# On Prime Factors of Terms of Linear Recurrence Sequences

**C.L. Stewart**

*In memory of Alf van der Poorten*

## 1 Introduction

Let $k$ be a positive integer, $r_1,\dots,r_k$ and $u_0,\dots,u_{k-1}$ be integers and put

$$u_n = r_1 u_{n-1} + \cdots + r_k u_{n-k},$$

for $n = k, k+1, \dots$. Suppose that $r_k$ is non-zero and that $u_0,\dots,u_{k-1}$ are not all zero. The sequence $(u_n)_{n=0}^{\infty}$ is a recurrence sequence of order $k$. It has a characteristic polynomial $G(z)$ given by

$$G(z) = z^k - r_1 z^{k-1} - \cdots - r_k.$$

Let

$$G(z) = \prod_{i=1}^{t} (z-\alpha_i)^{\ell_i},$$

with $\alpha_1,\dots,\alpha_t$ distinct. Then, see Theorem C.1 of [34], there exist polynomials $f_1,\dots,f_t$ of degrees less than $\ell_1,\dots,\ell_t$, respectively, and with coefficients from $\mathbb{Q}(\alpha_1,\dots,\alpha_t)$ such that

$$u_n = f_1(n)\alpha_1^n + \cdots + f_t(n)\alpha_t^n, \tag{1}$$

C.L. Stewart (✉)
Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
e-mail: cstewart@uwaterloo.ca

J.M. Borwein et al. (eds.), *Number Theory and Related Fields: In Memory of Alf van der Poorten*, Springer Proceedings in Mathematics & Statistics 43,
DOI 10.1007/978-1-4614-6642-0_18, 

for $n = 0, 1, 2, \ldots$. The recurrence sequence $(u_n)_{n=0}^{\infty}$ is said to be degenerate if $\alpha_i/\alpha_j$ is a root of unity for a pair $(i, j)$ with $1 \leq i < j \leq t$ and is said to be non-degenerate otherwise. In 1935 Mahler [20] proved that

$$|u_n| \to \infty \quad \text{as} \quad n \to \infty$$

whenever $(u_n)_{n=0}^{\infty}$ is a non-degenerate linear recurrence sequence. Mahler's proof is not effective in the following sense. Given a positive integer $m$ the proof does not yield a number $C(m)$ which is effectively computable in terms of $m$, such that $|u_n| > m$ whenever $n > C(m)$. However, Schmidt [31, 32], Allen [1] and Amoroso and Viada [2] have given estimates in terms of $t$ only for the number of times $|u_n|$ assumes a given value when the recurrence sequence is non-degenerate.

For any integer $n$ let $P(n)$ denote the greatest prime factor of $n$ with the convention that $P(0) = P(\pm 1) = 1$. Suppose that in (1) $t > 1$, $f_1, \ldots, f_t$ are polynomials which are not the zero polynomial and that $\alpha_1, \ldots, \alpha_t$ are non-zero. van der Poorten and Schlickewei [25] in 1982 and independently Evertse [12] proved, under the above assumption, that if the sequence $(u_n)_{n=0}^{\infty}$ is non-degenerate then

$$P(u_n) \to \infty \quad \text{as} \quad n \to \infty. \tag{2}$$

A key feature of the work of van der Poorten and Schlickewei and of Evertse is an appeal to a $p$-adic version of Schmidt's Subspace Theorem due to Schlickewei [30] and so (2) is also an ineffective result.

We may suppose, without loss of generality, that

$$|\alpha_1| \geq |\alpha_2| \geq \cdots \geq |\alpha_t| > 0.$$

If $|\alpha_1| > |\alpha_2|$ then plainly $|u_n|$ tends to infinity with $n$. In this case Shparlinski [35] and Stewart [40] independently obtained effective lower bounds for $P(u_n)$ which tend to infinity with $n$. The sharpest result obtained to date [41] when $u_n$ is the $n$th term of a non-degenerate linear recurrence as in (1) with $|\alpha_1| > |\alpha_2|$ and $u_n \neq f_1(n)\alpha_1^n$ is that there are positive numbers $c_1$ and $c_2$, which are effectively computable in terms of $r_1, \ldots, r_k$ and $u_0, \ldots, u_{k-1}$, such that

$$P(u_n) > c_1 \log n \frac{\log\log n}{\log\log\log n}, \tag{3}$$

provided that $n$ exceeds $c_2$. A key tool in the proof of (3) is a lower bound, due to Matveev [23], for linear forms in the logarithms of algebraic numbers.

