ON PRIME FACTORS OF TERMS OF BINARY RECURRENCE SEQUENCES

C.L. STEWART

In memory of Professor Andrzej Schinzel

ABSTRACT. We establish estimates from below for the greatest prime factor of the n-th term of a non-degenerate binary recurrence sequence when the sequence belongs to a class of sequences which includes the Lucas sequences.

1. INTRODUCTION

Let r and s be integers with $r^2 + 4s \neq 0$. Let u_0 and u_1 be integers and put

$$u_n = ru_{n-1} + su_{n-2}, \tag{1}$$

for $n = 2, 3, \dots$. Then for $n \geq 0$

$$u_n = a\alpha^n + b\beta^n, \tag{2}$$

where α and β are the roots of the characteristic polynomial $x^2 - rx - s$ and

$$a = \frac{u_1 - u_0\beta}{\alpha - \beta}, \qquad b = \frac{u_0\alpha - u_1}{\alpha - \beta} \tag{3}$$

when $\alpha \neq \beta$. The sequence of integers $(u_n)_{n=0}^{\infty}$ is a binary recurrence sequence. It is said to be non-degenerate if $ab\alpha\beta \neq 0$ and α/β is not a root of unity.

In 1934 Mahler [14] proved that if u_n is the n-th term of a non-degenerate binary recurrence sequence then the greatest prime factor of u_n tends to infinity with n. His proof was ineffective however since it depended on a p-adic version of the Thue-Siegel theorem. In 1967 Schinzel [18] refined work of Gelfond on estimates for linear forms in the logarithms of two algebraic numbers and as a consequence he was able to give an effective lower bound. For any integer m let $P(m)$ denote the greatest prime factor of m with the convention that $P(0) = P(\pm 1) = 1$. Schinzel proved that there exists a

1991 *Mathematics Subject Classification.* Primary 11B37; Secondary 11J86.
Key words and phrases. binary recurrence sequences, linear forms in logarithms.

positive number C_0 which is effectively computable in terms of a, b, α and β such that

$$P(u_n) > C_0 n^{c_1} (\log n)^{c_2},$$

where

$$(c_1, c_2) = \begin{cases} (1/84, 7/12) & \text{if } \alpha \text{ and } \beta \text{ are integers} \\ (1/133, 7/19) & \text{otherwise.} \end{cases}$$

The above result was subsequently improved by Stewart [22], by Yu and Hung [26] and in 2013 by Stewart [24] who showed that there is a positive number C, which is effectively computable in terms of a, b, α and β such that if n exceeds C then

$$P(u_n) > n^{1/2} \exp(\log n / 104 \log\log n). \tag{4}$$

Let $(t_n)_{n=0}^{\infty}$ be a non-degenerate binary recurrence sequence with $t_0 = 0$ and $t_1 = 1$. Then, recall (2) and (3),

$$t_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{5}$$

for $n = 0, 1, 2, \ldots$ and the sequence is known as a Lucas sequence. Note that a Lucas sequence is non-degenerate. Lucas sequences have a rich divisibility structure and have been extensively studied, eg. [4], [6], [8], [11], [13], [21] and [27]. In 2013 Stewart [23] proved that if t_n is the n-th term of a Lucas sequence then

$$P(t_n) > n \exp(\log n / 104 \log\log n) \tag{6}$$

provided that n exceeds a number which is effectively computable in terms of α and β, see also [5] and [9].

In 1967 Schinzel [18] introduced a class of binary recurrence sequences which includes the Lucas sequences and whose members have similar divisibility properties to the Lucas sequences. He considered those sequences for which a/b and α/β are multiplicatively dependent and proved that if α and β are real numbers then there is a positive number c, which is effectively computable in terms of a, b, α and β, such that

$$P(u_n) > n - c. \tag{7}$$

Schinzel's proof of (7) depended on a result [17] of his on primitive divisors of Lucas numbers. In 2003 Luca [12] proved (7) in the case when α and β are not real numbers. Observe that if $(u_n)_{n=0}^{\infty}$ is a non-degenerate binary recurrence sequence with a term which is zero then a/b and α/β are multiplicatively dependent.

We shall prove the following result.

Theorem 1. *Let* $(u_n)_{n=0}^{\infty}$ *be a non-degenerate binary recurrence sequence, as in* (2)*, with* a/b *and* α/β *multiplicatively dependent. There exists a positive number* C*, which is effectively computable in terms of* a, b, α *and* β*, such that if* n *exceeds* C *then*

$$P(u_n) > n \exp(\log n/104 \log\log n). \tag{8}$$

The proof of Theorem 1 relies on arguments from [23] as well as the work of Schinzel [19] on primitive divisors in algebraic number fields.

For any non-degenerate binary recurrence sequence $(u_n)_{n=0}^{\infty}$ we are able to improve (4) for all positive integers n except perhaps for a set of asymptotic density zero. Let $\varepsilon(n)$ be a real valued function on the positive integers for which $\lim_{n\to\infty} \varepsilon(n) = 0$. In [22] Stewart proved that for all positive integers, except perhaps for a set of asymptotic density zero,

$$P(u_n) > \varepsilon(n) n \log n;$$

see the papers of Murty, Séguin and Stewart [16] and Balaji and Luca [3] for related work. Combining the approaches of [22] and [23] we are able to prove the following result.

Theorem 2. *Let* $(u_n)_{n=0}^{\infty}$ *be a non-degenerate binary recurrence sequence. For all positive integers* n*, except perhaps a set of asymptotic density zero,*

$$P(u_n) > n \exp(\log n/104 \log\log n). \tag{9}$$

The proofs of Theorem 1 and Theorem 2 ultimately depend on an estimate for p-adic linear forms in the logarithms of algebraic numbers due to Yu [25] and, as discussed in [23], the constant 104 which appears in our estimates has no arithmetical significance but instead is a consequence of the bounds in [25]. For a more detailed historical account of these topics see [24].

