. Mauduit, Sommes des chiffres et nombres presque premiers, *Math. Ann.* **305** (1996), 571–599.
- [12] J. B. Friedlander and I. E. Shparlinski, On the distribution of Diffie–Hellman triples with sparse exponents, *SIAM J. Discrete Math.* **14** (2001), 162–169.
- [13] A. O. Gel’fond, Sur les nombres qui ont des propriétés additives et multiplicatives données, *Acta Arith.* **13** (1968), 259–265.
- [14] S. V. Konyagin, Arithmetic properties of integers with missing digits: distribution in residue classes, *Period. Math. Hungar.* **42** (2001), 145–162.
- [15] S. V. Konyagin, C. Mauduit and A. Sárközy, On the number of prime factors of integers characterized by digit properties, *Period. Math. Hungar.* **40** (2000), 37–52.
- [16] F. Luca, Distinct digits in base b expansions of linear recurrence sequences, *Quaest. Math.* **23** (2000), 389–404.
- [17] F. Luca, Arithmetic properties of positive integers with fixed digit sum, to appear in *Rev. Mat. Iberoamericana*.
- [18] C. Mauduit and A. Sárközy, On the arithmetic structure of sets characterized by sum of digits properties, *J. Number Theory* **61** (1996), 25–38.
- [19] C. Mauduit and A. Sárközy, On the arithmetic structure of the integers whose sum of digits is fixed, *Acta Arith.* **81** (1997), 145–173.
- [20] M. Laurent, M. Mignotte and Y. Nesterenko, Formes linéaires en deux logarithmes et déterminants d’interpolation, *J. Number Theory* **55** (1995), 285–321.
- [21] H. P. Schlickewei, S -unit equations over number fields, *Invent. Math.* **102** (1990), 95–107.

- [22] W. M. Schmidt, *Diophantine Approximations*, Springer Verlag, LNM **785** (1980).
- [23] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Springer Verlag, LNM **1467** (1991).
- [24] H. G. Senge and E. G. Straus, PV-numbers and sets of multiplicity, in *Proceedings of the Washington State Conference in Number Theory (Washington State Univ., Pullman, Wash., 1971)*, 55–67, Dept. Math. Washington State Univ., Pullman, Washington, 1971.
- [25] H. G. Senge and E. G. Straus, PV-numbers and sets of multiplicity, in “Collection of articles dedicated to the memory of Alfréd Rényi, II”, *Period. Math. Hungar.* **3** (1973), 93–100.
- [26] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge Univ. Press, 1986.
- [27] I. E. Shparlinski, Prime divisors of sparse integers, *Period. Math. Hungar.* **46** (2003), 215–222.
- [28] C. L. Stewart, On the representation of an integer in two different bases, *J. Reine Angew. Math.* **319** (1980), 63–72.