On the Furstenberg closure of a class of binary recurrences

Kevin A. Broughan
Department of Mathematics
University of Waikato
Private Bag 3105, Hamilton, New Zealand
kab@waikato.ac.nz

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

23rd January 2009

Abstract

In this paper, we determine the closure in the full topology over $\mathbb{Z}$ of the set $\{u_n : n \geq 0\}$, where $(u_n)_{n\geq 0}$ is a nondegenerate binary recurrent sequence with integer coefficients whose characteristic roots are quadratic units. This generalizes the result for the case when $u_n = F_n$ was the nth Fibonacci number.

Keywords: Full topology, Binary recurrence sequences, Primitive divisors

AMS Subject Classification: 1B39, 11B50

1 Introduction

Let $\mathbb{Z}$ be the ring of integers equipped with the topology τ in which the base of neighborhoods for a point $a \in \mathbb{Z}$ is given by the sets

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\} \qquad \text{for } b \in \mathbb{Z},\ b \geq 1. \tag{1}$$

This topology was proposed by H. Fürstenberg in [7]. It can be used to give a very elegant proof of the fact that the set of prime numbers is infinite (see [1]). It is called the *full topology*. This topology was studied in detail in the recent paper [3], where the following conjecture was proposed.

Let $F = \{F_n\}_{n \geq 0}$ denote the Fibonacci sequence given by $F_0 = 0$, $F_1 = 1$ and

$$F_{n+2} = F_{n+1} + F_n \qquad \text{for all } n \geq 0. \tag{2}$$

Let F^- denote the set $\{(-1)^{n+1} F_n : n \in \mathbb{N}\}$. Then the closure of $F \subset \mathbb{Z}$ in the topology τ is $F \cup F^-$. Some numerical evidence supporting the above conjecture was given in the last section of [3]. The above conjecture was confirmed in [8].

In this paper, we revisit the arguments from [8] and prove a more general version of the above result. Namely, let $(u_n)_{n \geq 0}$ be any sequence of integers satisfying the recurrence

$$u_{n+2} = r u_{n+1} + s u_n \qquad \text{for all } n \geq 0. \tag{3}$$

Here, r and s are some fixed integers. We assume that $rs(r^2 + 4s) \neq 0$. It is then well-known that if one writes α and β for the two roots of the *characteristic equation* $x^2 - rx - s = 0$, then there exist constants γ and δ in $\mathbb{K} = \mathbb{Q}(\alpha)$ such that

$$u_n = \gamma \alpha^n + \delta \beta^n \qquad \text{for all } n \geq 0. \tag{4}$$

We assume further that $\gamma\delta \neq 0$ and that α/β is not a root of unity. Under these conditions, it is said that the sequence $(u_n)_{n \geq 0}$ is *nondegenerate*.

Here, we only consider the case when $s = \pm 1$. In this case, one checks easily that $\mathbb{K}$ is a real quadratic field in which α and β are units. We may also define u_n for $n < 0$, either recursively via formula (3), or simply by allowing n to be negative in formula (4). We have the following result.

Theorem 1. *The closure of the set $\{u_n : n \geq 0\}$ in the full topology is the set $\{u_n : n \in \mathbb{Z}\}$.*

The above result applies to the Fibonacci sequence $(F_n)_{n\geq 0}$ which satisfies the recurrence relation (3) with $s = 1$. Since $(-1)^{n+1}F_n = F_{-n}$, the main result of [8] is an immediate consequence of our Theorem 1.

2 Some Conventions

We first make some reductions. Put

$$v_n = u_{2n} = \gamma\alpha^{2n} + \delta\beta^{2n} \qquad \text{and} \qquad w_n = u_{2n+1} = (\gamma\alpha)\alpha^{2n} + (\delta\beta)\beta^{2n}$$

for all $n = 0, 1, \ldots$. Both $(v_n)_{n\geq 0}$ and $(w_n)_{n\geq 0}$ are binary recurrent sequences, with the same characteristic equation having roots α^2 and β^2, and the closure $\overline{\mathcal{U}}$ of $\mathcal{U} = \{u_n : n \geq 0\}$ is the union of the closures of $\mathcal{V} = \{v_n : n \geq 0\}$ and $\mathcal{W} = \{w_n : n \geq 0\}$.

This argument shows that it suffices to prove Theorem 1 for the two sequences $(v_n)_{n\geq 0}$ and $(w_n)_{n\geq 0}$. In particular, it suffices to prove Theorem 1 when α and β are both positive. Thus, $r > 0$ and $s = -1$. Furthermore, we use α for the root which is > 1. We put $\Delta = r^2 + 4s = r^2 - 4 = dt^2$, where d is squarefree. Then

$$\alpha = \frac{r + \sqrt{\Delta}}{2} \qquad \text{and} \qquad \beta = \frac{r - \sqrt{\Delta}}{2}.$$

Since the multiplication by any nonzero integer is a continuous map, we may assume that $\gamma > 0$ for if not, we may then replace the sequence $(u_n)_{n\geq 0}$ by the sequence $(-u_n)_{n\geq 0}$, which has as effect replacing the pair (γ, δ) by $(-\gamma, -\delta)$. Observe that with these conditions we have $u_n > 0$ for all n sufficiently large, say $n > n_0$.

