ACTA ARITHMETICA
109.1 (2003)

Arithmetic properties of members of a binary recurrent sequence

by

Florian Luca (Morelia)

Introduction. Let r and s be non-zero integers with $r^2+4s\neq 0$. A *binary recurrent sequence* of integers $(u_n)_{n\geq 0}$ is a sequence such that $u_0, u_1\in\mathbb{Z}$ and

$$u_{n+2}=ru_{n+1}+su_n \quad \text{for } n=0,1,\ldots \tag{1}$$

It is well known that if one denotes by α and β the two roots of the equation

$$x^2-rx-s=0, \tag{2}$$

then there exist two numbers c and d such that

$$u_n=c\alpha^n+d\beta^n \quad \text{for } n=0,1,\ldots; \tag{3}$$

moreover, the numbers c and d can be easily computed in terms of u_0, u_1, α and β, and they belong to $\mathbb{K}:=\mathbb{Q}[\alpha]$. In fact, c and d are conjugate in $\mathbb{K}$ when α is irrational. We set $d_{\mathbb{K}}:=[\mathbb{K}:\mathbb{Q}]$. We say that the sequence $(u_n)_{n\geq 0}$ is *non-degenerate* if $cd\neq 0$ and α/β is not a root of 1. From now on, $(u_n)_{n\geq 0}$ denotes a non-degenerate binary recurrent sequence and $C_1, C_2,\ldots$ are positive computable constants which are either absolute or depend on our sequence $(u_n)_{n\geq 0}$.

In this paper, we deal with arithmetic properties of the numbers u_m when m is a positive integer. Such properties have been considered before in the literature. For example, in [14] (see Corollary 3.5), it is shown that there exist computable positive constants C_1, C_2, depending only on the sequence $(u_n)_{n\geq 0}$, such that for $m>n$, $m>C_1$, and $u_n\neq 0$,

$$P\biggl(\frac{u_m}{\gcd(u_m,u_n)}\biggr)>C_2\biggl(\frac{m}{\log m}\biggr)^{1/(d_{\mathbb{K}}+1)}, \tag{4}$$

where for an integer k we use $P(k)$ to denote the largest prime factor of k with the convention that $P(0)=P(\pm 1)=1$ (see also [6] for some improve-

2000 *Mathematics Subject Classification*: Primary 11B37.

ments of (4)). As a corollary, there exists a computable constant C_3 depending only on $(u_n)_{n\geq 0}$ such that whenever $u_m \mid u_n$ for some $m > n$ and $u_n \neq 0$ we have $m < C_3$. This result has been improved by Pethő [10], who showed the existence of two computable constants C_4 and C_5, depending only on $(u_n)_{n\geq 0}$, such that if $u_n \mid u_m$ for some $n > C_4$, then $m > 2n - C_5 \log n$. Since Lucas sequences of the first type, i.e., binary recurrent sequences $(u_n)_{n\geq 0}$ with $u_0 = 0$, $u_1 = 1$ for which formula (3) is

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{for } n = 0, 1, \ldots, \tag{5}$$

have the property that $u_n \mid u_{2n}$ for all $n \geq 1$, it would seem that the above result from [10] is best possible. However, only recently has it been noticed (see [7]) that, in fact, one can say a lot more about the pairs of positive integers (n, m) with $n < m$ for which $u_n \mid u_m$ only by looking at the two numbers c/d and α/β. Indeed, the main result in [7] asserts the following:

1. If c/d and α/β are multiplicatively *dependent*, then there exists a computable constant C_6 such that $u_n \mid u_m$ for infinitely many pairs (n, m) with $n < m < C_6 n$. Moreover, such m and n can be chosen from certain effectively computable arithmetic progressions of positive integers.

2. If c/d and α/β are multiplicatively *independent*, then there exist two computable constants C_7 and C_8, depending only on $(u_n)_{n\geq 0}$, such that if $u_n \mid u_m$ and $C_7 < n$, then $m > C_8 n^2/\log n$.

In a certain sense, what the above result says is that the divisibility properties of the sequences $(u_n)_{n\geq 0}$ for which c/d and α/β are multiplicatively dependent resemble the divisibility properties of the Lucas sequences of the first type, while the divisibility properties of the sequences $(u_n)_{n\geq 0}$ for which c/d and α/β are multiplicatively independent are quite different. We will make this statement more precise later.

By replacing $(u_n)_{n\geq 0}$ by $(\eta u_n)_{n\geq 0}$, where η is a greatest common denominator of c and d, we may assume that c and d are algebraic integers, and from now on we will work under this assumption. Notice that the above replacement will affect, for example, the number $\gcd(u_m, u_n)$ only by the constant factor η. For the purpose of the next theorem, we shall assume that c/d and α/β are multiplicatively independent. Notice that $u_n \neq 0$ for all $n \geq 0$ in this case. Fix $n < m$ and let $D(m, n) := \gcd(u_m, u_n)/S$, where we use S for the largest divisor of $\gcd(u_m, u_n)$ composed only of prime factors p with $p \mid N_{\mathbb{K}}(cd\alpha\beta)$. The reason for analyzing only this *truncated* greatest common divisor $D(m, n)$ of u_m and u_n comes from the fact that the divisor S (more precisely, its size) is very easy to bound. Indeed, put $l := \gcd(r^2, s)$. Then (see [14, p. 74]) the numbers $\alpha_1 = \alpha^2/l$ and $\beta_1 = \beta^2/l$ are algebraic integers and the principal ideals $[\alpha_1]$ and $[\beta_1]$ are coprime in $\mathbb{K}$. In particular, we may write

$$u_n = l^{\lfloor n/2\rfloor}(c\alpha^i\alpha_1^{\lfloor n/2\rfloor} + d\beta^i\beta_1^{\lfloor n/2\rfloor}), \tag{6}$$

where $i = 0$ or 1 according to whether n is even or odd. Since $[\alpha_1]$ and $[\beta_1]$ are coprime in $\mathbb{K}$, it follows, by standard applications of linear forms in p-adic logarithms (see, for example, [22]) together with the fact that $u_n \neq 0$ for all $n \geq 0$, that if p is any fixed prime, then

$$\mathrm{ord}_p(c\alpha^i\alpha_1^{\lfloor n/2\rfloor} - d\beta^i\beta_1^{\lfloor n/2\rfloor}) < C_9 \log n \quad \text{for } i = 0, 1, \tag{7}$$

where the constant C_9 is computable but depends also on the prime number p. To summarize, if p is any prime dividing $N_{\mathbb{K}}(cd\alpha\beta)$, we have

$$\mathrm{ord}_p(u_n) = \begin{cases} C_{10}n + O(\log n) & \text{if } p \mid l, \text{ where } C_{10} = \mathrm{ord}_p(l)/2, \\ O(\log n) & \text{if } p \nmid l, \end{cases} \tag{8}$$

where the two implied constants are both computable and depend only on $(u_n)_{n\geq 0}$.

Theorem 1. *Let $(u_n)_{n\geq 0}$ be a non-degenerate binary recurrent sequence of integers. Assume that u_n is given by formula* (3) *with c and d algebraic integers, and that c/d and α/β are multiplicatively independent. Then, for any positive integers $m > n$, we have*

$$D(m,n) \leq 2\exp(C_{11}\sqrt{m}), \tag{9}$$

where $D(m,n)$ is the largest divisor of $\gcd(u_n, u_m)$ *free of primes dividing $N_{\mathbb{K}}(\alpha\beta cd)$, and $C_{11} := 2\log(\max(|\alpha|, |\beta|, |c|, |d|))$.*

As previously mentioned, the condition that c and d be algebraic integers can be avoided. In fact, if c and d are just algebraic numbers, then the statement of Theorem 1 still remains true with C_{11} replaced by $2\log(\max(|\alpha|, |\beta|, |c\eta|, |d\eta|)$ where η is the greatest common denominator of c and d. In this case, we also need to slightly modify the definition of $D(m,n)$, and take it to be the largest common divisor of u_m and u_n which is free of primes dividing $N_{\mathbb{K}}(\alpha\beta cd\eta^2)$. Notice that Theorem 1 says that if $u_n \mid u_m$ and c/d and α/β are multiplicatively independent, then $m > C_{12}n^2$, where C_{12} can be taken to be any constant slightly smaller than $1/C_{11}$ provided that m is large, which is an improvement upon our previous results from [7]. The proof of Theorem 1 above is entirely elementary. From Theorem 1, one may read immediately statements of the sort

$$\gcd(2^m - 3, 2^n - 3) \leq 2\cdot 3^{2\sqrt{m}} \quad \text{for all } m > n \geq 0,$$

as well as

$$\gcd(a^m - 2, a^n - 2) \leq 2\gcd(a,2)\cdot a^{2\sqrt{m}} \quad \text{for all } m > n \geq 0,$$

where $a \in \mathbb{Z}$, $a \neq 0, \pm 2^s$, with $s \geq 0$, inequalities which do not seem to have been noticed before. A result of the same flavour as Theorem 1 above has recently been proved by Bugeaud, Corvaja and Zannier [3] and asserts that if a and b are multiplicatively independent integers and $\varepsilon > 0$ is any positive number then

$$\gcd(a^m - 1, b^m - 1) = O(\exp(\varepsilon m))$$

when m is large. The implied constant above depends on a, b and ε.

A better version of Theorem 1 above might be able to shed some light on the *primitive divisor problem* for arbitrary binary recurrent sequences of integers. Recall that for a given positive integer m a prime number p with $p \mid u_m$ is called *primitive* if $p \nmid u_n$ for any $n < m$ for which $u_n \neq 0$. We conjecture that for every non-degenerate binary recurrent sequence $(u_n)_{n\geq 0}$ there exists a computable constant C_{13} such that u_m has a primitive divisor for all $m > C_{13}$. The fact that this is indeed so at least when c/d and α/β are multiplicatively dependent is contained in the next theorem.