2. Cyclotomic polynomials

Let r and s be integers. We denote the greatest common divisor of r and s by (r, s). For each positive integer k put $\zeta_k = e^{2\pi i/k}$. Let n be a positive integer. The n-th cyclotomic polynomial $\Phi_n(x, y)$ is given by

$$\Phi_n(x, y) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} (x - \zeta_n^j y). \tag{10}$$

Let e be a positive integer and let i be an integer. Put

$$\Phi_{n,e}^{(i)}(x,y) = \prod_{\substack{j=1 \\ (j,ne)=1 \\ j\equiv i \bmod e}}^{ne} (x - \zeta_{ne}^{j} y). \tag{11}$$

Note that if $(i,e) > 1$ then $\Phi_{n,e}^{(i)}(x,y) = 1$ and that

$$\prod_{\substack{i=1 \\ (i,e)=1}}^{e} \Phi_{n,e}^{(i)}(x,y) = \Phi_{ne}(x,y). \tag{12}$$

We remark that when $(i,e) = 1$ the degree of $\Phi_{n,e}^{(i)}(x,y)$ is $\phi(ne)/\phi(e)$ where $\phi()$ denotes Euler's totient function.

For any integer i we have

$$\prod_{\substack{j=1 \\ j\equiv i \bmod e}}^{ne} (x - \zeta_{ne}^{j} y) = x^n - \zeta_e^i y^n \tag{13}$$

and so by the inclusion-exclusion principle, see also Lemma 4 of [19], when $(i,e) = 1$

$$\Phi_{n,e}^{(i)}(x,y) = \prod_{\substack{m|n \\ (m,e)=1 \\ \overline{m}m\equiv i \bmod e}} (x^{n/m} - \zeta_e^{\overline{m}} y^{n/m})^{\mu(m)}. \tag{14}$$

It follows from (14) that $\Phi_{n,e}^{(i)}(x,y)$ has coefficients in $\mathbb{Q}(\zeta_e)$ and then from (11) that the coefficients of $\Phi_{n,e}^{(i)}(x,y)$ are from $\mathbb{Z}[\zeta_e]$, the ring of algebraic integers of $\mathbb{Q}(\zeta_e)$.

Next we put

$$\Psi_{n,e}^{(i)}(x,y) = \prod_{\substack{j=1 \\ (j,ne)>1 \\ j\equiv i \bmod e}}^{ne} (x - \zeta_{ne}^{j} y). \tag{15}$$

By (13) we have

$$\Phi_{n,e}^{(i)}(x,y)\Psi_{n,e}^{(i)}(x,y) = x^n - \zeta_e^i y^n. \tag{16}$$

Since $\Phi_{n,e}^{(i)}(x,y)$ is in $\mathbb{Z}[\zeta_e][x,y]$ we see from (15) and (16) that $\Psi_{n,e}^{(i)}(x,y)$ is also in $\mathbb{Z}[\zeta_e][x,y]$.

3. Divisibility of values of the cyclotomic polynomial and of Lucas numbers

We first record two results describing the arithmetical character of values of the cyclotomic polynomial. Observe that $\Phi_n(\alpha,\beta)$ is an integer for $n > 2$ if $(\alpha+\beta)^2$ and $\alpha\beta$ are integers, see for example p.428 of [21].

Lemma 3. *Suppose that* $(\alpha+\beta)^2$ *and* $\alpha\beta$ *are coprime non-zero integers and that* α/β *is not a root of unity. If* $n > 4$ *and* $n \neq 6, 12$ *then* $P(n/(3,n))$ *divides* $\Phi_n(\alpha,\beta)$ *to at most the first power. All other prime factors of* $\Phi_n(\alpha,\beta)$ *are congruent to* $\pm 1 \pmod{n}$.

Proof. This is Lemma 6 of [21]. □

Our next result follows from the proof of Theorem 1.1 of [23]. Note that we do not require $(\alpha+\beta)^2$ and $\alpha\beta$ to be coprime.

Lemma 4. *Let* α *and* β *be complex numbers such that* $(\alpha+\beta)^2$ *and* $\alpha\beta$ *are non-zero integers and* α/β *is not a root of unity. There exists a positive number* C*, which is effectively computable in terms of* α *and* β*, such that for* $n > C$,

$$P(\Phi_n(\alpha,\beta)) > n \exp(\log n / 103.95 \log\log n). \tag{17}$$

Proof. This follows from the second last line in the proof of Theorem 1.1 of [23]. □

For any non-zero rational number x let $\operatorname{ord}_p x$ denote the p-adic order of x.

Lemma 5. *Let* $(u_n)_{n=0}^{\infty}$ *be a non-degenerate binary recurrence sequence as in* (2) *with* a/b *and* α/β *multiplicatively independent. There exists a positive number* C *which is effectively computable in terms of* a, b, α *and* β *such that if* p *exceeds* C *then*

$$\operatorname{ord}_p u_n < p \exp(-\log p / 51.9 \log\log p) \log n.$$

Proof. This is Lemma 7 of [24]. □

We shall now describe the prime decomposition of terms of a Lucas sequence $(t_n)_{n=0}^{\infty}$.

Lemma 6. *Let* $(t_n)_{n=0}^{\infty}$ *be a Lucas sequence as in* (5)*. If* p *is a prime number which does not divide* $\alpha\beta$ *then* p *divides* t_n *for some positive integer* n *and if* l *is the smallest positive integer for which* p *divides* t_l *then*

$$l \leq p+1.$$

Proof. This follows, for example, from Lemma 7 of [22]. □

For any rational number x let $|x|_p$ denote the p-adic value of x, normalized so that $|p|_p = p^{-1}$.