We write $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ for the real quadratic field containing α and β. We also put α_1 for the fundamental unit in $\mathbb{K}$ and β_1 for its conjugate. Since $\alpha > 1$, it follows that there exists a positive integer k such that $\alpha = \alpha_1^k$. Clearly, $\beta = \beta_1^k$. Observe that k is even if the norm of α_1; i.e., the number

$\alpha_1\beta_1$, equals -1. We write $N_{\mathbb{K}/\mathbb{Q}}$ for the norm of an element, or norm of an integer or fractional ideal, of $\mathbb{K}$ relative to $\mathbb{Q}$.

Throughout, for three algebraic integers μ_1, μ_2 and $\nu \neq 0$ we say that $\mu_1 \equiv \mu_2 \pmod{\nu}$ if $(\mu_1 - \mu_2)/\nu$ is an algebraic integer.

We use the Landau symbol O and the Vinogradov symbols $\gg$ and $\ll$ with their usual meanings. We shall also use $c_1, c_2, \ldots$ for positive computable constants depending on the sequence $(u_n)_{n\geq 0}$.

3 The Proof of Theorem 1

We first prove that $\{u_n : n \in \mathbb{Z}\} \subseteq \overline{\mathcal{U}}$. Indeed, since $s = \pm 1$, it is known that for every positive integer m the sequence $(u_n)_{n\geq 0}$ is periodic modulo m with some period $T(m)$. In fact, since α and β are units, it follows that they remain units in the finite ring $\mathbb{Z}[\alpha]/(\Delta m\mathbb{Z}[\alpha])$. Thus, there exists a positive integer $T(m)$ such that both relations $\alpha^{T(m)} \equiv 1 \pmod{\Delta m}$ and $\beta^{T(m)} \equiv 1 \pmod{\Delta m}$ hold. Observe now that since

$$u_0 = \gamma + \delta \qquad \text{and} \qquad u_1 = \gamma\alpha + \delta\beta,$$

it follows that

$$\gamma = \frac{u_1 - \beta u_0}{\alpha - \beta} \qquad \text{and} \qquad \delta = \frac{\alpha u_0 - u_1}{\alpha - \beta}.$$

In particular, both numbers $(\alpha - \beta)\gamma$ and $(\alpha - \beta)\delta$ are algebraic integers. Now note that

$$\begin{aligned} (\alpha - \beta)u_{n+T(m)} &= ((\alpha-\beta)\gamma)\alpha^{n+T(m)} + ((\alpha-\beta)\delta)\beta^{n+T(m)} \\ &\equiv ((\alpha-\beta)\gamma)\alpha^{n} + ((\alpha-\beta)\delta)\beta^{n} \pmod{\Delta m} \\ &\equiv (\alpha-\beta)u_n \pmod{\Delta m}, \end{aligned}$$

therefore $(\alpha - \beta)\left(u_{n+T(m)} - u_n\right) \equiv 0 \pmod{\Delta m}$. Since $\Delta = (\alpha - \beta)^2$, it follows that $(u_{n+T(m)} - u_n)/m$ is an algebraic integer. Since it is also a rational number, it follows that it is an integer. The above argument was valid for all integers n. Thus, given any integer n and any modulus m, we may let T be a sufficiently large positive integer such that $n + T(m)T$ is positive. Then $u_n \equiv u_{n+T(m)T} \pmod{m}$. Since m was arbitrary, we conclude that $\{u_n : n \in \mathbb{Z}\} \subseteq \overline{\mathcal{U}}$, which is what we wanted to prove.

We next demonstrate the reverse containment.

We let $\mathcal{U} = \{u_n : n \geq 0\}$ and let $a \in \overline{\mathcal{U}}$. We want to show that $a = u_n$ for some $n \in \mathbb{Z}$. We start with the case $a = 0$.

The case $a = 0$.

In this case, since $0 \in \overline{\mathcal{U}}$, it follows that the equation $u_n \equiv 0 \pmod{p}$ has a solution n for each large prime p. Writing

$$u_n = \gamma\beta^n \left(\alpha^{2n} + \frac{\delta}{\gamma}\right),$$

it follows that if p is sufficiently large, say if p is large enough so that it it is coprime with the prime ideals of $\mathbb{K}$ appearing in the factorization of either γ or δ, then the congruence

$$-\frac{\delta}{\gamma} \equiv \alpha^{2n} \pmod{p}$$

has an integer solution n. It follows from the lemma [9, Page 108], that δ/γ is a unit in $\mathbb{K}$. In particular, $\delta/\gamma = \pm\alpha_1^s$ for some integer s. Thus,

$$u_n = \gamma\alpha_1^{-kn+s}\left(\alpha_1^{2kn-s} \pm 1\right). \tag{5}$$

We next show that s is a multiple of k and that the sign is -1. Consider the sequence with the general term

$$V_n = \alpha_1^n - 1 \in \mathcal{O}_{\mathbb{K}} \qquad \text{for } n = 1, 2, \ldots$$

We say a prime ideal $\mathcal{P}$ of $\mathcal{O}_{\mathbb{K}}$ is *primitive* for V_n if it has the property that $\mathcal{P} \mid V_n$ but $\mathcal{P}$ does not divide V_m for any $1 \leq m < n$. It follows from results of Schinzel [10] and Stewart [11, Theorem 1] that V_n always has primitive divisor $\mathcal{P}$ if n exceeds some absolute constant.