Theorem 2. *Let $(u_n)_{n\geq 0}$ be a binary recurrent sequence of integers and assume that c/d and α/β are multiplicatively dependent. Then there exists an effectively computable constant C_{13} which depends on c, d, α and β such that u_m has a primitive divisor for $m > C_{13}$. Moreover, there exists another effectively computable constant C_{14} such that*

$$P(u_m) \geq m - C_{14} \quad \textit{for all } m \geq 0. \tag{10}$$

The above Theorem 2 is probably known to the experts and is implicit in [7], but since we are unaware of the existence of a formal proof in the literature we have decided to include it here. It would be interesting to find a sharp dependence of C_{13} on c, d, α, and β. When $c := 1/(\alpha - \beta)$ and $d := -1/(\alpha - \beta)$ and α and β are coprime then C_{13} can be taken to be absolute and its best value is $C_{13} = 30$ (see [1]). However, in the general case asserted by Theorem 2 above C_{13} is not absolute. The example $u_n := k!(2^n - 1)$ for all $n \geq 0$ with some positive integer k shows that C_{13} must depend on the prime divisors of $\gcd([c\alpha], [d\beta])$ in $\mathbb{K}$. Taking α to be any real irrational quadratic unit, β to be its conjugate, and $\mathbb{K}$ to be the quadratic field containing α, and setting $c := \alpha^{-m}$, $d := \beta^{-m}$ with some large positive integer m, we see immediately that $u_m = 0$ and $u_{m-1} = \pm u_{m+1}$. This example shows that C_{13} must also depend on the size of the multiplicative relation between c/d and α/β. It will be plain from our proof of Theorem 2 that, at least when c and d are algebraic integers, C_{13} can be taken to depend only on the largest prime factor of $\gcd([c\alpha], [d\beta]) \cdot \gcd([c\beta], [d\alpha])$, the degree and class number of $\mathbb{K}$, as well as the minimal multiplicative relation between c/d and α/β. When c and d are just algebraic numbers, our argument only shows that C_{13} depends also on the prime factors of the discriminant $\Delta := (\alpha - \beta)^2$ of our recurrence $(u_n)_{n\geq 0}$ as well. The same remarks apply to the constant C_{14}.

For sequences $(u_n)_{n\ge 0}$ with c/d and α/β multiplicatively independent, not only are we unable prove the existence of a primitive divisor for u_m when m is large, but we cannot even prove that the divisibility relation

$$u_m \mid \prod_{i=1}^{m-1} u_i \tag{11}$$

does not happen for infinitely many positive integers m, although an immediate application of our Theorem 1 shows that if

$$u_m \mid u_{n_1} \dots u_{n_t}, \tag{12}$$

where $0 \le n_1 \le \dots \le n_t$, then $t > C_{15}\sqrt{m}$, where C_{15} is a computable constant depending only on the sequence $(u_n)_{n\ge 0}$, thus extending, for example, Corollary 3.6 on page 67 in [14].

It could also be that our Theorem 1 might be used to get better lower bounds on $P(u_m)$ than the ones which follow from combining lower bounds for linear forms in complex and p-adic logarithms with the prime number theorem (such as inequality (4), for example) and which hold either for all large enough values of m, or on sets of indices m of asymptotic density 1. Such lower bounds do already exist in the literature and they have various shapes according to whether the binary recurrent sequence involved is Lucas or not. For example, it follows from results of [5], [13], [16] and [18] that for fixed non-zero integers u, v with $u \ne \pm v$ the inequality

$$P(u^m \pm v^m) > \frac{m(\log m)^2}{(\log\log m)^2} \tag{13}$$

holds for almost all positive integers m, while

$$P(2^p - 1) > \frac{p(\log p)^2}{\log\log p} \tag{14}$$

for almost all prime numbers p. On the other hand, C. Pomerance points out that it is still not known whether $P(2^n - 1) > 2n + 1$ for all but finitely many positive integers n.

For general binary recurrent sequences, it follows from results of Stewart [20] that for all positive integers n, except perhaps a set of asymptotic density zero,

$$P(u_n) > \varepsilon(n) n \log n, \tag{15}$$

where $\varepsilon(n)$ is any real-valued function for which $\lim_{n\to\infty} \varepsilon(n) = 0$. For these results and several related ones the reader should consult the excellent survey [21].

It has also become customary, when proving results concerning non-degenerate binary recurrent sequences of integers, to see to what extent one can generalize such results to non-degenerate binary recurrent sequences consisting of algebraic integers. Our results are easily amenable to such generalizations. Assume that c, d, α and β are non-zero algebraic integers and let $\mathbb{K}$ be a number field containing all four numbers c, d, α and β. Put again $d_{\mathbb{K}} := [\mathbb{K} : \mathbb{Q}]$ and let u_n be the algebraic integer in $\mathbb{K}$ given by formula (3) for all $n \geq 0$. Assume that α/β is not a root of 1. Then we have the following generalizations of Theorems 1 and 2.

Theorem 3. *Assume that c, d, α and β are non-zero algebraic integers and that α/β is not a root of* 1. *Let $\mathbb{K}$ be the smallest number field containing c, d, α and β and all their conjugates, and let $d_{\mathbb{K}}$ be its degree over $\mathbb{Q}$. For every positive integer n define the algebraic integer u_n in $\mathbb{K}$ according to formula* (3). *Assume that c/d and α/β are multiplicatively independent. For any pair of positive integers $m > n$ set $D(m, n)$ to be the largest ideal divisor of* $\gcd([u_m], [u_n])$ *which is free of primes dividing $N_{\mathbb{K}}(cd\alpha\beta)$. Then*

$$N_{\mathbb{K}}(D(m,n)) \leq 2^{d_{\mathbb{K}}} \exp(d_{\mathbb{K}} C_{16} \sqrt{m}), \tag{16}$$

where $C_{16} := 2 \log M$, and M is the maximum of the absolute values of all the conjugates of c, d, α and β.

Theorem 4. *Assume that $(u_n)_{n \geq 0}$ is given by formula* (3) *where c, d, α and β are non-zero algebraic integers and α/β is not a root of* 1. *Assume that c/d and α/β are multiplicatively dependent and let $\mathbb{K}$ be the smallest number field containing c, d, α and β* (*but not necessarily their conjugates*). *Then there exists an effectively computable constant C_{17} which depends on c, d, α and β such that u_m has a primitive divisor for $m > C_{17}$. Moreover, there exists another effectively computable constant C_{18} such that*

$$P(N_{\mathbb{K}}(u_m)) \geq (m - C_{18})^{1/d_{\mathbb{K}}} \quad \textit{for all } m \geq 0. \tag{17}$$

By a *primitive divisor* of u_m in the statement of Theorem 4 above we mean a prime ideal π in $\mathbb{K}$ such that π divides u_m but π does not divide u_n for any $n < m$ with $u_n \neq 0$. Notice that inequality (17) from Theorem 4 above is weaker than its analogue (10) from Theorem 2 and the reason for this is explained in Remark 1 following the proof of Theorem 4. Moreover, the same remarks as the ones following the statement of Theorem 2 concerning the dependence of the constants C_{17} and C_{18} on the given data apply here as well.

We now leave the exciting world of binary recurrent sequences of integers and we look at binary recurrent sequences of polynomials with rational coefficients. To fix ideas, let r and s be non-zero polynomials in $\mathbb{Q}[X]$ such that $r^2 + 4s \neq 0$. A binary recurrent sequence of polynomials $(u_n)_{n \geq 0}$ is simply a sequence with $u_0, u_1 \in \mathbb{Q}[X]$ and such that

$$u_{n+2} = ru_{n+1} + su_n \quad \text{for } n = 0, 1, \dots \tag{18}$$

If one denotes by α and β the two roots of the characteristic equation (2), then one may again infer that there exist c and d such that

$$u_n = c\alpha^n + d\beta^n \quad \text{for } n = 0, 1, \dots \tag{19}$$

Here, α is an algebraic integer of degree at most 2 over $\mathbb{Q}(X)$. Set again $\mathbb{K} := \mathbb{Q}(X)[\alpha]$. Then α, β, c and d are all in $\mathbb{K}$, and if $\mathbb{K} \neq \mathbb{Q}(X)$, then α and β are conjugate in $\mathbb{K}$, and so are c and d. We say again that the sequence $(u_n)_{n\geq 0}$ is non-degenerate if $cd \neq 0$, α/β is not a root of 1, and at least one of the two functions α/β and c/d is not constant. The reason for this last condition is that it is easy to prove that when α/β and c/d are both constants, then there exist two polynomials f and g in $\mathbb{Q}[X]$ and a non-degenerate binary recurrent sequence of integers $(v_n)_{n\geq 0}$ such that $u_n = fg^n v_n$ for all $n \geq 0$. In particular, as an element of $\mathbb{Q}[X]$, the polynomial u_n will be either zero or associated with the polynomial fg^n, and hence its divisibility properties are not all that interesting. Notice that when $(u_n)_{n\geq 0}$ is non-degenerate, then at least one of the four polynomials r, s, u_0 and u_1 is not constant.

Our next result adresses primitive divisors for u_m. Here, for a positive integer m we say that an irreducible factor p in $\mathbb{Q}[X]$ of u_m is *primitive* for u_m if p does not divide u_n for any $n < m$ for which $u_n \neq 0$. An analogue of Theorems 2 and 4 can be easily formulated and proved to hold for the case in which c/d and α/β are multiplicatively dependent, so we will restrict ourselves to considering the case when c/d and α/β are multiplicatively independent. Moreover, to make the statement of the next theorem clearer we shall assume that r and s are coprime, although this is not a real obstruction and a general statement can be recovered from the result below together with the pertinent analogues in the polynomial setting of the remarks preceding formula (6).

THEOREM 5. *Let $(u_n)_{n\geq 0}$ be a non-degenerate binary recurrent sequence of polynomials satisfying the recurrence* (18) *and such that the general formula of u_n is given by* (19). *Assume moreover that r and s are coprime and that c/d and α/β are multiplicatively independent. Then there exists a computable constant C_{19} such that u_m has primitive divisors for $m > C_{19}$. In fact, when α/β is not constant, a lot more holds, namely: For any positive integer m let* $\mathrm{Prim}(u_m)$ *be the product of all the non-associated primitive divisors of u_m. Then there exists a constant C_{20} such that*

$$\deg(\mathrm{Prim}(u_m)) > \deg(u_m) - C_{20} \quad \textit{for all } m \geq 0. \tag{20}$$

Finally, both constants C_{19} and C_{20} mentioned above are effectively computable and they depend only on the degrees of the polynomials u_0, u_1, r and s, but not on the polynomials themselves.

We point out that in a certain sense Theorem 5 above suggests that in the world of polynomials with rational coefficients the primitive part of u_m behaves better when c/d and $\alpha\beta$ are multiplicatively independent than when they are multiplicatively dependent. Indeed, the Lucas sequence $(u_n)_{n\geq 0}$ of general term

$$u_n := \frac{X^n - 1}{X - 1} \quad \text{for } n = 0, 1, \dots \tag{21}$$

has the property that $\mathrm{Prim}(u_m) = \Phi_m(X)$, the mth cyclotomic polynomial, and we thus have $\deg(\mathrm{Prim}(u_m)) = \phi(m)$, while $\deg(u_m) = m - 1$. Since

$$\phi(m) \leq m - \sqrt{m}$$

for all positive integers m which are not primes, we see that an inequality of the type (20) is impossible for almost all positive integers m in this particular example. In fact, even worse,

$$\phi(m) < e^{\gamma} \frac{m}{\log\log m} \tag{22}$$

for infinitely many positive integers m, where γ is the Euler constant (see [9]).