## 2 Binary Recurrence Sequences

When the minimal order $k$ of the recurrence is 2 the sequence is known as a binary recurrence sequence. In this case, for $n \geq 0$,

$$u_n = a\alpha^n + b\beta^n, \tag{4}$$

where $\alpha$ and $\beta$ are the roots of the characteristic polynomial $x^2 - r_1x - r_2$ and

$$a = \frac{u_1 - u_0\beta}{\alpha - \beta}, \qquad b = \frac{u_0\alpha - u_1}{\alpha - \beta} \tag{5}$$

when $\alpha \neq \beta$. Since the recurrence sequence has order 2, $r_2$ is non-zero and so $\alpha\beta$ is non-zero. When $(u_n)_{n=0}^{\infty}$ is non-degenerate $\alpha \neq \beta$ and we see that $ab \neq 0$ since the recurrence sequence has minimal order 2. We may assume, without loss of generality that

$$|\alpha| \geq |\beta| > 0.$$

In 1934 Mahler [19] employed a $p$-adic version of the Thue-Siegel theorem in order to prove that if $u_n$ is the $n$th term of a non-degenerate binary recurrence sequence then

$$P(u_n) \to \infty \quad \text{as } n \to \infty.$$

Mahler's result is not effective. This defect was remedied by Schinzel [28] in 1967. He refined work of Gelfond on estimates for linear forms in the logarithms of two algebraic numbers in order to prove that if $(u_n)_{n=0}^{\infty}$ is a non-degenerate binary recurrence sequence then there exists a positive number $C_0$ which is effectively computable in terms of $a$, $b$, $\alpha$ and $\beta$ and positive numbers $c_1$ and $c_2$ such that

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

where

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

In 1982 Stewart [40] used estimates for linear forms in the logarithms of algebraic numbers due to Waldschmidt [44] in the Archimedean setting and due to van der Poorten [24] in the non-Archimedean setting to prove that there is a positive number $C_3$, which is effectively computable in terms of $u_0$, $u_1$, $r_1$ and $r_2$, such that for $n > 1$,

$$P(u_n) > C_3 (n/\log n)^{1/(d+1)} \tag{6}$$

where $d$ is the degree of $\alpha$ over the rationals. In 1995 Yu and Hung [46] were able to refine (6) by replacing the term $n/\log n$ by $n$. We are now able to make a further improvement on (6).

**Theorem 1.** *Let $u_n$, as in (4), be the nth term of a non-degenerate binary recurrence sequence with $ab\alpha\beta \neq 0$. There exists a positive number C which is effectively computable in terms of $u_0$, $u_1$, $r_1$ and $r_2$ such that for $n > C$*

$$P(u_n) > n^{1/2}\exp(\log n/104\log\log n). \tag{7}$$

The proof of Theorem 1 makes use of ideas from [42] which we will discuss in the next section. They were essential in resolving a conjecture made by Erdős in 1965 [11].

It is possible to sharpen (7) for most integers $n$. In [40] Stewart proved that if $(u_n)_{n=0}^{\infty}$ is a non-degenerate binary recurrence sequence then for all integers $n$, except perhaps a set of asymptotic density zero,

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

where $\varepsilon(n)$ is any real-valued function for which $\lim_{n\to\infty}\varepsilon(n) = 0$. Furthermore it is possible to strengthen (7) whenever $u_n$ is non-zero and is divisible by a prime $p$ which does not divide $u_m$ for any non-zero $u_m$ with $0 \le m < n$. In this case Stewart [40] proved that there is a positive number $C_4$, which is effectively computable in terms of $a$ and $b$ only such that

$$P(u_n) > n - C_4.$$

Luca [17] strengthened (7) when $(u_n)_{n=0}^{\infty}$ is a binary recurrence sequence as in (4) with $a/b$ and $\alpha/\beta$ multiplicatively dependent. He proved that then there exists a positive number $C_5$, which is effectively computable in terms of $a$, $b$, $\alpha$ and $\beta$, such that

$$P(u_n) > n - C_5 \tag{8}$$

for all positive integers $n$. Schinzel [28] had earlier obtained such a result in the case that $\alpha$ and $\beta$ are real numbers.