If $\mathcal{P}$ is such a primitive divisor and p is the prime number such that $\mathcal{P} \mid p$, then $p \gg n^{1/2}$: to see this since $\mathbb{K}$ is quadratic, $N(\mathcal{P}) = p$ or $N(\mathcal{P}) = p^2$

where p is the unique rational prime with $\mathcal{P} \mid p$. Therefore the order of the multiplicative group of $\mathcal{O}_{\mathbb{K}}/\mathcal{P}$ is $p-1$ or p^2-1 and $\alpha_1^{N(P)-1} \equiv 1 \bmod \mathcal{P}$ shows that $n \mid p$ or $n \mid p^2-1$, from which the inequality follows [10].

Armed with these facts, let us go back to relation (5). Assume that s is not a multiple of k. Let m be large, let $\mathcal{P}$ be a primitive prime for V_{2km}, and let p be the prime number such that $\mathcal{P} \mid p$. For large enough m, p is coprime with the prime ideals appearing in the factorization of either γ or δ in $\mathbb{K}$. There exists n such that $u_n \equiv 0 \pmod{p}$. We may assume that $n > s/(2k)$, for otherwise we may replace n by the sum of n and some large multiple of $T(p)$. This implies that $\mathcal{P} \mid \alpha_1^{2kn-s} \pm 1 \mid V_{4kn-2s}$. Since also $\mathcal{P} \mid V_{2km}$, we obtain $\mathcal{P} \mid V_{\gcd(4kn-2s,2km)}$. To see this, we used the fact that if m and n are two positive integers with $d = \gcd(m,n)$, then $\gcd(V_m, V_n) = V_d$, which follows from the fact that there exist two polynomials $P(X)$ and $Q(X)$ with integer coefficients such that

$$P(X)(X^m-1) + Q(X)(X^n-1) = X^d - 1$$

(see, for example, the proof of Lemma 1 in [4]). In particular, if α is an algebraic integer and $\mathcal{I}$ is an ideal such that $\mathcal{I}$ divides both V_m and V_n, then $\mathcal{I}$ divides V_d.

Since s is not a multiple of k, it follows that the integer $\gcd(4kn-2s, 2km)$ is a proper divisor of $2km$, which contradicts the choice of $\mathcal{P}$ as a primitive prime ideal divisor of $\alpha_1^{2km}-1$. Thus, $s = ks_1$.

We next show that the sign is -1. Assume that it were $+1$. Then

$$u_n = \gamma\alpha_1^{-k(n+s_1)}\left(\alpha_1^{(2n-s_1)k}+1\right).$$

We now take a large prime q, put $m = kq$, and consider a primitive prime ideal $\mathcal{P}$ of V_{kq}. Let p be the prime such that $\mathcal{P} \mid p$, and let n be such that $u_n \equiv 0 \pmod{p}$. Again, we assume that $n > s/(2k) = s_1/2$. Since p is large, it follows that $\alpha_1^{(2n-s_1)k} \equiv -1 \pmod{\mathcal{P}}$. But we also have that $\alpha_1^{kq} \equiv 1 \pmod{\mathcal{P}}$. If $2n - s_1$ is a multiple of q, we then get that $-1 \equiv \alpha_1^{(2n-s_1)k} \pmod{\mathcal{P}} \equiv 1 \pmod{\mathcal{P}}$, so $\mathcal{P} \mid 2$, giving $p = 2$, which is false since we have assumed that p is large. So assuming q does not divide $(2n-s_1)$, we then have $\mathcal{P} \mid \alpha_1^{(2n-s_1)k}+1 \mid V_{(4n-2s_1)k}$ and $\mathcal{P} \mid V_{kq}$, therefore $\mathcal{P} \mid V_{\gcd((4n-2s_1)k,kq)} \mid V_k$, where we used the fact that $q > 2$ and q does not divide $2n - s_1$. This contradicts the definition of $\mathcal{P}$ as a primitive divisor of V_{kq}. Hence, the sign is -1.

We have arrived at the conclusion that

$$u_n = \gamma\beta^n\alpha_1^s\left(\alpha_1^{(2n-s_1)k} - 1\right).$$

Finally, we show that s_1 is even. We use a similar method to that used above. If s_1 were odd, let m be a large even number and choose a primitive prime factor $\mathcal{P}$ of V_{km}. With p the prime such that $\mathcal{P} \mid p$ and n such that $p \mid u_n$ and large, we get that $\mathcal{P} \mid V_{(2n-s_1)k}$. Hence, $\mathcal{P} \mid V_{\gcd((2n-s_1)k,km)} \mid V_{mk/2}$, where we used the fact that $2n - s_1$ and odd and m is even. This contradicts the choice of $\mathcal{P}$ as a primitive prime factor of V_{km}.