Lemma 7. *Let $\{t_n\}_{n=0}^{\infty}$ be a Lucas sequence, as in (5), with $\alpha+\beta$ and $\alpha\beta$ coprime. Let p be a prime number which does not divide $\alpha\beta$, let l be the smallest positive integer for which p divides t_l and let n be a positive integer. If l does not divide n, then*

$$|t_n|_p = 1.$$

If $n = lk$ for some positive integer k, we have, for $p > 2$,

$$|t_n|_p = |t_l|_p \, |k|_p \, ,$$

while for $p = 2$,

$$|t_n|_2 = \begin{cases} |t_l|_2 & \text{for } k \text{ odd} \\ 2\,|t_{2l}|_2\,|k|_2 & \text{for } k \text{ even.} \end{cases}$$

Proof. This is Lemma 8 of [22] . □

Lemma 8. *Let $\{t_n\}_{n=0}^{\infty}$ be a Lucas sequence, as in (5), with $\alpha+\beta$ and $\alpha\beta$ coprime and $|\alpha| \geq |\beta|$. Let n be an integer larger than 1. There exists a positive number C, which is effectively computable in terms of α and β, such that if p is a prime number larger than C then*

$$\operatorname{ord}_p t_n < p \exp(-\log p / 51.9 \log\log p) \log|\alpha| \log n.$$

Proof. We may suppose that C exceeds $|\alpha\beta|$ and the absolute value of the discriminant of $\mathbb{Q}(\alpha/\beta)$. The result then follows from Lemma 4.3 of [23]. □

4. Cyclotomic polynomials at algebraic points in quadratic cyclotomic extensions

Let θ_1 and θ_2 be non-zero algebraic integers in $\mathbb{Q}(\zeta_e)$ with e equal to $3, 4$ or 6 and suppose that θ_1/θ_2 is not a root of unity and that $\theta_1 = \overline{\theta}_2$. Then θ_1 and θ_2 are algebraic conjugates. Put

$$g = ((\theta_1+\theta_2)^2, \theta_1\theta_2),$$

and

$$\lambda_1 = \theta_1/\sqrt{g}, \lambda_2 = \theta_2/\sqrt{g}.$$

Note that

$$(x-\lambda_1)(x+\lambda_1)(x-\lambda_2)(x+\lambda_2) = x^4 - ((\theta_1+\theta_2)^2/g - 2\theta_1\theta_2/g)x^2 - (\theta_1\theta_2/g)^2$$

is a polynomial with integer coefficients and thus λ_1 and λ_2 are algebraic integers. Further λ_1 is of degree 2 over $\mathbb{Q}$ with conjugate λ_2 when g is a perfect square and is of degree 4 over $\mathbb{Q}$ with conjugates $\lambda_1, -\lambda_1, \lambda_2, -\lambda_2$ when g is not a perfect square. Since $\theta_1/\theta_2 = \lambda_1/\lambda_2$ is not a root of unity we see that λ_1 is not a root of unity. In both cases the conjugates of λ_1 have the same absolute value as λ_1 and, since λ_1 is not a root of unity,

$$|\lambda_1| \geq 2^{1/4}, \tag{18}$$

as is readily checked. Furthermore, since $\theta_1 = \overline{\theta}_2$ we find that $\overline{\lambda_1/\lambda_2} = \lambda_2/\lambda_1$ and as λ_1/λ_2 is not a root of unity it is an algebraic number of degree at least 2. In fact it has conjugate λ_2/λ_1 and minimal polynomial

$$\lambda_1\lambda_2 x^2 - (\lambda_1^2 + \lambda_2^2)x - \lambda_1\lambda_2.$$

For any algebraic number α let $M(\alpha)$ denote the Mahler measure of α, see [7]. We then have

$$M(\lambda_1/\lambda_2) = M(\lambda_2/\lambda_1) = |\lambda_1\lambda_2| \max(1, |\lambda_1/\lambda_2|) \max(1, |\lambda_2/\lambda_1|) = |\lambda_1|^2. \tag{19}$$

Lemma 9. *Let n be a positive integer and ζ an e-th root of unity with e equal to $3, 4$ or 6. There exists an effectively computable positive number c_1 such that*

$$n \log|\lambda_1| - c_1 \log(n+1) \log|\lambda_1| \leq \log|\lambda_1^n - \zeta\lambda_2^n| \leq n \log|\lambda_1| + \log 2.$$

Proof. Note that

$$\log|\lambda_1^n - \zeta\lambda_2^n| = n\log|\lambda_1| + \log|\zeta(\lambda_2/\lambda_1)^n - 1|$$

Since $\theta_1 = \overline{\theta}_2$ we see that $|\lambda_2/\lambda_1| = 1$ and so $|\zeta(\lambda_2/\lambda_1)^n - 1| \leq 2$. It remains to establish a lower bound for $|\zeta(\lambda_2/\lambda_1)^n - 1|$. For any complex number z, either $1/4 \leq |e^z - 1|$ or

$$|z - ib\pi| \leq 4|e^z - 1|$$

for some integer b, see page 176 of [1]. Let $z = \log\zeta + n\log(\lambda_2/\lambda_1)$ where we take the principal value of the logarithms. Then either

$$|\zeta(\lambda_2/\lambda_1)^n - 1| \geq 1/4 \tag{20}$$

or

$$4|\zeta(\lambda_2/\lambda_1)^n - 1| \geq \min_{b\in\mathbb{Z}} |\log\zeta + n\log(\lambda_2/\lambda_1) - b\pi i|.$$

Suppose that the minimum occurs at b_0. Then $|b_0| \leq n+1$. Further

$$\log\zeta - b_0\pi i = b_1 \log\zeta_{12}$$

with $|b_1| \leq 6(|b_0|+1) \leq 6n + 12$ and thus if (20) does not hold then

$$4|\zeta(\lambda_2/\lambda_1)^n - 1| \geq |n\log(\lambda_2/\lambda_1) + b_1\log\zeta_{12}|. \tag{21}$$

Let $c_1, c_2, \ldots$ denote effectively computable positive numbers. This is a linear form in two logarithms and by [10], [2] or [15] we see from (20) and (21), since λ_2/λ_1 is not a root of unity, that

$$\log|\zeta(\lambda_2/\lambda_1)^n - 1| > -c_2 \log(n+1) \log \max(4, A) \tag{22}$$

where A is the Mahler measure of λ_2/λ_1. Thus, by (18) and (19),

$$\max(4, A) \leq |\lambda_1|^{c_3}$$

hence, from (22),

$$\log|\zeta(\lambda_2/\lambda_1)^n - 1| > -c_4 \log(n+1) \log|\lambda_1|$$

and our result follows. □

For any positive integer n let $\omega(n)$ denote the number of distinct prime factors of n and put $q(n) = 2^{\omega(n)}$.