Current research in diophantine equations has also touched on equations of the form $u_n(x) = u_m(y)$ with solutions in integers x, y, and positive integers $m > n$, where $(u_n)_{n\geq 0}$ is a binary recurrent sequence of polynomials with rational coefficients (see, for example, [4]). In general, one conjectures that a diophantine equation of the type $f(x) = g(y)$ with integer solutions x, y, where f and g are two polynomials with rational coefficients, has only finitely many solutions (unless there are some obvious reasons for such an equation to have infinitely many solutions), but in proving that this is indeed so for quite general polynomials f and g one goes about either by using an old result of Siegel [15] concerning the finiteness of integer points on an irreducible curve defined over $\mathbb{Q}$ of positive genus, or by using a quite new result of Bilu and Tichy [2], which asserts that such equations do indeed have only finitely many solutions unless, up to some affine transformations, the pair of polynomials (f, g) belongs to one of five specific parametric families (called *standard pairs* in [2]), involving powers of polynomials, Dickson polynomials, and a few others, instances in which infinitely many integer solutions of such an equation may exist. Regardless of which method one uses, one still has to check that the conditions from either the theorem of Siegel, or the theorem of Bilu and Tichy, are fulfilled for the starting pair of polynomials (f, g), and checking that is not always a trivial task. It is our hope that our Theorem 5, or its method of proof, might make checking such conditions easier for a diophantine equation of the sort $u_n(x) = u_m(y)$ in integer unknowns x, y, and positive integers $m > n$, where $(u_n)_{n\geq 0}$ is a binary recurrent sequence of polynomials, or variations of those.

The proofs

The proof of Theorem 1. Throughout this proof, we write $D := D(m,n)$, and we assume that $|\alpha| \geq |\beta|$. Notice that if $n \leq \sqrt{m}$, then the inequality (9) is clear via

$$D \leq |u_n| = |c\alpha^n + d\beta^n| \leq 2\max(|c|,|d|)|\alpha|^{\sqrt{m}} \leq 2\exp(C_{11}\sqrt{m}).$$

So, we assume that $n > \sqrt{m}$. We write $m_0 := m$, $m_1 := n$, and the Euclidean algorithm

$$\begin{aligned} m_0 &:= q_0 m_1 + m_2, \\ m_1 &:= q_1 m_2 + m_3, \ \ldots, \\ m_j &:= q_j m_{j+1} + m_{j+2}, \end{aligned}$$

where we assume that $j \geq 0$ is the smallest index for which $m_{j+2} \leq \sqrt{m}$. Here, $m_i > m_{i+1}$ for all $i = 0,1,\ldots,j+1$, and $q_i = \lfloor m_i/m_{i+1} \rfloor$ is always a positive integer. The existence of j follows from the fact that we are assuming that $m_1 = n > \sqrt{m}$. We now fix $i \in \{0,1,\ldots,j+2\}$. We construct recursively non-negative integers r_i, s_i, t_i, v_i, and signs $\varepsilon_i \in \{\pm 1\}$ such that

$$c^{r_i} d^{s_i} \alpha^{m_i} + \varepsilon_i c^{t_i} d^{v_i} \beta^{m_i} \equiv 0 \pmod{D} \tag{23}$$

for $i = 0,1,\ldots,j+2$. Here, and in what follows, we will say that two algebraic integers x and y from $\mathbb{K}$ are *congruent* modulo a rational integer A if $x - y = Az$ with an algebraic integer z in $\mathbb{K}$. At $i = 0$ and 1 we have the relations

$$u_m = c\alpha^m + d\beta^m = c\alpha^{m_0} + d\beta^{m_0} \equiv 0 \pmod{D}$$

and

$$u_n = c\alpha^n + d\beta^n = c\alpha^{m_1} + d\beta^{m_1} \equiv 0 \pmod{D},$$

and we may therefore set $r_0 = r_1 = 1$, $s_0 = s_1 = 0$, $t_0 = t_1 = 0$, $v_0 = v_1 = 1$, and $\varepsilon_0 = \varepsilon_1 = +1$. Assume that $k \leq j$ is given and that r_i, s_i, t_i, v_i have been constructed for $i = 0,1,\ldots,k+1$ in such a way that (23) holds with some $\varepsilon_i \in \{\pm 1\}$. From now on, we will forget about the ε_i's (which, as the reader will see, are irrelevant), and we will simply write them as ± 1. To construct r_{k+2}, s_{k+2}, t_{k+2}, and v_{k+2}, write

$$c^{r_{k+1}} d^{s_{k+1}} \alpha^{m_{k+1}} \pm c^{t_{k+1}} d^{v_{k+1}} \beta^{m_{k+1}} \equiv 0 \pmod{D}, \tag{24}$$

therefore

$$c^{r_{k+1}} d^{s_{k+1}} \alpha^{m_{k+1}} \equiv \mp c^{t_{k+1}} d^{v_{k+1}} \beta^{m_{k+1}} \pmod{D},$$

and raising the above congruence to the power q_k and regrouping we get

$$c^{q_k r_{k+1}} d^{q_k s_{k+1}} (\alpha^{q_k m_{k+1}}) \pm c^{q_k t_{k+1}} d^{q_k v_{k+1}} (\beta^{q_k m_{k+1}}) \equiv 0 \pmod{D}. \tag{25}$$

But we also have

$$c^{r_k} d^{s_k} \alpha^{m_k} \pm c^{t_k} d^{v_k} \beta^{m_k} \equiv 0 \pmod{D}, \tag{26}$$

and using $m_k = q_k m_{k+1} + m_{k+2}$ we can write (26) as

$$c^{r_k} d^{s_k} \alpha^{m_{k+2}} (\alpha^{q_k m_{k+1}}) \pm c^{t_k} d^{v_k} \beta^{m_{k+2}} (\beta^{q_k m_{k+1}}) \equiv 0 \pmod{D}. \tag{27}$$

We now write $X := \alpha^{q_k m_{k+1}}$ and $Y := \beta^{q_k m_{k+1}}$ and treat the pair of congruences (25) and (27) as a modular homogeneous system in the indeterminates X and Y:

$$\begin{cases} c^{q_k r_{k+1}} d^{q_k s_{k+1}} X \pm c^{q_k t_{k+1}} d^{q_k v_{k+1}} Y \equiv 0 \pmod{D}, \\ c^{r_k} d^{s_k} \alpha^{m_{k+2}} X \pm c^{t_k} d^{v_k} \beta^{m_{k+2}} Y \equiv 0 \pmod{D}. \end{cases} \tag{28}$$

This system, together with the fact that its solution $(X, Y) = (\alpha^{z_k}, \beta^{z_k})$ with $z_k := q_k m_{k+1}$ has the property that both $N_{\mathbb{K}}(X)$ and $N_{\mathbb{K}}(Y)$ are coprime to D, leads to the conclusion that the determinant of the coefficient matrix of (28) must be a multiple of D. In particular, we get

$$c^{(r_k+q_k t_{k+1})} d^{(s_k+q_k v_{k+1})} \alpha^{m_{k+2}} \pm c^{(t_k+q_k r_{k+1})} d^{(v_k+q_k s_{k+1})} \beta^{m_{k+2}} \equiv 0 \pmod{D}. \tag{29}$$

By looking at (23), we may set

$$\begin{cases} r_{k+2} := r_k + q_k t_{k+1}, \\ s_{k+2} := s_k + q_k v_{k+1}, \\ t_{k+2} := t_k + q_k r_{k+1}, \\ v_{k+2} := v_k + q_k s_{k+1}. \end{cases} \tag{30}$$

It is now easy to see that

$$r_i = t_i \quad \text{and} \quad s_i = v_i \qquad \text{for all } i = 0, 1, \dots, j+2. \tag{31}$$

Indeed, this holds at $i = 0$ and $i = 1$ and by induction on i via the recurrence formulae (30). With (31), it follows that we may eliminate the numbers t_i and v_i and simply conclude that

$$c^{r_i} d^{s_i} \alpha^{m_i} \pm c^{s_i} d^{r_i} \beta^{m_i} \equiv 0 \pmod{D} \tag{32}$$

for all $i = 0, 1, \dots, j+2$, where $r_0 = r_1 = 1$, $s_0 = s_1 = 0$, and

$$\begin{cases} r_{i+2} = r_i + q_i s_{i+1} \\ s_{i+2} = s_i + q_i r_{i+1} \end{cases} \qquad \text{for } i = 0, 1, \dots, j. \tag{33}$$

Let $\delta_i := r_i - s_i$. Then $\delta_0 = \delta_1 = 1$, and relations (33) imply

$$\delta_{i+2} = -q_i \delta_{i+1} + \delta_i.$$

We notice that $\delta_2 = 1 - q_0 \le 0$ and $\delta_3 = -q_1 \delta_2 + \delta_1 = -q_1(1 - q_0) + 1 = q_1(q_0 - 1) + 1 > 0$. By induction, $\delta_i > 0$ for all $i \ge 1$ odd, and $\delta_i < 0$ for all $i \ge 4$ even. Indeed, assume, for example, that $i \ge 5$ is odd and that $(-1)^k \delta_k < 0$ for all $k < i$ except for δ_2 which might be zero. Then $\delta_i = -q_i \delta_{i-1} + \delta_{i-2} \ge \delta_{i-2} > 0$. The same argument shows that $\delta_i < 0$ for all $i \ge 4$ even. Let $\Delta_i := (-1)^{i-1} \delta_i$ for $i = 1, \dots, j+2$. Then $\Delta_i > 0$ for all i

except $\varDelta_2$ which might be zero, and the numbers $\varDelta_i$ satisfy $\varDelta_1 = 1$, $\varDelta_2 = q_0 - 1$, and the recurrence

$$\varDelta_{i+2} = q_i \varDelta_{i+1} + \varDelta_i \quad \text{for } i = 1, \ldots, j. \tag{34}$$

We may now rewrite relation (23) as

$$\begin{cases} (cd)^{s_i}(c^{\varDelta_i}\alpha^{m_i} \pm d^{\varDelta_i}\beta^{m_i}) \equiv 0 \pmod{D} & \text{if } i \geq 1 \text{ is odd,} \\ (cd)^{r_i}(d^{\varDelta_i}\alpha^{m_i} \pm c^{\varDelta_i}\beta^{m_i}) \equiv 0 \pmod{D} & \text{if } i \geq 2 \text{ is even,} \end{cases} \tag{35}$$

and since D is free of prime factors dividing $N_{\mathbb{K}}(cd)$, it follows that we may interpret (35) as

$$e^{\varDelta_i}\alpha^{m_i} \pm f^{\varDelta_i}\beta^{m_i} \equiv 0 \pmod{D} \quad \text{for } i = 1, \ldots, j+2, \tag{36}$$

where $\{e, f\} = \{c, d\}$. More precisely, $e = c$, $f = d$, when $i \geq 1$ is odd, and $e = d$, $f = c$, when $i \geq 2$ is even. The first thing we need to ensure is that the divisibility relation (36) is non-trivial, that is, that the expression appearing on the left hand side is never zero. Since at any rate $e/f \in \{c/d, d/c\}$ and c/d and α/β are multiplicatively independent, the expression on the left hand side of (36) can be zero only for $\varDelta_i = 0$ and $m_i = 0$. But from what we have said before $\varDelta_i = 0$ is possible only when $i = 2$ and $q_0 = 1$, and now $m_2 = 0$ and $q_0 = 1$ imply $m_0 = q_0 m_1 + m_2 = m_1$, therefore $m = n$, which is not possible. Next we notice that since relations (36) are not trivial, they imply that

$$D \leq |e^{\varDelta_i}\alpha_{m_i} \pm f^{\varDelta_i}\beta^{m_i}| \leq 2\exp(C_{11}\max(\varDelta_i, m_i)) \quad \text{for } i = 0, 1, \ldots, j+2. \tag{37}$$