Thus, s_1 is even and we can write it as $s_1 = 2s_0$ for some integer s_0.

Thus,

$$u_n = \gamma\beta^n\alpha_1^s\left(\alpha_1^{2(n-s_0)k} - 1\right),$$

and taking $n = s_0 \in \mathbb{Z}$, we get that $a = 0 \in \{u_n : n \in \mathbb{Z}\}$, which is what we wanted.

The case $a \neq 0$.

This case is much more interesting and harder. Here, we put $U_n = (\alpha^n - \beta^n)/(\alpha-\beta)$ for all $n \geq 0$. The sequence $(U_n)_{n\geq 0}$ satisfies the same recurrence relation (3) as $(u_n)_{n\geq 0}$ does and its initial values are $U_0 = 0$ and $U_1 = 1$.

We proceed in ten steps.

1. First we show that the sequence $(u_n : n \geq 0)$, when taken modulo U_m, has a well determined period.

Lemma 2. *Let $m \geq 1$. The sequence $(u_n)_{n\geq 0}$ is periodic modulo U_m with period $4m$.*

Proof. Note that

$$\alpha^{4m} - 1 = \alpha^{4m} - (\alpha\beta)^{2m} = \alpha^{2m}(\alpha^{2m} - \beta^{2m}) \equiv 0 \pmod{\alpha^m - \beta^m}.$$

Thus, $\alpha^{4m} \equiv 1 \pmod{\alpha^m - \beta^m}$. Similarly, $\beta^{4m} \equiv 1 \pmod{\alpha^m - \beta^m}$. Hence,

$$\begin{aligned}
(\alpha-\beta)u_{n+4m} &= ((\alpha-\beta)\gamma)\alpha^n\alpha^{4m} + ((\alpha-\beta)\delta)\beta^n\beta^{4m} \\
&\equiv ((\alpha-\beta)\gamma)\alpha^n + ((\alpha-\beta)\delta)\beta^n \pmod{\alpha^m - \beta^m} \\
&\equiv (\alpha-\beta)u_n \pmod{\alpha^m - \beta^m}.
\end{aligned}$$

Canceling the factor of $(\alpha-\beta)$, we get that $u_{n+4m} \equiv u_n \pmod{U_m}$, which is what we wanted. $\square$

2. We next take a close look at the number $u_n - a$. Observe that

$$\begin{aligned} u_n - a &= \gamma\alpha^n + \delta\beta^n - a = \gamma\beta^n\left(\alpha^{2n} - \frac{a}{\gamma}\alpha^n + \frac{\delta}{\gamma}\right) \\ &= \gamma\beta^n(\alpha^n - z_1)(\alpha^n - z_2), \end{aligned}$$

where

$$z_{1,2} = \frac{a \pm \sqrt{\Delta_1}}{2\gamma} \qquad \text{and} \qquad \Delta_1 = a^2 - 4\gamma\delta.$$

Recall that a primitive prime factor of U_m is a rational prime dividing U_m which does not divide U_ℓ for any $1 \le \ell < m$ and which does not divide Δ either. It is known that if $m > 12$, then U_m has primitive divisors [11, Theorem 1]. In fact, putting

$$W_m = \prod_{\substack{p^{a_p} \| U_m \\ p \text{ primitive}}} p^{a_p},$$

then we have the following lemma due to Stewart [12, Page 603], but see also [2, Eqn. 17]. In the next statement we use $P(n)$ for the largest prime factor of n and $\Phi_n(X,Y)$ for the homogeneous cyclotomic polynomial of order n.

Lemma 3. *For all $n > 12$, $P(\frac{n}{\gcd(n,3)})W_n \ge \Phi_n(\alpha,\beta)$.*

Proof. Any primitive prime divisor of U_n divides $\Phi_n := \Phi_n(\alpha,\beta)$. If p is a prime divisor of Φ_n and $p \nmid n$ then p is a primitive divisor of Φ_n. The only possible prime dividing both n and Φ_n is $P(n/\gcd(n,3))$ and it divides Φ_n to the first power, so the lemma follows from the prime factorization of Φ_n. $\square$

Therefore

$$\begin{aligned} W_m &\ge \frac{1}{m} \prod_{\substack{1 \le \ell \le m \\ \gcd(\ell,m)=1}} (\alpha - \mathbf{e}^{2\pi i \ell/m}\beta) > \frac{(\alpha-\beta)^{\phi(m)}}{m} \\ &= \exp((\log(\alpha-\beta))\phi(m) - \log m), \end{aligned}$$

where $\phi(m)$ is the Euler function. Using the fact that $\phi(m) \gg m/\log\log m$, it follows that for all large m we have

$$W_m \geq \exp(c_1\phi(m)),$$

where we can take $c_1 = (\log(\alpha - \beta))/2 = (\log \Delta)/4$.