Lemma 10. *Let e be $3, 4$ or 6 and let i be an integer coprime with e. There exists an effectively computable positive number c such that if $n > 2$ then*

$$(\phi(ne)/\phi(e) - cq(n)\log n)\log|\lambda_1| \leq \log|\Phi_{n,e}^{(i)}(\lambda_1, \lambda_2)|$$

and

$$\log|\Phi_{n,e}^{(i)}(\lambda_1, \lambda_2)| \leq (\phi(ne)/\phi(e) + cq(n)\log n)\log|\lambda_1|.$$

Proof. By (14)

$$\log|\Phi_{n,e}^{(i)}(\lambda_1, \lambda_2)| = \sum_{\substack{m|n \\ (m,e)=1 \\ \overline{m}m \equiv i \bmod e}} \mu(m) \log|\lambda_1^{n/m} - \zeta_e^{\overline{m}} \lambda_2^{n/m}|$$

and so, by Lemma 9,

$$\Big|\log|\Phi_{n,e}^{(i)}(\lambda_1, \lambda_2)| - \sum_{\substack{m|n \\ (m,e)=1}} \mu(m)(n/m)\log|\lambda_1|\Big| \leq \sum_{\substack{m|n \\ (m,e)=1 \\ \mu(m)\neq 0}} c_1 \log(n+1)\log|\lambda_1|.$$

The result now follows. □

Lemma 11. *Let e be $3, 4$ or 6 and let i be an integer coprime with e. There exists an effectively computable positive number C such that if n exceeds C then*

$$\log|\Phi_{n,e}^{(i)}(\lambda_1, \lambda_2)| > (\phi(ne)/2\phi(e))\log|\lambda_1|.$$

Proof. For n sufficiently large

$$\phi(n) > n/(2\log\log n)$$

and

$$q(n) < n^{1/\log\log n}$$

and so by (18) the result follows from Lemma 10.

□

Lemma 12. *Let e be $3, 4$ or 6 and let p be a prime number. There exists a positive number C, which is effectively computable in terms of a, b, α and β, such that for $n > C$*

$$\operatorname{ord}_p \Phi_{ne}(\lambda_1, \lambda_2) < p \exp(-\log p/51.9 \log\log p) \log|\lambda_1| \log ne.$$

Proof. This follows from (5.3) and (5.4) of [23]. □

Lemma 13. *Let e be $3, 4$ or 6 and let i be 1 or -1. There exists a positive number C, which is effectively computable in terms of θ_1 and θ_2, such that if m exceeds C then there is an irreducible π in $\mathbb{Z}[\zeta_e]$ which divides*

$$\theta_1^m - \zeta_e^i \theta_2^m$$

in $\mathbb{Z}[\zeta_e]$ which is either a rational prime p or is such that $\pi\overline{\pi} = p$ and, in both cases,

$$p > m \exp(\log m/103.95 \log\log m).$$

Proof. Let $c_1, c_2, \ldots$ denote positive numbers which are effectively computable in terms of θ_1 and θ_2. From Section 2 we see that $\Phi_{m,e}^{(i)}(x, y)$ is a polynomial with coefficients in $\mathbb{Z}[\zeta_e]$. Thus $\Phi_{m,e}^{(i)}(\theta_1, \theta_2)$ is in $\mathbb{Z}[\zeta_e]$ and, by (16), $\Phi_{m,e}^{(i)}(\theta_1, \theta_2)$ divides $\theta_1^m - \zeta_e^i \theta_2^m$ in $\mathbb{Z}[\zeta_e]$. By (12)

$$\Phi_{m,e}^{(1)}(\theta_1, \theta_2)\Phi_{m,e}^{(-1)}(\theta_1, \theta_2) = \Phi_{me}(\theta_1, \theta_2)$$

and therefore

$$\Phi_{m,e}^{(1)}(\lambda_1, \lambda_2)\Phi_{m,e}^{(-1)}(\lambda_1, \lambda_2) = \Phi_{me}(\lambda_1, \lambda_2). \tag{23}$$

Notice that $\Phi_{m,e}^{(j)}(\lambda_1, \lambda_2) = g^{-\phi(me)/2\phi(e)}\Phi_{m,e}^{(j)}(\theta_1, \theta_2)$ for $j = \pm 1$. Since $\Phi_{m,e}^{(j)}(\theta_1, \theta_2)$ is in $\mathbb{Z}[\zeta_e]$ and $\Phi_{m,e}^{(j)}(\lambda_1, \lambda_2)$ is an algebraic integer we see that $\Phi_{m,e}^{(j)}(\lambda_1, \lambda_2)$ is in $\mathbb{Z}[\zeta_e]$ for $j = \pm 1$. Therefore if π is an irreducible in $\mathbb{Z}[\zeta_e]$ which divides $\Phi_{m,e}^{(i)}(\lambda_1, \lambda_2)$ then π divides $\Phi_{m,e}^{(i)}(\theta_1, \theta_2)$ and so divides $\theta_1^m - \zeta_e^i \theta_2^m$. We shall now show that $\Phi_{m,e}^{(i)}(\lambda_1, \lambda_2)$ is divisible by an irreducible π which is either a large rational prime or is such that $\pi\overline{\pi}$ is a large rational prime.