Notice that (37) needs some justification, the expressions on the left hand side being only algebraic integers and not rational integers. That is, if a positive integer D divides a non-zero algebraic integer ζ, then it is not true, in general, that $D \leq |\zeta|$. To justify (37), notice that if $\mathbb{K} = \mathbb{Q}$, then e, f, α, β are integers and (37) obviously holds. Assume now that $\alpha \notin \mathbb{Q}$. Then α and β are conjugate in $\mathbb{K}$, and so are c and d, therefore e and f. In particular, if the sign in (36) is $+1$, then the expression at (36) is a rational integer and so (37) holds. If on the other hand the sign is -1, then the expression at (36) is of the form $A\sqrt{d}$, where A is an integer and d is the squarefree part of the discriminant $r^2 + 4s$ of the characteristic equation (2) of our binary recurrent sequence. In particular, the square of the expression on the left hand side of (36) is a non-zero integer, and this implies again that inequality (37) must hold.

Inequality (37) at $i = j+2$ implies, in particular, that

$$D \leq 2\max(C_{11}\max(\varDelta_{j+2}, m_{j+2})), \tag{38}$$

and since we already know that $m_{j+2} \leq \sqrt{m}$, we conclude that the inequality asserted in Theorem 1 will follow provided that we show that

$$\Delta_{j+2} \le \sqrt{m}. \tag{39}$$

Notice that for $j = 0$ we have

$$\Delta_2 = q_0 - 1 < q_0 = \left\lfloor \frac{m}{n} \right\rfloor < \sqrt{m},$$

because $n > \sqrt{m}$, so that (39) obviously holds if $j = 0$. From now on, we assume that $j > 0$. To prove (39), we introduce a new finite sequence A_i for $i = 1, \ldots, j+2$, satisfying $A_1 := 1$, $A_2 := q_0$, and $A_{i+2} := q_i A_{i+1} + A_i$ for $i = 1, \ldots, j$. Notice that $A_2 = q_0 > q_0 - 1 = \Delta_2$ and $A_3 = q_1 A_2 + A_1 = q_1 q_0 + 1 > q_1(q_0 - 1) + 1 = q_1 \Delta_2 + \Delta_1 = \Delta_3$, and so, since the numbers A_i and Δ_i satisfy the same recurrence relation for $i = 1, \ldots, j+2$, we find that $A_i > \Delta_i$ for all $i = 2, \ldots, j+2$. We now notice that the numbers A_i are related to the numbers m_i via the relation

$$m_0 = A_{i+1} m_i + A_i m_{i+1} \quad \text{for } i = 1, \ldots, j+1. \tag{40}$$

To check (40), notice that at $i = 1$ it simply says that

$$m_0 = A_2 m_1 + A_1 m_2 = q_0 m_1 + m_2,$$

which obviously holds. Assuming that (40) holds for some $i < j+1$, we have

$$\begin{aligned} m_0 = A_{i+1} m_i + A_i m_{i+1} &= A_{i+1}(q_i m_{i+1} + m_{i+2}) + A_i m_{i+1} \\ &= (q_i A_{i+1} + A_i) m_{i+1} + A_{i+1} m_{i+2} = A_{i+2} m_{i+1} + A_{i+1} m_{i+2}, \end{aligned}$$

and so it does indeed hold with the numbers A_i for $i = 1, \ldots, j+1$ as defined above. Evaluating (40) at $i = j+1$ and using the fact that $m_{j+1} > \sqrt{m}$ we get

$$m = m_0 = A_{j+2} m_{j+1} + A_{j+1} m_{j+2} \ge A_{j+2} m_{j+1} > A_{j+2}\sqrt{m},$$

therefore $A_{j+2} < \sqrt{m}$. Since we also know that $\Delta_{j+2} < A_{j+2}$, we get $\Delta_{j+2} < \sqrt{m}$, which is precisely (39), and which concludes the proof of our Theorem 1.

The proof of Theorem 3. Set again $D := D(m, n)$, assume that $n > \sqrt{m}$ and proceed identically as in the proof of Theorem 1 to conclude that a relation like (35) holds, namely

$$e^{\Delta_i} \alpha^{m_i} \pm f^{\Delta_i} \beta^{m_i} \equiv 0 \pmod{D}, \tag{41}$$

where $e/f \in \{c/d,\ d/c\}$. Conjugating (41) by an arbitrary element σ of the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, we also get relations of the form

$$\sigma(e)^{\Delta_i} \sigma(\alpha)^{m_i} \pm \sigma(f)^{\Delta_i} \sigma(\beta)^{m_i} \equiv 0 \pmod{\sigma(D)}. \tag{42}$$

Since the property of two numbers to be multiplicatively independent is preserved under conjugation by the σ's, it follows that none of the expressions on the left hand side of (42) is zero. Taking the products of all the above congruences (42) over all the σ's, we get

$$N_{\mathbb{K}}(D) \mid N_{\mathbb{K}}(e^{\varDelta_i}\alpha^{m_i} \pm f^{\varDelta_i}\beta^{m_i}), \tag{43}$$

and the integer on the right hand side of (43) is non-zero. Thus, by the absolute value inequality, we immediately get

$$N_{\mathbb{K}}(D) \le 2^{d_{\mathbb{K}}} \exp(d_{\mathbb{K}} C_{16} \max(\varDelta_i, m_i)) \quad \text{for } i = 0, 1, \ldots, j+2. \tag{44}$$

Inequality (44) at $i = j+2$ together with (39) implies (16) and concludes the proof of Theorem 3.

The proofs of Theorems 2 and 4. We proceed to the proof of Theorem 4 and we shall point out at the appropriate moment why Theorem 2 is slightly better.

First we assume that c and d are algebraic integers. This is part of the hypothesis in Theorem 4. In the case of Theorem 2, if c and d are not algebraic integers, we replace $(u_n)_{n\ge0}$ by $(\eta u_n)_{n\ge0}$ where η is a greatest common denominator of c and d, thus replacing (c,d) by $(\eta c, \eta d)$ of algebraic integers. Notice that since $c = (\alpha u_0 - u_1)/(\alpha-\beta)$ and $d = (u_1 - \beta u_0)/(\alpha-\beta)$, it follows that η divides $(\alpha-\beta)^2$.

Assume that c/d and α/β are multiplicatively dependent and belong to $\mathbb{K}$. We first show that there exists a number $\varrho \in \mathbb{K}$ which is not a root of unity, two coprime integers t and $v > 0$ (here, $v = 1$ when $t = 0$), and two roots of unity ζ_1 and ζ_2 in $\mathbb{K}$ such that

$$c/d = \varrho^t \zeta_1 \quad \text{and} \quad \alpha/\beta = \varrho^v \zeta_2. \tag{45}$$

To prove this, we start with two integers k and l, not both zero, such that

$$\left(\frac{c}{d}\right)^k = \left(\frac{\alpha}{\beta}\right)^l. \tag{46}$$

Notice that $k \ne 0$ because $k = 0$ implies that $l \ne 0$, and now (46) leads to the conclusion that α/β is a root of unity, which contradicts our assumptions. If $k < 0$, we may replace (k,l) by $(-k,-l)$ and relation (46) still holds. Thus, we may assume that $k > 0$. If $l = 0$, we infer that $c/d = \zeta_1$ is some root of unity in $\mathbb{K}$, and we may set $t := 0$, $v := 1$, $\varrho := \alpha/\beta$, and $\zeta_2 := 1$. Assume now that $l \ne 0$. Let $d_1 := \gcd(k,l)$, and write $k = d_1 k_1$, $l = d_1 l_1$, where now k_1 and l_1 are coprime. Taking d_1th roots in (46), we conclude that

$$\left(\frac{c}{d}\right)^{k_1} = \left(\frac{\alpha}{\beta}\right)^{l_1} \zeta \tag{47}$$

with ζ some root of unity in $\mathbb{K}$ of order dividing d_1. Let ϱ_1 denote the common value of the two sides of (47). Clearly, ϱ_1 is not a root of 1. On the one hand, taking k_1th roots in (47), we get $\varrho_1^{1/k_1} = c/d \in \mathbb{K}$, where ϱ_1^{1/k_1} is the determination of the k_1th root of ϱ_1 for which the above equality holds. On the other hand, $(\varrho_1\zeta^{-1})^{1/l_1} = \alpha/\beta \in \mathbb{K}$, where again we set $(\varrho_1\zeta^{-1})^{1/l_1}$ for the unique determination of the l_1th root of $\varrho_1\zeta^{-1}$ such that the above equality holds. Since k_1 and l_1 are coprime, there exist integers x and y so that $xl_1 + yk_1 = 1$. Set

$$\varrho := (\varrho_1^{1/k_1})^x((\varrho_1\zeta^{-1})^{1/l_1})^y \in \mathbb{K}. \tag{48}$$

Since any two determinations of any fixed root of a fixed complex number differ multiplicatively just by roots of unity, relation (48) together with the fact that $x/k_1 + y/l_1 = 1/(k_1l_1)$ immediately gives the relations $\varrho^{l_1} = \varrho_1^{1/k_1}\zeta_1 = c\zeta_1/d$ and $\varrho^{k_1} = (\varrho_1\zeta^{-1})^{1/l_1}\zeta_2 = \alpha\zeta_2/\beta$ with two roots of unity ζ_1 and ζ_2, and now the fact that all three numbers ϱ, c/d, and α/β are in $\mathbb{K}$ implies that ζ_1 and ζ_2 are in $\mathbb{K}$ as well. Setting now $v := k_1$ and $t := l_1$ we have obtained a representation of the form (45). Since α/β is not a root of unity, it follows easily that the exponents v and t are uniquely determined and that the value of ϱ is also uniquely determined up to roots of unity in $\mathbb{K}$.