3. Next we take a large positive integer m which is a multiple of $8k$ and we shall look at the simultaneous solutions n of the congruences

$$u_n - a \equiv 0 \pmod{M},$$

with

$$M \in \{W_m, W_{m/2}W_{m/4}, W_m W_{m/2} W_{m/4}\}$$

for reasons which will become clear later. Since $M \mid U_m$, it follows, by Lemma 2, that we can take $n \in [4m, 8m)$. We have

$$\begin{aligned} e^{c_1\phi(m)} &\leq M \ll N_{\mathbb{L}/\mathbb{Q}}\left(\gcd(M, (\alpha^n - z_1)(\alpha^n - z_2)\right) \\ &\ll N_{\mathbb{L}/\mathbb{Q}}\left(\gcd(M, \alpha^n - z_1\right) N_{\mathbb{L}/\mathbb{Q}}\left(\gcd(M, \alpha^n - z_2)\right). \end{aligned}$$

In the above, the greatest common divisors are to be thought of as fractional ideals of $\mathcal{O}_{\mathbb{L}}$, where $\mathbb{L} = \mathbb{K}(z_1)$. It now follows that there exists a constant c_2, which can be taken to be $c_1/3$, such that if m is large, then for some $i \in \{1, 2\}$ we have

$$N_{\mathbb{L}/\mathbb{Q}}\left(\gcd(M, \alpha^n - z_i)\right) > \exp(c_2\phi(m)). \tag{6}$$

4. The following argument has appeared in the proof of the main result in [8]. We supply the proof of it for convenience.

Lemma 4. *With the previous notations, if z_i and α are multiplicatively independent, and $n \in [4m, 8m)$, then*

$$N_{\mathbb{L}/\mathbb{Q}}\left(\gcd(M, \alpha^n - z_i)\right) = \exp(O(\sqrt{m})). \tag{7}$$

Proof. Let

$$\mathcal{S} = \{\lambda n + 2\mu m \;:\; \lambda,\ \mu \in \{1, \ldots, \lfloor m^{1/2} \rfloor\}.$$

If $s = \lambda n + 2\mu m$, then $1 \leq s \leq (n+2m)m^{1/2} < 10m^{3/2}$. Since there are $(\lfloor m^{1/2} \rfloor)^2$ pairs of positive integers (λ, μ) with $\lambda, \mu \in \{1, \ldots, \lfloor m^{1/2} \rfloor\}$, it follows, by the *Pigeon-Hole Principle*, that there exist two distinct pairs $(\lambda_1, \mu_1) \neq (\lambda_2, \mu_2)$ such that

$$|(\lambda_1 - \lambda_2)n + 2(\mu_1 - \mu_2)m| < \frac{10m^{3/2}}{\lfloor m^{1/2} \rfloor^2 - 1} < 11m^{1/2} \qquad \text{for } m \text{ large enough.}$$

Writing $x = \lambda_1 - \lambda_2$ and $y = \mu_1 - \mu_2$, we get that $(x, y) \neq (0, 0)$, that $x,\ y \in [-m^{1/2},\ m^{1/2}]$, and that if we write $s = nx + 2my$, then $|s| < 11m^{1/2}$. Note now that $\star$ if we define the fractional ideals

$$\mathcal{I}_i = \gcd([M], [\alpha^n - z_i]),$$

where $[\theta]$ represents the principal ideal generated by θ in $\mathbb{L}$ $\star$, then since $M \mid (\alpha^m - \beta^m) \mid (\alpha^{2m} - 1)$, we have

$$\alpha^{2m} \equiv -1 \pmod{\mathcal{I}_i} \qquad \text{and} \qquad \alpha^n \equiv z_i \pmod{\mathcal{I}_i}.$$

Here, z_i is invertible modulo $\mathcal{I}_i$ for large m although z_i might not be an algebraic integer. The reason here is that M consists only of primitive prime factors of U_m, or of $U_{m/2}$, or of $U_{m/4}$, and all of them are congruent to ± 1 modulo $m/4$. In particular, if m is sufficiently large, then z_i is invertible modulo $\mathcal{I}_i$.

Raising the first congruence to the power y and the second to the power x (notice that such operations are justified even if x and y are negative since α is a unit in $\mathbb{K}$, therefore also in $\mathbb{L}$), and multiplying the resulting congruences we get

$$\alpha^s \equiv (-1)^y z_i^x \pmod{\mathcal{I}_i}.$$

Thus, $\mathcal{I}_i$ divides $(\alpha^s - (-1)^y z_i^x)$. Note that this last ideal is not zero. Indeed, for if not, then we would get that $\alpha^{2s} = z_i^{2x}$. Since we are assuming that α and z_i are multiplicatively independent, we get $x = s = 0$, and since $s = nx + 2my$, we get that $y = 0$ as well, which contradicts the fact that $(x, y) \neq (0, 0)$. Hence, $\mathcal{I}_i$ divides the nonzero ideal $(\alpha^s - (-1)^y z_i^x)$. Taking norms in $\mathbb{L}$ and observing that the degree of $\mathbb{L}$ over $\mathbb{Q}$ is at most 4, we get that

$$N_{\mathbb{L}/\mathbb{Q}}(\mathcal{I}_i) \leq (Z^{|x|}\alpha^{|s|} + \max\{|Z_i^{(j)}| : i, j\}^{|x|})^4 = \exp(O(\sqrt{m})),$$

where we put $z_i = Z_i/Z$ with some integer Z and algebraic integer Z_i and let $Z_i^{(j)}$ stand for all the conjugates of Z_i in $\mathbb{L}$ for $i = 1, 2$. This is what we wanted to prove. $\square$