Since $(\lambda_1 + \lambda_2)^2$ and $\lambda_1\lambda_2$ are coprime integers $\Phi_{me}(\lambda_1, \lambda_2)$ is an integer for $me > 12$ and, by Lemma 3, $P(me/(3, me))$ divides $\Phi_{me}(\lambda_1, \lambda_2)$ to at most the first power. All other prime factors are congruent to $\pm 1 (\bmod\, me)$. Thus

$$\Phi_{m,e}^{(i)}(\lambda_1, \lambda_2) = \gamma \pi_1^{l_1} \ldots \pi_t^{l_t}$$

where γ is a divisor of $P(me/(3, me))$, $t \geq 0$, $\pi_1, \ldots, \pi_t$ are irreducibles of $\mathbb{Z}[\zeta_e]$ and $l_1, \ldots, l_t$ are positive integers. Note that $t \geq 1$ for $m > c_1$ by Lemma 11. Let P be the largest prime associated with an irreducible π_j. Then, by (23) and Lemma 12,

$$\max_j l_j \leq 2P \exp(-\log P/51.9 \log\log P) \log|\lambda_1| \log me$$

hence

(24)

$$\log|\Phi_{m,e}^{(i)}(\lambda_1, \lambda_2)| \leq \log me + 2tP \log P \exp(-\log P/51.9 \log\log P) \log|\lambda_1| \log me.$$

But $t \leq 2(\pi(P, me, 1) + \pi(P, me, -1))$ and so

$$t \leq 5P/me. \tag{25}$$

Thus by (24) and (25)

(26)

$$\log|\Phi_{m,e}^{(i)}(\lambda_1, \lambda_2)| \leq c_2(P^2 \log P \exp(-\log P/51.9 \log\log P) \log me)/me,$$

and by Lemma 11, for $m > c_3$,

$$\log|\Phi_{m,e}^{(i)}(\lambda_1, \lambda_2)| > (\phi(me)/2\phi(e)) \log|\lambda_1|. \tag{27}$$

Comparing (26) and (27) we find that, for $m > c_4$,

$$me\phi(me)/\log m < c_5 P^2 \log P \exp(-\log P/51.9 \log\log P).$$

Since $\phi(me) > c_6 m/\log\log m$

$$P > m \exp(\log m/103.95 \log\log m)$$

for $m > c_7$ as required.

□

5. Proof of Theorem 1

Put $\mathbb{K} = \mathbb{Q}(\alpha)$ and let $\mathcal{O}_{\mathbb{K}}$ denote the ring of algebraic integers of $\mathbb{K}$. Let w be the smallest positive integer for which wa and wb are algebraic integers. By considering the sequence $(v_n)_{n=0}^{\infty}$ with $v_n = wu_n$ for $n = 0, 1, \ldots$ we see that it suffices to prove our result for sequences $(u_n)_{n=0}^{\infty}$ for which a, b, α and β are algebraic integers. Since a/b and α/β are multiplicatively dependent there exist integers k and l, not both zero, for which

$$(a/b)^k = (\alpha/\beta)^l. \tag{28}$$

By inverting (28) if necessary we may suppose that $k \geq 0$. Notice that $k \neq 0$ since otherwise α/β is a root of unity contrary to the assumption that $(u_n)_{n=0}^{\infty}$ is non-degenerate. Thus $k > 0$.

If $l = 0$ then a/b is a root of unity and we put

$$u_n = a(\theta_1^n - \zeta\theta_2^n) \tag{29}$$

where

$$(\theta_1, \theta_2) = (\alpha, \beta)$$

and ζ is a root of unity from $\mathbb{K}$.

We now suppose that $k > 0$ and $l \neq 0$ and, following Schinzel [18] and Luca [12], we put

$$l_1 = l/(k,l), k_1 = k/(k,l).$$

It follows from (28) that

$$(a/b)^{k_1} = (\alpha/\beta)^{l_1}\zeta \tag{30}$$

where ζ is a root of unity from $\mathbb{K}$. There exists a unique pair of integers (x, y) for which

$$xl_1 + yk_1 = 1 \tag{31}$$

and

$$0 < y \leq |l_1|.$$

Put

$$\rho = a^x\alpha^y/b^x\beta^y.$$

Then, by (31),

$$\rho^{l_1} = (a/b)^{xl_1}(\alpha/\beta)^{yl_1} = (a/b)^{xl_1}(a/b)^{yk_1}\zeta^{-y} = (a/b)\zeta^{-y} \tag{32}$$

and

$$\rho^{k_1} = (a/b)^{xk_1}(\alpha/\beta)^{yk_1} = (\alpha/\beta)^{xl_1}\zeta^x(\alpha/\beta)^{yk_1} = (\alpha/\beta)\zeta^x. \tag{33}$$

Thus

$$(a/b)(\alpha/\beta)^n = \rho^{l_1}\zeta^y\rho^{k_1 n}\zeta^{-xn} = \rho^{l_1+k_1 n}\zeta^{y-xn}.$$

Accordingly

$$u_n = b\beta^n((a/b)(\alpha/\beta)^n + 1)$$

so

$$u_n = b\beta^n\zeta^{y-xn}(\rho^{l_1+k_1 n} + \zeta^{xn-y}),$$

and we find that

$$\theta_2^{l_1+k_1 n}u_n = b\beta^n\zeta^{y-xn}(\theta_1^{l_1+k_1 n} - (-\zeta^{xn-y})\theta_2^{l_1+k_1 n}) \tag{34}$$

where

$$(\theta_1, \theta_2) = (a^x\alpha^y, b^x\beta^y) \tag{35}$$

when $x \geq 0$ and

$$(\theta_1, \theta_2) = (b^{-x}\alpha^y, a^{-x}\beta^y). \tag{36}$$

when $x < 0$. Observe that

$$\theta_1/\theta_2 = \alpha/\beta$$

in case (29) while

$$\theta_1/\theta_2 = \rho$$

in cases (35) and (36). Thus, by (33) and the fact that α/β is not a root of unity we see that in all three cases θ_1/θ_2 is not a root of unity. Furthermore either a, b, α, β are non-zero integers or α and β are algebraic conjugates hence θ_1 and θ_2 are algebraic conjugates. In both cases $\theta_1 + \theta_2$ and $\theta_1\theta_2$ are non-zero integers. Note that in the former case $\mathbb{K} = \mathbb{Q}$ and so the root of unity ζ in (29), and also in (30), is 1 or -1.