Having proved (45), we may now write $\varrho = \gamma/\delta$ where γ and δ are algebraic integers in $\mathbb{K}$. The most canonical way of doing this for us is the following. With the two integers x and y such that $1 = xl_1 + yk_1 = xt + yv$, relations (45) imply that

$$\varrho = \frac{c^x\alpha^y\zeta_3}{d^x\beta^y},$$

where $\zeta_3 := \zeta_1^{-x}\zeta_2^{-y}$ is a root of unity in $\mathbb{K}$. Replacing ϱ by $\varrho\zeta_3^{-1}$, it follows that we may assume that

$$\varrho = \frac{c^x\alpha^y}{d^x\beta^y}. \tag{49}$$

We put

$$(\gamma,\delta) := \begin{cases} (c^x\alpha^y, d^x\beta^y) & \text{if } x \geq 0 \text{ and } y \geq 0,\\ (d^{-x}\beta^{-y}, c^{-x}\alpha^{-y}) & \text{if } x \leq 0 \text{ and } y \leq 0,\\ (c^x\beta^{-y}, d^x\alpha^{-y}) & \text{if } x > 0 \text{ and } y < 0,\\ (d^{-x}\alpha^y, c^{-x}\beta^y) & \text{if } x < 0 \text{ and } y > 0. \end{cases}$$

All the above representations of ϱ as a ratio of two algebraic integers γ and δ have the property that if π is a prime ideal dividing both γ and δ, then π divides the ideal $D := \gcd([c\alpha],[d\beta])\gcd([c\beta],[d\alpha])$.

It thus follows that for any positive integer m we may write

$$u_m = \frac{d\beta^m}{\delta^{vm+t}}\,(\delta^{vm+t} - \zeta_m\gamma^{vm+t}). \tag{50}$$

In (50), the numbers $\zeta_m = -\zeta_1\zeta_2^m$ are roots of unity, but they may obviously depend on m. When $(u_n)_{n\geq 0}$ is a binary recurrent sequence of integers, (50) can be made more precise. Namely, if α is rational, then we may take

$\varrho = \gamma/\delta$ to be a rational number in reduced form, thus $D := 1$ and (50) holds with $\zeta_m \in \{\pm 1\}$. When α is irrational, then upon setting γ and δ as before and writing σ for the unique Galois automorphism of $\mathbb{K}$ over $\mathbb{Q}$, the fact that $\sigma(c) = d$ and $\sigma(\alpha) = \beta$ implies immediately that $\sigma(\gamma) = \delta$. Applying σ in the equations (45) and using the fact that $\sigma(c/d) = d/c$, $\sigma(\alpha/\beta) = \beta/\alpha$ and $\sigma(\varrho) = \varrho^{-1}$ we get $\sigma(\zeta_1) = \zeta_1$ and $\sigma(\zeta_2) = \zeta_2$. Thus, $\zeta_1 = \pm 1$ and $\zeta_2 = \pm 1$, and this shows that $\zeta_m = \pm 1$ in (50) in this case as well.

We now leave formula (50) for a while and we introduce some more notations. Let U be the group of roots of unity inside $\mathbb{K}$, and assume that U contains R elements. We label the elements of U somehow, say $\zeta_1, \ldots, \zeta_R$. U is cyclic and the field $\mathbb{K}$ contains a primitive root of unity of order R whose degree over $\mathbb{Q}$ is $\phi(R)$, so $\phi(R) \le d_{\mathbb{K}}$. In particular, $R < C_{21} d_{\mathbb{K}} \log\log\max(d_{\mathbb{K}}, e^e)$, where C_{21} is an absolute constant. For two fixed algebraic numbers γ and δ we say that the collection of algebraic integers $(w_{m,i})_{m,i}$ in $\mathbb{K}$ given by

$$(51) \qquad w_{m,i} := \delta^m - \zeta_i \gamma^m \quad \text{for all } m \ge 0 \text{ and } i = 1, \ldots, R$$

is a *generalized Lucas sequence* in $\mathbb{K}$.

We now neglect for a while the fact that the powers appearing in (50) run only in a certain arithmetic progression of positive integers and we address the *primitive divisor problem* for the generalized Lucas sequence $(w_{m,i})_{m,i}$. Fix a positive integer m and an index $i \in \{1, \ldots, R\}$. We say that the algebraic number $w_{m,i}$ has a *primitive divisor* if there exists a prime π in $\mathbb{K}$ dividing $w_{m,i}$ such that π does not divide $w_{n,j}$ for any pair of integers n, j with $w_{n,j} \ne 0$ and $0 \le n < m$.

We shall show that there exists a computable constant C_{22} depending only on $d_{\mathbb{K}}$, the class number $h := h_{\mathbb{K}}$ of $\mathbb{K}$, and $P(N_{\mathbb{K}}(D))$, so that when $m > C_{22}$ then $w_{m,i}$ has a primitive divisor. The remaining part of this proof is due to A. Schinzel. When $[\gamma]$ and $[\delta]$ are coprime, it has been first shown by Schinzel in [11], in the particular case $R = 1$ (i.e., when $\zeta_i = 1$ always), and then in the general case in [12], that such a constant C_{22} exists and that it can be taken to depend only on $d_{\mathbb{K}}$. When $R = 1$, Stewart (see [17] and [19]) showed that one may take $C_{22} := \max(2(2^{d_{\mathbb{K}}} - 1), e^{452} d_{\mathbb{K}}^{67})$. Assume now that $[\gamma]$ and $[\delta]$ are not coprime. Write $[\gamma] = D_1 I$ and $[\delta] = D_1 J$, where $D_1 := \gcd([\gamma], [\delta])$. Notice that every prime divisor of D_1 divides D. Let λ_1 be a generator of the principal ideal D_1^h. Then, since $[\gamma^h] = D_1^h I^h$ and $[\delta^h] = D_1^h J^h$, it follows that $\gamma^h = \lambda_1 \gamma_1$ and $\delta^h = \lambda_1 \delta_1$, where γ_1 and δ_1 are generators of the coprime principal ideals I^h and J^h, and obviously γ_1/δ_1 is not a root of 1. Let $\lambda := \lambda_1^{1/h}$ be any fixed determination of an hth root of λ and write $\gamma = \lambda\gamma_2$ and $\delta = \lambda\delta_2$, where γ_2 and δ_2 are the unique determinations of $\gamma_1^{1/h}$ and $\delta_1^{1/h}$ such that the above formulae hold. Notice that $(\delta_2/\gamma_2)^h = (\delta/\gamma)^h$, so that δ_2/γ_2 is not a root of unity.

Let $\mathbb{K}_1 := \mathbb{K}[\lambda_1]$. Then obviously $d_{\mathbb{K}_1} \le h d_{\mathbb{K}}$, so the degree of $\mathbb{K}_1$ can be bounded in terms of $d_{\mathbb{K}}$ and h. Since $\lambda \in \mathbb{K}_1$, we see that both γ_2 and δ_2 belong to $\mathbb{K}_1$, and obviously $[\gamma_2]$ and $[\delta_2]$ are coprime in $\mathbb{K}_1$ (this is because by considering the ideals $[\gamma_2]^h$ and $[\delta_2]^h$ in $\mathbb{K}_1$ and intersecting them with the ring of algebraic integers in $\mathbb{K}$ we get I^h and J^h which are coprime). Thus, in $\mathbb{K}_1$, we have $w_{m,i} = \lambda^m(\gamma_2^m - \zeta_i \delta_2^m)$, and $[\gamma_2]$ and $[\delta_2]$ are coprime. By Schinzel's result from [12], there exists a constant C_{23} depending only on $d_{\mathbb{K}_1}$ such that if we set $w'_{m,i} := \gamma_2^m - \zeta_i\delta_2^m$, then $w'_{m,i}$ has primitive divisors for $m > C_{23}$. It is easy to see that any primitive divisor π_1 in $\mathbb{K}_1$ of $w'_{m,i}$ sits above a rational prime $p \in \mathbb{Z}$ such that $p > (m+1)^{1/d_{\mathbb{K}_1}}$. Indeed, since π_1 obviously does not divide either γ_2 or δ_2, it follows that δ_2 is invertible modulo π_1 and $(\gamma_2/\delta_2)^m \equiv \zeta_i \pmod{\pi_1}$. Since π_1 is also primitive, it follows that the order of γ_2/δ_2 in the finite field $\mathcal{O}_{\mathbb{K}_1}/\pi_1$ is at least m. Since on the other hand this order divides $N_{\mathbb{K}_1}(\pi_1) - 1 \le p^{d_{\mathbb{K}_1}} - 1$, we do indeed get $p \ge (m+1)^{1/d_{\mathbb{K}_1}}$. Thus, choosing $C_{24} := P_1^{1/d_{\mathbb{K}_1}} \ge P(N_{\mathbb{K}}(D_1))^{1/d_{\mathbb{K}_1}}$ and imposing that $m > C_{22} := \max(C_{23}, C_{24})$, it follows that $w'_{m,i}$ has a primitive divisor π_1 in $\mathbb{K}_1$ which does not divide λ. It is now clear that if π is the prime ideal in $\mathbb{K}$ such that π_1 sits above π, then π is a primitive divisor of $w_{m,i}$. In particular, π does not divide $\gamma\delta$. We now set C_{17} (respectively C_{13}) to be such that $vm + t > \max(|t|, C_{22})$ whenever $m > C_{13}$. Take $m > C_{13}$ and take π to be a primitive prime divisor of $w_{vm+t,i}$, where i is the index in $\{1, \ldots, R\}$ so that $\zeta_i = \zeta_m$. Since π does not divide δ, it follows that π divides u_m. It is clear that π does not divide $d\beta^m$, because $\frac{d\beta^m}{\delta^{vm+t}} = \frac{c\alpha^m}{\gamma^{vm+t}}\zeta_m$ implies that if π divides $d\beta^m$, then π divides $c\alpha^m$ as well, therefore π divides D, which is not possible by our choice of the constant C_{24}. Thus, if π is not primitive for u_m, there exists $n < m$ so that π divides $\delta^{vn+t} - \zeta_n\gamma^{vn+t} \ne 0$. Clearly, $vn + t < vm + t$. When $vn + t \ge 0$ we get a contradiction with the fact that π is primitive for $w_{vm+t,i}$. If $vn + t < 0$, then

$$\begin{aligned}\delta^{vn+t} - \zeta_n\gamma^{vn+t} &= -\left(\frac{\zeta_n\gamma^{vn+t}}{\delta^{vn+t}}\right)(\delta^{-vn-t} - \zeta_n^{-1}\gamma^{-vn+t})\\ &= -\left(\frac{\zeta_n\gamma^{vn+t}}{\delta^{vn+t}}\right)w_{-vn-t,j},\end{aligned}$$

where we write j for the index in $\{1, \ldots, R\}$ such that $\zeta_j = \zeta_n^{-1}$. Thus, π divides $w_{-vn-t,j}$ and since $-vn - t = |vn + t| \le |t| < vm + t$, we get again a contradiction with the fact that π is primitive for $w_{vm+t,i}$.