5. From Lemma 4, we conclude that if both z_1 and z_2 are both multiplicatively independent with respect to α, then both

$$N_{\mathbb{L}/\mathbb{Q}}(M, \alpha^n - z_i) = \exp(O(\sqrt{m})) \qquad \text{hold for } i = 1, 2.$$

Since $\phi(m) \gg m/\log\log m$, we get a contradiction with estimate (6) for large m. Thus, there exists $i \in \{1, 2\}$ such that z_i and α are multiplicatively dependent. Let it be z_1.

6. We next show that $z_1 \in \mathbb{K}$. If $\Delta_1 = 0$, there is nothing to prove. If not, write $\Delta_1 = d_1 t_1^2$, where d_1 is a squarefree integer and t_1 is a nonzero rational. Then, since z_1 and x are multiplicatively dependent, there exist integers x and y not both zero and $\varepsilon \in \{\pm 1\}$ such that $z_1^x = \alpha^y$ i.e.

$$\left(\frac{a + \varepsilon t_1 \sqrt{d_1}}{2}\right)^x = \gamma^x \alpha^y. \tag{8}$$

By replacing x with $-x$ if needed, we may assume that $x \geq 0$. By replacing the pair (x, y) by the pair $(2x, 2y)$, we may assume that both x and y are even. The left hand side is in $\mathbb{Q}(\sqrt{d_1})$, while the right hand side is in $\mathbb{Q}(\sqrt{d})$. If $d_1 = 1$ or d, then $z_1 \in \mathbb{K}$, which is what we wanted. Assume that $d_1 \neq 1,\ d$. Then the two numbers in both sides of (8) are in $\mathbb{Q}(\sqrt{d}) \cap \mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}$. Since the right hand side is real and positive (since γ and α_1 are real and x and y are even), it follows that there exists a positive rational number q such that $\gamma^x \alpha_1^{ky} = q$. Thus, $\gamma^x = q\alpha_1^{-ky}$. Conjugating we get $\delta^x = q\beta_1^{-ky}$. Multiplying the above relations and using the fact that $(\alpha_1\beta_1)^{-ky} = 1$ (because y is even), we get $(\gamma\delta)^x = q^2$. Now $\gamma\delta = q_1$ is a rational number. Thus, $q_1^x = q^2$, and since q is positive, we get that $q = |q_1|^{x/2}$. Hence,

$$\left(\frac{a + \varepsilon t_1 \sqrt{d_1}}{2}\right)^x = q = |q_1|^{x/2},$$

leading to

$$\left(\frac{a + \varepsilon t_1 \sqrt{d_1}}{2}\right)^2 = \pm q_1.$$

We are thus lead to

$$(a^2 + d_1 t_1^2) + 2\varepsilon a t_1 \sqrt{d_1} = \pm 4q_1,$$

which is false for $at_1 \neq 0$ and $d_1 \neq 1$ and squarefree. Thus, indeed $z_1 \in \mathbb{K}$. Since $z_1 \in \mathbb{K}$ and is multiplicatively dependent with respect to α, it follows that it is an algebraic integer since from what we have seen above it is a solution $X = z_1$ of an equation of the form $X^x - \alpha_1^{ky}$ with some integers $x > 0$ and even and y, and α_1^{ky} is an algebraic integer. Thus, $z_1 \in \mathcal{O}_{\mathbb{K}}$ and some power of it is a unit, therefore itself is a unit. Thus, $z_1 = \pm\alpha_1^s$ for some integer s.

7. It remains to prove that s is a multiple of k and that the sign is $+1$. (Compare this with the case $a = 0$ where the sign was -1.) Indeed, to see that we have finished in this way, observe that if this is the case, then writing $s = ks_1$ for some integer s_1, the relation

$$\frac{a + \varepsilon t_1\sqrt{d_1}}{2} = \gamma\alpha_1^{ks_1} = \gamma\alpha^{s_1} \tag{9}$$

holds. Conjugating this relation in $\mathbb{K}$, we also get

$$\frac{a - \varepsilon t_1\sqrt{d_1}}{2} = \delta\beta^{s_1}, \tag{10}$$

and summing up relations (9) and (10) we arrive at

$$a = \gamma\alpha^{s_1} + \delta\beta^{s_1} = u_{s_1} \in \{u_n : n \in \mathbb{Z}\},$$

which is what we wanted.