If in (29) ζ is 1 then $\Phi_n(\theta_1, \theta_2)$ divides u_n while if ζ is -1 then $\Phi_{2n}(\theta_1, \theta_2)$ divides u_n and in both cases the result follows from Lemma 4. If $l \neq 0$ then (34) holds and $\theta_2^{l_1+k_1n}u_n$ is an algebraic integer in $\mathbb{K}$ which is divisible by $\Phi_{k_1n+l_1}(\theta_1, \theta_2)$ in $\mathcal{O}_{\mathbb{K}}$ if $-\zeta^{xn-y}$ is 1 and is divisible by $\Phi_{2(k_1n+l_1)}(\theta_1, \theta_2)$ in $\mathcal{O}_{\mathbb{K}}$ if $-\zeta^{xn-y}$ is -1. Again the result follows from Lemma 4.

It remains to consider the possibility that ζ in (29) or $-\zeta^{xn-y}$ in (34) is a root of unity in $\mathbb{K}$ different from 1 or -1. Since the degree of $\mathbb{K}$ is at most 2 over $\mathbb{Q}$ we find that the root of unity must be a primitive third, fourth or sixth root of unity and so $\mathbb{K} = \mathbb{Q}(\zeta_e)$ with e equal to $3, 4$ or 6, hence equal to 3 or 4. Notice that $\mathbb{Z}[\zeta_e]$ is the ring of algebraic integers of $\mathbb{Q}(\zeta_e)$ and that $\mathbb{Z}[\zeta_e]$ is a unique factorization domain. Since $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_e)$ we see that α and β and also a and b are complex conjugates hence

$$\theta_1 = \overline{\theta}_2,$$

in all three cases.

Let $c_1, c_2, \ldots$ denote positive numbers which are effectively computable in terms of a, b, α and β. Note that if π is an irreducible in $\mathbb{Z}[\zeta_e]$ which is not a rational prime then $\pi\overline{\pi}$ is a prime p and since u_n is an integer if π divides u_n then p divides u_n. If ζ in (29) is a root of unity different from 1 or -1 then we may apply Lemma 13 with m equal to n to give the result. If $-\zeta^{xn-y}$ in (34) is a root of unity different from 1 or -1 then we may apply Lemma 13 with $m = l_1 + k_1n$. Since $l_1 + k_1n > n/2$ for $n > c_1$ we see that

$$\theta_1^{l_1+k_1n} - (-\zeta^{xn-y})\theta_2^{l_1+k_1n}$$

is divisible by an irreducible π in $\mathbb{Z}[\zeta_e]$ which is either a rational prime p or is such that $\pi\overline{\pi} = p$ and in both cases

$$p > n \exp(\log n/104 \log\log n)$$

for $n > c_2$. By (34) p divides u_n since $b\beta^n\zeta^{y-xn}$ is an algebraic integer and for $n > c_3$ we see that neither π nor $\overline{\pi}$ divides θ_2. The result now follows.

6. Proof of Theorem 2

Let u_n denote the n-th term of a non-degenerate binary recurrence sequence as in (1) and let $g = (r^2, s)$. Let $\mathbb{K} = \mathbb{Q}(\alpha)$ and let $\mathcal{O}_{\mathbb{K}}$ denote the ring of algebraic integers of $\mathbb{K}$. For any θ in $\mathcal{O}_{\mathbb{K}}$ let $[\theta]$ denote the ideal in $\mathcal{O}_{\mathbb{K}}$ generated by θ. Notice that, as in Lemma A.10 of [20],

$$(x - \alpha^2/g)(x - \beta^2/g) = x^2 - ((r^2 + 2s)/g)x + (s/g)^2.$$

Since $(r^2 + 2s)/g$ and s/g are coprime

$$([\alpha^2/g], [\beta^2/g]) = [1].$$

Put

$$v_n = g^{-n} u_{2n} = a(\alpha^2/g)^n + b(\beta^2/g)^n$$

and

$$w_n = g^{-n} u_{2n+1} = a\alpha(\alpha^2/g)^n + b\beta(\beta^2/g)^n$$

for $n = 0, 1, 2, \ldots$.

We shall prove that if $(u_n)_{n=0}^{\infty}$ is a non-degenerate binary recurrence sequence as in (1) with $([\alpha], [\beta]) = [1]$ then for all positive integers n, except perhaps a set of asymptotic density 0,

$$P(u_n) \geq n \exp(\log n / 103.95 \log\log n). \tag{37}$$

Since $(n/2) - 1 \geq n/3$ for $n \geq 6$ and

$$(n/3) \exp(\log(n/3)/103.95 \log\log(n/3)) > n \exp(\log n / 104 \log\log n)$$

for n sufficiently large we see that this suffices to prove our result in general on considering the non-degenerate binary recurrence sequences $(v_n)_{n=0}^{\infty}$ and $(w_n)_{n=0}^{\infty}$ in place of $(u_n)_{n=0}^{\infty}$.

Let $c_1, c_2, \ldots$ denote positive numbers which are effectively computable in terms of a, b, α and β. By Theorem 1 it suffices to prove our result under the additional assumption that a/b and α/β are multiplicatively independent. Further we may assume, without loss of generality, that $|\alpha| \geq |\beta|$.

To establish (37) we shall assume that there is a positive number δ such that

$$P(u_m) < m \exp(\log m / 103.95 \log\log m), \tag{38}$$

for a set of integers m of positive upper density δ and we shall show that this leads to a contradiction. Accordingly, we can find arbitrarily large integers n such that between n and $2n$ there are at least $\delta n/2$ integers m which satisfy (38). Fix such an integer n and denote the set of these integers by M. Put

$$T = 2n \exp(\log 2n/103.95 \log\log 2n), \tag{39}$$

and for each prime number p less than T let $u_{m(p)}$ be the term with $n \le m(p) \le 2n$ which is divisible by the highest power of p; if more than one term is divisible by p raised to the largest exponent then denote the one with least index by $u_{m(p)}$.

It is proved on page 24 of [22] that, for n sufficiently large, at most 3 of the integers m with $n \le m \le 2n$ satisfy

$$|u_m| < |\alpha|^{3m/4}.$$

Further, since u_m is non-zero for m sufficiently large, we see that

$$\log |\prod_{m \in M} u_m| > \frac{\delta n^2}{4} \log |\alpha| \tag{40}$$

for n sufficiently large.