This completes the proof of the existence of the primitive divisors for both instances of Theorems 2 and 4. It remains to justify the inequalities (10) and (17). In the case of Theorem 2, we have $\zeta_m = \pm 1$ and the numbers δ and γ are either coprime integers, or quadratic conjugate algebraic numbers. When $m > C_{22}$, $w_{m,\pm 1}$ has primitive prime divisors π in $\mathbb{K}$ which sit above rational primes $p \in \mathbb{Z}$, which are primitive in the classical sense for the Lucas sequence of first or second kind (according to whether $\zeta_m = -1$ or $+1$) whose roots are γ and δ. Thus, this rational prime p divides $w_{m,\pm 1}$ and it is known that such a prime number p is congruent to either 1 or -1 modulo m. This shows that $P(u_m) \ge vm + t - 1 > m - (|t| + 1)$ for $m > C_{13}$, which implies that $P(u_m) > m - C_{14}$ for all $m \ge 0$ with $C_{14} := C_{13} + |t| + 2$. Finally, inequality (17) follows in the same way from the fact that for $m > C_{22}$ any primitive divisor of $w_{m,i}$ is a prime ideal π of $\mathbb{K}$ sitting above a rational prime $p \in \mathbb{Z}$ with the property that both δ and γ are invertible modulo π and that the order of δ/γ modulo π is at least m. Since this order divides $N_{\mathbb{K}}(\pi) - 1 \le p^{d_{\mathbb{K}}} - 1$, we get $P(N_{\mathbb{K}}(w_{m,i})) > (m+1)^{1/d_{\mathbb{K}}}$. Thus, for $m > C_{17}$, we have $P(N_{\mathbb{K}}(u_m)) > (vm + t + 1)^{1/d_{\mathbb{K}}} > (m - (|t| - 1))^{1/d_{\mathbb{K}}}$, and therefore $P(N_{\mathbb{K}}(u_m)) > (m - C_{20})^{1/d_{\mathbb{K}}}$ for all $m \ge 0$ with $C_{20} := |t| + C_{17}$.

Remark 1. The arguments employed in the above proof show that under the assumptions of Theorem 4 we can conclude that for infinitely many positive integers m the slightly better inequality $P(N_{\mathbb{K}}(u_m)) > C_{25} m^{1/(d_{\mathbb{K}}-1)}$ holds, and, in fact, for large x, the number of such positive integers $m < x$ is $\gg x/\log x$, where both C_{25} and the implied constant are effectively computable in terms of the sequence $(u_n)_{n \ge 0}$. To see this, recall that the numbers v and t defined in the proof of Theorem 4 are coprime, so by Dirichlet's theorem on primes in arithmetic progressions it follows that for large x, the number of positive integers $m < x$ for which $vm + t = q$ is a prime is $\gg x/\log x$. When $vm + t = q$ is a large prime, u_m has a prime divisor π in $\mathbb{K}$ sitting above a rational prime $p \in \mathbb{Z}$ such that $p^f - 1 \equiv 0 \pmod{q}$, where $f \le d_{\mathbb{K}}$ is the dimension of the finite field $\mathcal{O}_{\mathbb{K}}/\pi$ as a vector space over $\mathbb{Z}_p$. In particular,

$$q \mid p^f - 1$$

or, equivalently,

$$q \,\Big|\, \prod_{d \mid f} \Phi_d(p),$$

and from the above divisibility relation we deduce that $p > C_{25} m^{1/(d_{\mathbb{K}}-1)}$ for large m.

Remark 2. As the reader might have noticed, the bulk of the proofs of Theorems 2 and 4 consists in proving that if δ, γ and ζ are non-zero algebraic integers in an algebraic number field $\mathbb{K}$ such that ζ is a root of unity and δ/γ is not a root of unity, then for all sufficiently large values of the positive integer m, the algebraic number $\delta^m - \zeta\gamma^m$ is divisible by a prime ideal not dividing any of the numbers $\gamma^n - \zeta'\delta^n$ for $0 < n < m$ and any root of unity ζ'. This fact is not new and has been proved by Schinzel in [12], but only for the case in which δ and γ are coprime. Thus, our Theorems 2 and

4 are a bit more general not only in the above sense, but also because they apply to quite general binary recurrent sequences of algebraic integers (in particular, to any binary recurrent sequence $(u_n)_{n\geq 0}$ of algebraic integers for which the equation $u_m = 0$ has a non-negative integer solution m).

The proof of Theorem 5. A non-degenerate binary recurrent sequence of polynomials with rational coefficients $(u_n)_{n\geq 0}$ behaves essentially differently in the case when α/β is not a constant, than in the case where α/β is a constant. So, we shall treat the two cases separately. From now on, all the effectively computable constants $C_{26}, C_{27}, \ldots$ that will show up, except for C_{42}, will depend only on the degrees of the polynomials u_0, u_1, r, and s but not on the polynomials themselves. We start with the most interesting situation.

Case 1: *α/β is not constant.* Write

$$u_m = \prod_{p\mid u_m} p^{\alpha_p} = A(m)B(m), \tag{52}$$

where

$$A(m) := \prod_{\substack{p\mid u_m\\ \alpha_p>1}} p^{\alpha_p} \quad \text{and} \quad B(m) := \prod_{\substack{p\mid u_m\\ \alpha_p=1}} p.$$

We first show that there exists an effectively computable constant C_{26} such that $\deg(A(m)) \leq C_{26}$. Suppose first that $p \mid A(m)$ is a prime divisor of $s = -\alpha\beta$. Since $p^{\alpha_p} \mid u_m$, we have the divisibility relations

$$p^{\alpha_p} \mid c^2(-s)^m + (cd)\beta^{2m} \quad \text{and} \quad p^{\alpha_p} \mid (cd)\alpha^{2m} + d^2(-s)^m. \tag{53}$$

These relations, and many others that will appear throughout this proof, are to be interpreted in the ring of algebraic integers in the algebraic function field $\mathbb{K} := \mathbb{Q}(X)[\alpha]$. Assume first that $m > \alpha_p$. Then, from (53), we get $p^{\alpha_p} \mid cd(\alpha^{2m} + \beta^{2m})$. From the binomial formula and the fact that $p \mid s$ we infer that

$$r^{2m} \equiv (\alpha+\beta)^{2m} \pmod p \equiv \alpha^{2m} + \beta^{2m} \pmod p,$$

and since r and s are coprime, we conclude that $p^{\alpha_p} \mid cd$. In particular, $\alpha_p \leq \deg(cd) \leq C_{27}$ (notice that cd is a non-zero polynomial). If $m \leq \alpha_p$, (53) implies that $p^m \mid cd(\alpha^{2m} + \beta^{2m})$, and the above argument shows that $m \leq C_{27}$. From the recurrence relation $u_{n+2} = ru_{n+1} + su_n$ for $n = 0, 1, \ldots,$ one finds immediately, by induction on n, that

$$\deg(u_n) \leq C_{28}(n+1) \qquad \text{for all } n \geq 0,$$

where

$$C_{28} := \max(\deg(u_0), \deg(u_1), \deg(r), \deg(s)).$$

Hence, since $m \le C_{27}$ when $m \le \alpha_p$, we deduce, from the fact that $p^{\alpha_p} \mid u_m$, that

$$\alpha_p \le \deg(u_m) \le C_{28}(m+1) \le C_{29},$$

where $C_{29} := C_{27}(C_{28}+1)$. The above argument shows that if we write $A(m) = A_1(m)A_2(m)$, where

$$A_1(m) := \prod_{\substack{p \mid A(m) \\ p \mid s}} p^{\alpha_p} \quad \text{and} \quad A_2(m) := \prod_{\substack{p \mid A(m) \\ p \nmid s}} p^{\alpha_p},$$

then $\deg(A_1(m)) \le C_{29}$. It remains to bound the degree of $A_2(m)$. Write

$$A_3(m) = \prod_{p \mid A_2(m)} p^{\alpha_p - 1}.$$

Notice that $A_3(m)$ is equal to $A_2(m)/\mathrm{rad}(A_2(m))$, where for a non-zero polynomial f we write $\mathrm{rad}(f)$ for the polynomial which is the product of all the non-associated irreducible factors of f. If $A_2(m) = 1$, then there is nothing to prove. So, we may assume that $\deg(A_3(m)) \ge 1$. We may also assume that $m \ge 2$, otherwise $\deg(A(m)) \le \max(\deg(u_0), \deg(u_1)) \le C_{28}$. Taking derivatives in the congruence

$$c\alpha^m + d\beta^m \equiv 0 \pmod{A_2(m)} \tag{54}$$

we get

$$(c'\alpha + mc\alpha')\alpha^{m-1} + (d'\beta + md\beta')\beta^{m-1} \equiv 0 \pmod{A_3(m)}. \tag{55}$$

We treat the system of congruences (54) and (55) as a homogeneous linear system modulo $A_3(m)$ in the indeterminates $X := \alpha^{m-1}$ and $Y := \beta^{m-1}$, and as such we write it as

$$\begin{cases} c\alpha X + d\beta Y \equiv 0 \pmod{A_3(m)}, \\ (c'\alpha + mc\alpha')X + (d'\beta + md\beta')Y \equiv 0 \pmod{A_3(m)}. \end{cases} \tag{56}$$

Let $\Delta := -s(cd' - c'd) + mcd(\alpha\beta' - \alpha'\beta)$ be the discriminant of the above system. It is easy to see that $(\beta-\alpha)^2\Delta^2 = (r^2+4s)\Delta^2$ is a polynomial with rational coefficients. Indeed, if $\mathbb{K} = \mathbb{Q}(X)$, then Δ is an element of $\mathbb{Q}[X]$, while when $d_{\mathbb{K}} := [\mathbb{K} : \mathbb{Q}(X)] = 2$, the fact that $(r^2+4s)\Delta^2$ is an element of $\mathbb{Q}[X]$ follows from the fact that the four pairs (α, β), (c, d), (α', β') and (c', d') consist of conjugate elements in $\mathbb{K}$ and the first two consist of algebraic integers in $\mathbb{K}$ while the last two consist of elements of $\mathbb{K}$ whose denominators divide $r^2 + 4s = (\beta - \alpha)^2$. If $\Delta = 0$, the function $c\alpha^m/(d\beta^m)$ is a constant, and we may write $c\alpha^m = \gamma d\beta^m$, where γ is a constant which is not a root of unity because c/d and α/β are multiplicatively independent. In particular, $\gamma \ne -1$. But in this case, $u_m = d\beta^m(1+\gamma) \ne 0$, and since $A_2(m) \mid u_m$ and $A_2(m)$ is coprime to s, we see that $A_2(m) \mid cd$, therefore

$\deg(A_2(m)) \le C_{27}$. Finally, if $\Delta \neq 0$, then we may solve the above system (56) with Cramer's rule and find that both $A_3(m) \mid (r^2+4s)\Delta^2\alpha^{m-1}$ and $A_3(m) \mid (r^2+4s)\Delta^2\beta^{m-1}$. In particular,

$$(57) \qquad A_3(m) \mid (r^2+4s)\Delta^2 \gcd(\alpha^{m-1}+\beta^{m-1}, (-s)^{m-1}).$$

Since r and s are coprime and $m \ge 2$, the polynomials $\alpha^{m-1}+\beta^{m-1}$ and s^{m-1} are coprime, and therefore $A_3(m) \mid (r^2+4s)\Delta^2$. Thus,

$$\deg(A_3(m)) \le \deg((r^2+4s)\Delta^2) \le C_{30},$$

and now

$$(58) \qquad \deg(A_2(m)) \le 2\deg(A_3(m)) \le 2C_{30}.$$

Thus,

$$(59) \qquad \deg(A(m)) = \deg(A_1(m)) + \deg(A_2(m)) \le C_{26},$$

where we set $C_{26} := C_{29} + 2C_{30}$.