8. So, let us assume first that $z_1 = \pm\alpha_1^s$, where s is not a multiple of k. Then

$$\alpha^n - z_1 = \alpha_1^s\left(\alpha_1^{kn-s} \pm 1\right) \mid (\alpha_1^{2kn-2s} - 1).$$

We now take $M = W_m$ and observe that $W_m \mid (\alpha^m - \beta^m) \mid \alpha_1^{2km} - 1$. Thus,

$$\begin{aligned}\gcd(M, \alpha^n - z_1) \quad &\mid \quad \gcd(\alpha_1^{2km} - 1, \alpha_1^{2kn-2s} - 1)\\ &= \quad \gcd(V_{2km}, V_{2kn-2s}) = V_{\gcd(2km, 2kn-2s)}.\end{aligned}$$

Since k does not divide s, it follows that $\gcd(2km, 2kn-2s)$ is a proper divisor of $2km$. Thus, there exists a prime q dividing km such that $\gcd(2km, 2kn - 2s) \mid 2km/q$, and so

$$\gcd(M, \alpha^n - z_1) \mid V_{2km/q} = \alpha_1^{2km/q} - 1 = \alpha_1^{km/q}(\alpha - \beta)U_{m/q}.$$

Here, we used the fact that m is a multiple of 4 (so, km/q is even for all prime factors q of km), as well as the fact that m is divisible by k. However, since $M = W_m$ consists of the primitive prime factors of U_m, it follows that M is coprime to $U_{m/q}$. We thus get that

$$\gcd(M, \alpha^n - z_1) = O(1),$$

contradicting (6) with $i = 1$ for large m. Thus, $s = ks_1$ holds with integer s_1.

9. Now assume that the sign is -1, i.e. $z_1 = -\alpha_1^{ks_1} = -\alpha^{s_1}$. Here we take $M = W_m W_{m/2} W_{m/4}$ and we look at the solutions n of the congruence

$$u_n - a \equiv 0 \pmod{M}.$$

The left hand side is

$$\gamma\beta^n(\alpha^n - z_1)(\alpha^n - z_2).$$

We have

$$\alpha^n - z_1 = \alpha_1^{kn} + \alpha_1^{ks_1} = \alpha_1^{ks_1}(\alpha^{n-s_1} + 1).$$

Now M divides $\alpha^m - \beta^m = \beta^m(\alpha^{2m} - 1)$. Writing $v_2(u)$ for the exact power of 2 appearing in a positive integer u we have the following result which is implicit in [5, 6] for integers a and which is easily extended to algebraic integers:

Lemma 5. *If* $u, v, a \geq 1$ *and* $v_2(v) \leq v_2(u)$ *then* $\gcd(a^u + 1, a^v - 1) \mid 2$*, otherwise* $\gcd(a^u + 1, a^v - 1) = a^{\gcd(u,v)} + 1$.

Proof. If $v_2(v) \leq v_2(u)$, set $g = \gcd(a^u + 1, a^v - 1)$ and $k = \gcd(2u, v)$. Then

$$g \mid \gcd(a^{2u} - 1, a^v - 1) = a^{\gcd(2u,v)} - 1 = a^k - 1.$$

so $g \mid a^k - 1$. But if we write $u = 2^{v_2(u)}u_1$ and $v = 2^{v_2(v)}v_1$ then

$$\frac{k}{2^{v_2(v)}} = \gcd(u_1 \cdot 2^{1+v_2(u)-v_2(v)}, v_1)$$

which is an odd integer. Hence $k \mid 2^{v_2(v)}u_1 \mid u$. Therefore $-1 \equiv a^u \equiv a^{k\cdot\frac{n}{k}} \equiv 1 \bmod g$ so $g \mid 2$. If $v_2(v) > v_2(u)$, first set $b = a^{2^{v_2(u)}}$ so

$$\gcd(a^u+1, a^v-1) = \gcd(b^{u_1}+1, b^{v_1\cdot 2^{v_2(v)-v_2(u)}}-1)$$

where $r = u_1$ is odd and $s = 2^{v_2(v)-v_2(u)}v_1$ is even. Then $b^{\gcd(r,s)}+1 \mid \gcd(b^r+1, b^s-1)$. There exist y, z with $yr+zs = \gcd(r,s)$ and y must be odd. If $x \mid \gcd(b^r+1, b^s-1)$ then $b^r \equiv -1 \bmod x$ and $b^s \equiv 1 \bmod x$ implies $b^{\gcd(r,s)} \equiv b \equiv (-1)^{yr} \equiv -1 \bmod x$ so $x \mid b^{\gcd(r,s)}+1$. Hence $\gcd(b^r+1, b^s-1) = b^{\gcd(r,s)}+1$ and the lemma is proved. □