Put

$$S(p) = \frac{u_n \dots u_{2n}}{u_{m(p)}}.$$

Clearly

$$|\prod_{m\in M} u_m| \le \prod_{p<T} |u_{m(p)}|_p^{-1} |S(p)|_p^{-1}. \tag{41}$$

By Lemma 5, for $p > c_1$

$$\log |u_{m(p)}|_p^{-1} < p \log p \exp(-\log p/51.9 \log\log p) \log 2n. \tag{42}$$

Further, for $p \le c_1$

$$\log |u_{m(p)}|_p^{-1} < \max_{n \le m \le 2n} \log |u_m| < 4n \log |\alpha| \tag{43}$$

for n sufficiently large. Thus

$$\sum_{p<T} \log |u_{m(p)}|_p^{-1} \le \sum_{p \le c_1} \log |u_{m(p)}|_p^{-1} + \sum_{c_1 < p < T} \log |u_{m(p)}|_p^{-1}$$

and by (42) and (43)

$$\sum_{p<T} \log |u_{m(p)}|_p^{-1} \le c_2 n + \pi(T) T \log T \exp(-\log T/51.9 \log\log T) \log 2n.$$

Therefore, by (39), for n sufficiently large

$$\sum_{p<T} \log |u_{m(p)}|_p^{-1} < n^2 \exp(-\log n/40{,}000 \log\log n). \tag{44}$$

It remains to estimate $\prod_{p<T} |S(p)|_p^{-1}$.

Let p be a prime which divides $\alpha\beta$ and let $\mathfrak{p}$ be a prime ideal divisor of $[p]$ in $\mathcal{O}_{\mathbb{K}}$ with ramification index $e_{\mathfrak{p}}$. Then $\mathfrak{p}$ divides either $[\alpha]$ or $[\beta]$ and we shall assume, without loss of generality, that $\mathfrak{p}$ divides $[\alpha]$. Put $a' = (\beta - \alpha)a$ and $b' = (\beta - \alpha)b$. If p^l exactly divides $[u_m]$ then $\mathfrak{p}^{e_{\mathfrak{p}} l}$ exactly divides $[b']$ for m sufficiently large. Thus

$$|u_m|_p \geq |a'b'|_p,$$

and so

$$\prod_{\substack{p<T \\ p|\alpha\beta}} |S(p)|_p^{-1} \leq \prod_{\substack{p<T \\ p|\alpha\beta}} |a'b'|_p^{-n}. \tag{45}$$

Assume now that p does not divide $\alpha\beta$ and let t_n, as in (5), be the n-th term of the Lucas sequence associated with $(u_n)_{n=0}^{\infty}$. For positive integers m and r with $m \geq r$,

$$u_m - \beta^r u_{m-r} = a'\alpha^{m-r} t_r. \tag{46}$$

On setting $m = m(p)$ in (46) and letting r run over those integers such that $m(p) - r \geq n$ we find that

$$|u_{m(p)-1} \dots u_n|_p \geq \prod_{r=1}^{m(p)-n} (|t_r|_p |a'b'|_p). \tag{47}$$

Let $l = l(p)$ be the smallest integer for which p divides t_l; l exists by Lemma 6. For any real number x let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x. By Lemma 7, if $p > 2$ then

$$\prod_{r=1}^{m(p)-n} |t_r|_p = |t_l|_p^{s_1} |s_1!|_p, \tag{48}$$

where $s_1 = \lfloor \frac{m(p)-n}{l} \rfloor$, while if $p = 2$

$$\prod_{r=1}^{m(p)-n} |t_r|_2 = |t_l|_2^{s_1} \left| \frac{t_{2l}}{t_l} \right|_2^{s_2} |s_2!|_2, \tag{49}$$

where $s_2 = \lfloor \frac{m(p)-n}{2l} \rfloor$. Similarly on setting $m - r = m(p)$ in (46) and letting r run over those integers such that $m(p) + r \leq 2n$ we find that for $p > 2$

$$|u_{m(p)+1} \dots u_{2n}|_p \geq |t_l|_p^{s_3} |s_3!|_p |a'b'|_p^{2n-m(p)}, \tag{50}$$

while for $p = 2$,

$$|u_{m(p)+1} \dots u_{2n}|_2 \geq |t_l|_2^{s_3} \left| \frac{t_{2l}}{t_l} \right|_2^{s_4} |s_4!|_2 |a'b'|_2^{2n-m(p)}, \tag{51}$$

where $s_3 = \lfloor \frac{2n-m(p)}{l} \rfloor$ and $s_4 = \lfloor \frac{2n-m(p)}{2l} \rfloor$. Thus, from (47), (48) and (50) we see that if p is a prime number which does not divide $2\alpha\beta$ then

$$|S(p)|_p^{-1} \leq |t_l|_p^{-s} |s!|_p^{-1} |a'b'|_p^{-n} \tag{52}$$

and

$$|S(2)|_2^{-1} \leq |t_l|_2^{-s} \left|\frac{t_{2l}}{t_l}\right|_2^{-s} |s!|_2^{-1} |a'b'|_2^{-n} \tag{53}$$

where $s = \lfloor \frac{n}{l} \rfloor$.