Next we prove that there exist constants C_{31} and C_{32} such that

$$(60) \qquad \deg(u_m) \ge C_{31}m - C_{32}.$$

We split the argument into two subcases.

Subcase 1: $\deg(s) > 0$. We write $k := \deg(s)$ and we show that (60) holds with $C_{31} = k/2$ and some constant C_{32}. To prove this, we introduce the sequence $(w_n)_{n\ge0}$ by

$$w_n := (\beta-\alpha)d\alpha^n - (\beta-\alpha)c\beta^n \quad \text{for } n = 0,1,\ldots$$

An immediate computation shows that

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

therefore

$$\begin{aligned} w_0 &= (\beta-\alpha)(d-c) = (-u_0\alpha+u_1) - (\beta u_0 - u_1) \\ &= 2u_1 - u_0(\alpha+\beta) = 2u_1 - u_0 r \in \mathbb{Q}[X], \end{aligned}$$

and

$$\begin{aligned} w_1 &= (\beta-\alpha)(d\alpha - c\beta) = (-u_0\alpha^2 + u_1\alpha) - (\beta^2 u_0 - \beta u_1) \\ &= u_1(\alpha+\beta) - u_0(\alpha^2+\beta^2) = u_1 r - u_0(r^2+2s) \end{aligned}$$

is a polynomial in $\mathbb{Q}[X]$ as well. Since obviously

$$(61) \qquad w_{n+2} = rw_{n+1} + sw_n \quad \text{for } n = 0,1,\ldots,$$

it follows that $(w_n)_{n\ge0}$ is a non-degenerate binary recurrent sequence of polynomials with rational coefficients. Notice that w_n is never zero because c/d and α/β are multiplicatively independent. The polynomials u_n and w_n are related via the formula

$$(62) \qquad (r^2+4s)u_n^2 - w_n^2 = 4(r^2+4s)cd(-s)^n \quad \text{for } n = 0,1,\ldots$$

We now choose

$$C_{33} := 2C_{26} + C_{27} + 2C_{28} \geq 2\deg(A(m)) + \deg(cd) + \deg(r^2 + 4s)$$

and let $m > C_{33}$. We set $D := \gcd((r^2 + 4s)u_m^2, w_m^2)$ and notice that (62) implies that $D = (r^2 + 4s)\gcd(u_m^2, cds^m)$. From the way we have chosen the constant C_{33}, we infer that $\deg(D) < C_{33} < m$. Thus, we may write (62) as

$$\frac{(r^2 + 4s)u_m^2}{D} - \frac{w_m^2}{D} = \frac{4(r^2 + 4s)(cd)(-s)^m}{D}, \tag{63}$$

which is a polynomial relation of the type $A + B = C$ with

$$A := \frac{(r^2 + 4s)u_m^2}{D}, \qquad B := -\frac{w_m^2}{D}, \qquad C := \frac{4(r^2 + 4s)cd(-s)^m}{D}, \tag{64}$$

where the three polynomials A, B, C are coprime, non-zero, and at least one of them (namely C) is non-constant. We now recall the following theorem due to Mason (see [8]).

Mason's Theorem. *Let A, B, C be three non-zero and coprime polynomials with at least one of them non-constant and such that $A + B = C$. Then*

$$\max(\deg(A), \deg(B), \deg(C)) \leq N(ABC) - 1,$$

where for a non-constant polynomial f we denote by $N(f)$ the number of distinct complex roots of f.

To prove now that $\deg(u_m) \geq C_{31}m - C_{32}$ when $m > C_{33}$, we argue as follows. We look at formula (63). If

$$\deg((r^2 + 4s)u_m^2) \geq \deg(4(r^2 + 4s)cd(-s)^m),$$

then (60) obviously holds with any $C_{32} > 0$. If

$$\deg((r^2 + 4s)u_m^2) < \deg(4(r^2 + 4s)cd(-s)^m),$$

then

$$\deg(w_m^2) = \deg(4(r^2 + 4s)cd(-s)^m),$$

therefore $\deg(w_m) \geq C_{31}m + \deg((r^2 + 4s)cd)/2$. From (63), (64) and Mason's Theorem, we get

$$\begin{aligned}
2\deg(w_m) - \deg(D) &= \deg\left(\frac{w_m^2}{D}\right) = \max(\deg(A), \deg(B), \deg(C)) \\
&\leq N(ABC) - 1 = N\left(\frac{(r^2+4s)^2(cd)w_m^2u_m^2(-s)^m}{D^3}\right) - 1 \\
&\leq N((r^2 + 4s)cdw_mu_m) - 1 \\
&< \deg(u_m) + \deg(w_m) + \deg((r^2 + 4s)cd),
\end{aligned}$$

therefore

$$\begin{aligned}\deg(u_m) &\geq \deg(w_m) - \deg(D) - \deg((r^2+4s)cd)\\ &\geq C_{31}m - \deg(D) - \frac{\deg((r^2+4s)cd)}{2} \geq C_{31}m - C_{32},\end{aligned}$$

where we set

$$C_{32} := \frac{C_{31}}{2} + C_{28} + C_{33} \geq \frac{\deg((r^2+4s)cd)}{2} + \deg(D).$$

Subcase 2: $\deg(s) = 0$. In this case, s is a non-zero constant, and since α/β is not constant, we see that $\deg(r) > 0$. We will show that there exists an index $i \leq C_{28} + 1$ such that $\deg(ru_i) > \deg(u_{i-1})$. Assume for the moment that we have proved this. Since $u_{i+1} = ru_i + su_{i-1}$ and $\deg(s) = 0$, we get $\deg(u_{i+1}) = \deg(ru_i) = \deg(r) + \deg(u_i) > \deg(u_i)$. By induction, one proves immediately that for $m > i$

$$\deg(u_m) = (m-i)\deg(r) + \deg(u_i), \tag{65}$$

and so, in particular, (60) holds with $C_{31} := \deg(r)$ and $C_{32} := C_{28}(C_{28}+1) > i\deg(r)$. It remains to prove the existence of such an index i. But if

$$\deg(r) + \deg(u_i) = \deg(ru_i) \leq \deg(u_{i-1}) \tag{66}$$

for all $i = 0, 1, \ldots, j$, where $j := C_{28} + 1$, then, by summing up (66) for $i = 1, \ldots, j$, we get

$$\deg(u_j) \leq \deg(u_0) - j\deg(r) < \deg(u_0) - C_{28} < 0,$$

which is impossible.

Having now proved (60), we conclude at least that the inequality (20) which is claimed by our Theorem 5 is non-void. We now have enough facts about the general term u_m of our binary recurrent sequence of polynomials to be able to prove that u_m has primitive divisors for large m and that inequality (20) does indeed hold.

We denote by Q the polynomial $Q := s(cd)(r^2+4s)u_0$, and we write

$$B(m) := C(m)D(m), \tag{67}$$

where

$$C(m) := \prod_{\substack{p \mid B(m)\\ p \mid Q}} p \quad \text{and} \quad D(m) := \prod_{\substack{p \mid B(m)\\ p \nmid Q}} p. \tag{68}$$

Clearly, $\deg(C(m)) \leq \deg(Q) \leq C_{34}$, where

$$C_{34} := 4C_{28} + C_{27} \geq \deg(cd) + \deg(s) + \deg(r^2+4s) + \deg(u_0).$$

It suffices to look for the prime divisors p of $D(m)$ which are not primitive for u_m. Notice that by (60) we know that

$$\deg(D(m)) \geq \deg(u_m) - \deg(A(m)) - \deg(C(m)) \geq C_{31}m - C_{35}$$

with $C_{35} := C_{26} + C_{34}$, and, in particular, the degree of $D(m)$ increases linearly in m for large m. Let p be a prime divisor of $D(m)$ which is not primitive for u_m. Then there exists $m_1 < m$ such that $p \mid u_{m_1}$. Since p does not divide $cds(r^2 + 4s)$, it must divide the $(m - m_1)$th term L_{m-m_1} of the Lucas sequence of polynomials with rational coefficients given by

$$L_n := \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{for } n = 0, 1, \ldots \tag{69}$$