It follows that

$$\gcd(\alpha^{n-s_1}+1, \alpha^{2m}-1) = \alpha^{\gcd(n-s_1,2m)}+1$$

provided that 2^u divides m. Otherwise, the greatest common divisor appearing on the left hand side above is $O(1)$. By estimate (6), it follows that we may assume that 2^u divides m. Now

$$(\alpha-\beta)U_m = \beta^m(\alpha^{2m}-1) = \beta^m(\alpha^m+1)(\alpha^m-1),$$

and $\gcd(\alpha^n - z_1, \alpha^{2m}-1)$ divides one of the two factors α^m+1 or α^m-1, and has a bounded greatest common divisor with the other factor. In particular, $\alpha^n - z_1$ is coprime to either W_m, which divides $\alpha^m+1 = \beta^{m/2}U_m/U_{m/2}$, or to $W_{m/2}W_{m/4}$, which divides $\alpha^m - 1 = \beta^{m/2}U_{m/2}$. Since at any rate we have that $u_n \equiv 0 \pmod{M}$, we must deduce that with either $N = W_m$, or $N = W_{m/2}W_{m/4}$, the estimate

$$N \ll N_{\mathbb{L}/\mathbb{Q}}\left(\gcd(N, \alpha^n - z_2)\right)$$

holds. Since also $N \geq \exp(c_1\phi(m/2))$, Lemma 4 shows that z_2 and α must also be multiplicatively dependent. In particular, $z_2 = \pm\alpha^{s'}$ for some integer s'.

Thus,

$$\alpha^n - z_2 = \alpha_1^{s'}(\alpha_1^{kn-s'} \pm 1) \mid (\alpha_1^{2kn-2s'}-1).$$

Again we show that s' is a multiple of k. Assume that it is not. Then $N \mid \alpha_1^{2km}-1$. Thus,

$$\gcd(N, \alpha^n - z_2) \mid \gcd(V_{2km}, V_{2kn-2s'}) \mid V_{\gcd(2km, 2kn-2s')} \mid V_{km/8}.$$

Indeed, the last relation above follows from the fact that $2k$ cannot divide the greatest common divisor of $2km$ and $2kn - 2s'$, together with the fact that m is a multiple of 8. However, since $N \mid W_m W_{m/2} W_{m/4}$, we get that N is coprime to $V_{km/8}$, so $N_{\mathbb{L}/\mathbb{Q}}(\gcd(N, \alpha^n - z_2)) = O(1)$, which is false. Thus, $s' = ks'_1$.

10. If the sign is $+1$ we are through. So, assume again that the sign is -1, i.e. $z_2 = -\alpha^{s'}$. Then

$$u_n - a = \gamma\beta^n \alpha_1^{s+s'}(\alpha^{n-s_1} + 1)(\alpha^{n-s'_1} + 1).$$

Putting now u_1 for the exact power of 2 in the factorization of $n - s'_1$; i.e., such that $2^{u_1} \| n - s'_1$, we see that the only situation in which the $\gcd(\alpha^{n-s'_1} + 1, \alpha^{2m} - 1)$ is not $O(1)$ is when $2^{u_1} \mid m$. In this case, the given greatest common divisor is $\alpha^{\gcd(n-s'_1, 2m)} + 1$ and, as in a previous argument, this number can be divisible by only one of W_m, $W_{m/2}$ or $W_{m/4}$ and must be coprime to the other two. To summarize, in this last case,

$$\gcd(u_n - a, W_m W_{m/2} W_{m/4}) \ll W_m W_{m/2}.$$

Since the number on the left should in fact be $\gg W_m W_{m/2} W_{m/4}$, we get a contradiction for large m. The theorem is therefore proved.

Acknowledgements

Research of F. L. was supported in part by Grant SEP-CONACyT 79685 and PAPIIT 100508.

References

[1] M. Aigner and G. M. Ziegler, *Proofs from the book*, Springer-Verlag, 1998.

[2] Yu. Bilu, G. Hanrot and P. M. Voutier (with an appendix by M. Mignotte), 'Existence of primitive divisors of Lucas and Lehmer numbers', *J. Reine Angew Math.* **539** (2001), 75–122.

[3] K. A. Broughan, 'Adic Topologies for the Rational Integers' *Canad. J. Math.* **55** (2003), 711 - 723.

[4] Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek, Perfect powers from products of terms in Lucas sequences, *J. Reine Angew. Math.* **611** (2007), 109–129.

[5] R. D. Carmichael, 'On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$' Annals of Math. **15** (1913/14) 30–48.

[6] R. D. Carmichael, 'On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$' Annals of Math. **15** (1913/14) 49–70.

[7] H. Fürstenberg, 'On the infinitude of primes', *Amer. Math. Monthly* **62** (1955), 353.

[8] S. Hernández and F. Luca, 'On a question of Broughan', *Proc. Amer. Math. Soc.* **136** (2008), 403–407.

[9] F. Luca and F. Pappalardi, 'Members of binary recurrent sequences on lines of the Pascal triangle', *Publ. Math. (Debrecen)* **67** (2005), 103–113.

[10] A. Schinzel, 'Primitive divisors of the expression $A^n - B^n$ in algebraic number fields', J. reine angew Math. **268/269** (1974), 27–33.

[11] C. L. Stewart, 'Primitive divisors of Lucas and Lehmer numbers', in *Transcendence Theory: Advances and Applications*, Academic Press, London, 1977, 79–92.

[12] C. L. Stewart, 'On the greatest prime factor of terms of a linear recurrence sequence', *Rocky Mountain J. Math.* **15** (1985), 599-608.