By Lemma 6 either 2 divides $\alpha\beta$ or 2 divides t_n for some integer n and $l(2)$ is either 2 or 3. But in the latter case, since $|t_l| \leq 2|\alpha|^l$,

$$|t_l|_2^{-s} \left|\frac{t_{2l}}{t_l}\right|_2^{-s} \leq 2^n |\alpha|^{2n}. \tag{54}$$

Therefore, by (45), (52), (53) and (54)

$$\prod_{p<T} |S(p)|_p^{-1} \leq 2^n |\alpha|^{2n} (\prod_{\substack{p<T \\ p \nmid 2\alpha\beta}} |t_l|_p^{-s}) n! |a'b'|^n. \tag{55}$$

Now

$$\prod_{\substack{p<T \\ p \nmid 2\alpha\beta}} |t_l|_p^{-s} = AB \tag{56}$$

where

$$A = \prod_{\substack{l(p)<n/\log n \\ p<T \\ p \nmid 2\alpha\beta}} |t_{l(p)}|_p^{-\lfloor \frac{n}{l(p)} \rfloor}$$

and

$$B = \prod_{\substack{n/\log n \leq l(p) \\ p<T \\ p \nmid 2\alpha\beta}} |t_{l(p)}|_p^{-\lfloor \frac{n}{l(p)} \rfloor}$$

Observe that

$$A \leq \prod_{1 \leq l < n/\log n} |t_l|^{\frac{n}{l}}$$

and so

$$A \leq \prod_{1 \leq l < n/\log n} 2^n |\alpha|^n$$

hence

$$\log A \leq c_3 n^2 / \log n. \tag{57}$$

Further when $l(p) \geq n/\log n$ we have

$$\left\lfloor \frac{n}{l(p)} \right\rfloor \leq \log n$$

and, by Lemma 6, when $p < T$ we see that $l(p) < T + 1$. Since

$$p + 1 \geq l(p) \geq n/\log n$$

it follows from Lemma 8 that

$$\log B \leq \pi(T)\log n(T{+}1)\exp(-\log(T{+}1)/(51.9\log\log(T{+}1)))\log(T{+}1)\log|\alpha|\log 2n$$

hence, by (39),

$$\log B \leq n^2 \exp(-\log n/40,000\log\log n), \tag{58}$$

for n sufficiently large. By (55), (56), (57) and (58)

$$\log \prod_{p<T} |S(p)|_p^{-1} \leq c_4 n\log n + c_3 n^2/\log n + n^2\exp(-\log n/40,000\log\log n), \tag{59}$$

for n sufficiently large.

But the lower bound (40) for $\log|\prod_{m\in M} u_m|$ is incompatible with the upper bound which follows from (41), (44) and (59) for n sufficiently large. This contradiction establishes our result.

7. Remark

As the referee has noted, the proof of Theorem 2 shows not only that the set of positive integers m for which (38) holds is of density zero but that up to X it is of size $O(X/\log X)$. In fact, by modifying the definition of A and B, one may prove that there is a positive number c such that up to X the set is of size $O(X/\exp(c\log X/\log\log X))$.

8. Acknowledgements

I would like to thank the referee for their comments. This research was supported in part by the Canada Research Chairs Program and by grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

References

[1] A. Baker, Contributions to the theory of Diophantine equations I. On the representation of integers by binary forms, *Phil. Trans. Roy. Soc. London* **A263** (1968), 173–191.

[2] A.Baker and G.Wüstholz, Logarithmic forms and group varieties, *J.reine angew. Math.* **442** (1993),19-62.

[3] N. Balaji and F. Luca, Terms of Lucas sequences having a large smooth divisor, *Canadian Math. Bulletin* **66** (2023), 225-231.

[4] A.S. Bang, Taltheoretiske undersøgelser, *Tidsskrift for Mat.* **4** (1886), 70–78, 130–137.

[5] Y. Bilu, H. Hong and S. Gun, Uniform explicit Stewart's theorem on prime factors of linear recurrences, *Acta Arith.* **206** (2022), 223-243.

[6] G.D. Birkhoff and H.S. Vandiver, On the integral divisors of $a^n - b^n$, *Ann. Math.* **5** (1904), 173–180.

[7] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, Cambridge University Press, 2006.

[8] R.D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. Math.* **15** (1913), 30–70.

[9] H. Hong, Stewart's Theorem revisited: suppressing the norm ± 1 hypothesis, *Boletin de la Sociedad Mat. Mexicana* **28**, Article number: 60 (2022).

[10] M. Laurent, M. Mignotte and Y. Nesterenko, Formes linéaires en deux logarithmes et déterminants d'interpolation, *J. Number Theory* **55** (1995), 285-321.

[11] D.H. Lehmer, An extended theory of Lucas' functions, *Ann. Math.* **31** (1930), 419–448.

[12] F. Luca, Arithmetic properties of members of a binary recurrent sequence, *Acta Arith.* **109** (2003), 81–107.

[13] E. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* **1** (1878), 184–240, 289–321.

[14] K. Mahler, Eine arithmetische Eigenschaft der rekurrierenden Reihen, *Mathematica* (Leiden) **3** (1934–35), 153–156.

[15] E.M. Matveev, An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers, II, *Izvestiya Mathematics* **64** (2000), 1217–1269.

[16] M.R. Murty, F. Séguin and C.L. Stewart, A lower bound for the two-variable Artin conjecture and prime divisors of recurrence sequences, *Journal of Number Theory*, **194** (2019), 8-29.

[17] A. Schinzel, The intrinsic divisors of Lehmer numbers in the case of negative discriminant, *Ark. Mat.* **4** (1962), 413–416.

[18] A. Schinzel, On two theorems of Gelfond and some of their applications, *Acta Arith.* **13** (1967), 177–236.

[19] A. Schinzel, An extension of the theorem on primitive divisors in algebraic number fields, *Mathematics of Computation* **61** (1993), 441-444.

[20] T.N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge tracts in mathematics **87**, Cambridge University Press, 1986.

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

[22] C.L. Stewart, On divisors of terms of linear recurrence sequences, *J. reine angew. Math.* **333** (1982), 12–31.

[23] C.L. Stewart, On divisors of Lucas and Lehmer numbers, *Acta Mathematica*, **211** (2013), 291-314.

[24] C.L. Stewart, On prime factors of terms of linear recurrence sequences, "Number Theory and Related Fields, In memory of Alf van der Poorten" Springer Proceedings in Mathematics and Statistics, (J. Borwein, I. Shparlinski and W. Zudilin, eds.), Volume **43** (2013), 341-359.

[25] K. Yu, P-adic logarithmic forms and a problem of Erdős, *Acta Math.* **211** (2013), 315-382.

[26] Kunrui Yu and Ling-kei Hung, On binary recurrence sequences, *Indag. Mathem., N.S.* **6** (1995), 341–354.

[27] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math.* **3** (1892), 265–284.

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

Email address: cstewart@uwaterloo.ca