From the well-known divisibility properties of the Lucas sequence $(L_n)_{n \geq 0}$, it follows that there exists a positive integer $l < m$ such that $p \mid L_l$ and such that l is minimal with this property. In particular,

$$p \mid \Phi_l(\alpha, \beta), \tag{70}$$

where for a positive integer n we use the notation $\Phi_n(X, Y) \in \mathbb{Q}[X, Y]$ for the homogenization of the cyclotomic polynomial $\Phi_n(X) \in \mathbb{Q}[X]$. It is easy to see that $\Phi_n(\alpha, \beta)$ is a non-constant polynomial in $\mathbb{Q}[X]$. Moreover, since $p \mid u_m$, $p \nmid Q$ but $p \mid \Phi_l(\alpha, \beta)$, there exists a unique positive integer $k < l$ such that $p \mid u_k$. In particular, $p \mid u_k$ and $p \mid u_{k+l}$, and we conclude that $p \mid D(k + l, k)$, where $D(k + l, k)$ is the greatest common divisor of u_{k+l} and u_k which is free of primes dividing *scd*. An analogue of Theorem 1 to the polynomial setting can be easily formulated and proved to hold, and it yields

$$\deg(D(k + l, k)) \leq C_{36} \sqrt{k + l} \leq C_{37} \sqrt{l}, \tag{71}$$

where C_{36} depends only on C_{28} and $C_{37} := \sqrt{2}\, C_{36}$. In particular, we get

$$\deg(p) \leq C_{37} \sqrt{l}. \tag{72}$$

We now show that

$$\deg(p) \geq \phi(l)/2. \tag{73}$$

To see this, pick x to be any root of the irreducible polynomial p and set $\mathbb{K}_x := \mathbb{Q}[x]$. Clearly, $d_{\mathbb{K}_x} = [\mathbb{K}_x : \mathbb{Q}] = \deg(p)$. From (70), it follows that $\Phi_l(\alpha, \beta)(x) = 0$, therefore there exists a primitive root of unity ζ of order d such that

$$\alpha(x) - \zeta\beta(x) = 0. \tag{74}$$

If $\mathbb{K} = \mathbb{Q}(X)$, then α/β is a non-constant element of $\mathbb{Q}(X)$, and since p is coprime to Q we see that $s(x) = -\alpha(x)\beta(x) \neq 0$. Relation (74) now implies that

$$\zeta = \frac{\alpha(x)}{\beta(x)} \in \mathbb{K}_x,$$

therefore $\mathbb{K}_x$ contains the cyclotomic field $\mathbb{Q}[\zeta]$. In particular,

$$\deg(p) = d_{\mathbb{K}_x} \geq [\mathbb{Q}[\zeta] : \mathbb{Q}] = \phi(l),$$

which is a better inequality than (73). Assume now that $d_{\mathbb{K}} = 2$. Then (74) implies that

$$(\alpha(x) - \zeta\beta(x))(\beta(x) - \zeta\alpha(x)) = 0,$$

and since $\alpha(x)\beta(x) = -s(x) \neq 0$, we may write the above equation as

$$\zeta^2 - \frac{\alpha(x)^2 + \beta(x)^2}{\alpha(x)\beta(x)}\,\zeta + 1 = 0,$$

and both $\alpha(x)^2+\beta(x)^2 = r(x)^2+2s(x)$ and $\alpha(x)\beta(x) = -s(x)$ belong to $\mathbb{K}_x$. Thus, ζ satisfies an algebraic equation of degree 2 over $\mathbb{K}_x$, and since the degree of ζ over $\mathbb{Q}$ is precisely $\phi(l)$, we get inequality (73). Putting together (72) and (73), we get

$$\phi(l) \leq C_{38}\sqrt{l}, \tag{75}$$

where $C_{38} := 2C_{37}$. But it is well known that there exists an absolute constant C_{39} such that

$$\phi(n) > C_{39}\,\frac{n}{\log\log n} \tag{76}$$

for all positive integers $n > 1$. The combination of (75) and (76) gives

$$C_{39}\,\frac{l}{\log\log l} \leq C_{38}\,\sqrt{l}$$

and we get

$$l < C_{40}.$$

In particular, $k < C_{40}$, and any non-primitive prime divisor p of u_m dividing $D(m)$ divides

$$\prod_{1\leq k<C_{40}} u_k. \tag{77}$$

We finally set C_{41} to be an upper bound for the degree of the polynomial (77), and $C_{20} := C_{35} + C_{41}$, and notice that the above arguments imply that inequality (20) does hold with this constant C_{20}. The fact that the polynomial $\mathrm{Prim}(u_m)$ is non-constant for large m is a consequence of (20) and (70). This case is therefore settled.

Case 2: *α/β is constant.* In this case, we shall first show that α and β are both constants. Indeed, with $\gamma := \alpha/\beta$ we know that $\gamma \neq \pm 1$, and $\alpha = \frac{\gamma}{1+\gamma}r$ and $\beta = \frac{1}{1+\gamma}r$. In particular, $s = \alpha\beta = \frac{\gamma}{(1+\gamma)^2}r^2$, therefore the constant $\gamma/(1+\gamma)^2 = s/r^2$ is rational. Since we are assuming that r and s are coprime, both r and s are rational constants. So, α and β are both constants. We let Δ be the greatest common denominator of r and s, and we replace the pair (r, s) by $(\Delta r, \Delta^2 s)$, and the recurrent sequence $(u_n)_{n\geq 0}$ by $(\Delta^n u_n)_{n\geq 0}$. After this replacement, the two roots α and β of the characteristic equation (2) of our binary recurrent sequence of polynomials $(u_n)_{n\ge 0}$ become algebraic integers. We introduce the sequences of

$$(78) \qquad L_n := \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad L'_n := \alpha^n + \beta^n \qquad \text{for } n = 0, 1, \ldots,$$

and let c_1 and d_1 be the two polynomials in $\mathbb{Q}[X]$ such that

$$(79) \qquad u_n = c_1 L_n + d_1 L'_n$$

for all $n \ge 0$. It is a straightforward computation to verify that the pair (c_1, d_1) is related to (c, d) via

$$(80) \qquad c_1 = \frac{(c-d)(\alpha - \beta)}{2} \quad \text{and} \quad d_1 = \frac{c+d}{2}.$$

Since c/d is not constant, it follows that $c_1 d_1 \neq 0$ and c_1/d_1 is not a constant either. By replacing $(u_n)_{n\ge 0}$ by $(u_n/\lambda)_{n\ge 0}$, where $\lambda := \gcd(c_1, d_1)$, we may assume that c_1 and d_1 are coprime. Clearly, none of them is zero, and at least one of them is non-constant. We now show that $\deg(u_m) = \max(\deg(c_1), \deg(d_1))$ for large m. This is obvious if $\deg(c_1) \neq \deg(d_1)$. So, we assume that $\deg(c_1) = \deg(d_1) = \delta$, and we let μ_1 and ν_1 be the leading coefficients of c_1 and d_1, respectively. Then $\deg(u_m) < \delta$ precisely when

$$(81) \qquad \mu_1 L_m + \nu_1 L'_m = 0.$$

But it is easy to see that the binary recurrent sequence of integers $(v_n)_{n\ge 0}$ given by

$$(82) \qquad v_n := \mu_1 L_n + \nu_1 L'_n \qquad \text{for } n = 0, 1, \ldots$$

is non-degenerate, and therefore there exists a constant C_{42} such that $v_m \neq 0$ for $m > C_{42}$. In particular, u_m is not constant for $m > C_{42}$.

We now show that every prime divisor of u_m is primitive when $m > C_{42}$. Indeed, assume that this were not so and pick a prime divisor p of u_m such that there exists $n < m$ for which p divides u_n. We set $X := c_1$, $Y := d_1$ and notice that the divisibility relations $p \mid u_m$ and $p \mid u_n$ lead to the homogeneous linear system

$$(83) \qquad \begin{cases} L_m X + L'_m Y \equiv 0 \pmod{p}, \\ L_n X + L'_n Y \equiv 0 \pmod{p}, \end{cases}$$

in the field $\mathbb{Q}[X]/p$ which has the non-zero solution (X, Y) modulo p (this solution (X, Y) is indeed non-zero modulo p because $X = c_1$ and $Y = d_1$ are coprime polynomials). In particular, p must divide the determinant $L_m L'_n - L'_m L_n$ of the coefficient matrix of the above system, and since this determinant is an integer (i.e., a constant), it must be zero. Hence,

$$L_m L'_n = L_n L'_m,$$

which is easily seen to be equivalent to

$$\left(\frac{\alpha}{\beta}\right)^{m-n} = 1,$$

with $m-n>0$, contradicting the fact that α/β is not a root of 1. This case is therefore settled as well and the proof of our Theorem 5 is complete.

Acknowledgements. I would like to express my deep thanks to the anonymous referee and to Professors A. Pethő, I. Shparlinski and C. L. Stewart for their valuable comments on a previous version of the manuscript and for pointing out to me some bibliographical references. Special thanks are due to Professor A. Schinzel who supplied the second part of the present proof of Theorems 2 and 4 improving on my original proof of these results which was a lot longer. This work was partially supported by the grants SEP-CONACYT 37259-E and 37260-E.

References

[1] Y. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. 539 (2001), 75–122.

[2] Yu. F. Bilu and R. F. Tichy, *The Diophantine equation* $f(x) = g(y)$, Acta Arith. 95 (2000), 261–288.

[3] Y. Bugeaud, P. Corvaja and U. Zannier, *An upper bound for the GCD of* a^n-1 *and* b^n-1, preprint, 2001.

[4] A. Dujella and R. F. Tichy, *Diophantine equations for second-order recursive sequences of polynomials*, Quart. J. Math. 52 (2001), 161–169.

[5] P. Erdős and T. N. Shorey, *On the greatest prime factor of* 2^p-1 *for a prime* p *and other expressions*, Acta Arith. 30 (1976), 257–265.

[6] L. K. Hung and K. R. Yu, *On binary recurrence sequences*, Indag. Math. (N.S.) 6 (1995), 341–354.

[7] F. Luca, *Divisibility properties of binary recurrence sequences*, ibid. 12 (2001), 353–367.

[8] R. C. Mason, *Equations over function fields*, in: Lecture Notes in Math. 1068, Springer, Berlin, 1984, 149–157.

[9] J. L. Nicolas, *Petites valeurs de la fonction d'Euler*, J. Number Theory 17 (1983), 375–388.

[10] A. Pethő, *On the greatest prime factor and divisibility properties of linear recursive sequences*, Indag. Math. (N.S.) 1 (1990), 85–93.

[11] A. Schinzel, *Primitive divisors of the expression* A^n-B^n *in algebraic number fields*, J. Reine Angew. Math. 268/269 (1974), 27–33.

[12] —, *An extension of the theorem on primitive divisors in algebraic number fields*, Math. Comp. 61 (1993), 441–444.

[13] T. N. Shorey and C. L. Stewart, *On divisors of Fermat*, *Fibonacci*, *Lucas and Lehmer numbers II*, J. London Math. Soc. 23 (1981), no. 2, 17–23.

[14] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, 1986.

[15] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys-Math. Kl. 1929, no. 1, 70 pp.

[16] C. L. Stewart, *The greatest prime factor of* $a^n - b^n$, Acta Arith. 26 (1975), 427–433.

[17] —, *Divisor properties of arithmetical sequences*, Ph.D. thesis, University of Cambridge, 1976.

[18] —, *On divisors of Fermat*, *Fibonacci*, *Lucas and Lehmer numbers*, Proc. London Math. Soc. 35 (1977), 425–447.

[19] —, *Primitive divisors of Lucas and Lehmer numbers*, in: Transcendence Theory: Advances and Applications, Academic Press, London, 1977, 79–92.

[20] —, *On divisors of terms of linear recurrence sequences*, J. Reine Angew. Math. 333 (1982), 12–31.

[21] —, *On the greatest prime factor of terms of linear recurrence sequences*, Rocky Mountain J. Math. 15 (1985), 599–607.

[22] K. Yu, *Linear forms in p-adic logarithms*, Compositio Math. 91 (1994), 241–276.

Mathematical Institute, UNAM
Ap. Postal 61-3 (Xangari), CP 58 089
Morelia, Michoacán, Mexico
E-mail: fluca@matmor.unam.mx

Received on 4.3.2002
and in revised form on 31.7.2002 (4241)