## 3 Lucas Sequences

Let $a$ and $b$ be integers with $a > b > 0$ and consider the binary recurrence sequence $(a^n - b^n)_{n=0}^{\infty}$. In 1892 Zsigmondy [47], and independently in 1904 Birkhoff and Vandiver [8], proved that for $n > 2$

$$P(a^n - b^n) \ge n+1. \tag{9}$$

This result had been established by Bang [6] in 1886 for the case when $b = 1$. Schinzel [26] proved in 1962 that if $a$ and $b$ are coprime and $ab$ is a square or twice a square then

$$P(a^n - b^n) \ge 2n+1$$

provided that $(a,b,n)$ is not $(2,1,4)$, $(2,1,6)$ or $(2,1,12)$.

In 1965 Erdős [11] conjectured that

$$\frac{P(2^n-1)}{n} \to \infty \quad \text{as } n \to \infty.$$

In 2000 Murty and Wong [22] proved that if $\varepsilon$ is a positive real number and $a$ and $b$ are integers with $a > b > 0$ then

$$P(a^n - b^n) > n^{2-\varepsilon},$$

for $n$ sufficiently large in terms of $a$, $b$ and $\varepsilon$ subject to the *abc* conjecture [43]. A few years later Murata and Pomerance [21] assumed the truth of the generalized Riemann hypothesis and deduced that

$$P(2^n-1) > n^{4/3}\log\log n$$

for a set of positive integers $n$ of asymptotic density 1.

In 1975 Stewart [36] proved that the Erdős conjecture holds when we restrict $n$ to run over those integers with at most $\kappa \log\log n$ distinct prime factors where $\kappa$ is any real number less than $1/\log 2$. In 2009 Ford, Luca and Shparlinski [13] proved that the series

$$\sum_{n=1}^{\infty} 1/P(2^n-1)$$

is convergent. Recently Stewart [42] established the conjecture of Erdős by proving that if $a$ and $b$ are positive integers then

$$P(a^n - b^n) > n\exp(\log n/104\log\log n) \tag{10}$$

provided that $n$ is sufficiently large in terms of the number of distinct prime factors of $ab$.

Suppose that $(u_n)_{n=0}^{\infty}$ is a non-degenerate binary recurrence sequence with $u_0 = 0$ and $u_1 = 1$. Then, recall (4) and (5),

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{11}$$

for $n = 0, 1, 2, \ldots$. Lucas [18] undertook an extensive study of the divisibility properties of such numbers in 1878 and we now refer to sequences $(u_n)_{n=0}^{\infty}$ with $u_n$ given by (11) as Lucas sequences. In 1912 Carmichael [9] proved that if $\alpha$ and $\beta$ are real, $n > 12$ and $u_n$ is the $n$th term of a Lucas sequence then

$$P(u_n) \geq n - 1. \tag{12}$$

Schinzel [27] established the same estimate in the case when $\alpha$ and $\beta$ are not real for $n$ sufficiently large in terms of $\alpha$ and $\beta$. Both results were proved by showing that $u_n$ possesses a primitive divisor for $n$ sufficiently large. A prime $p$ which divides $u_n$ but does not divide $(\alpha-\beta)^2 u_2 \cdots u_{n-1}$ is known as a primitive divisor of $u_n$. Let us assume that $\alpha+\beta$ and $\alpha\beta$ are coprime. Then Schinzel [29], in 1974, proved that there is a positive number $C_6$, which does not depend on $\alpha$ and $\beta$, such that $u_n$ has a primitive divisor for $n$ greater than $C_6$. In [39] Stewart proved that one can take $C_6$ to be $e^{452}2^{67}$. Further he showed that one can take $C_6$ to be 6 with finitely many exceptions and that these exceptions may be found by solving a large but finite collection of Thue equations. Bilu, Hanrot and Voutier [7] were able to determine all exceptions and as a consequence deduce that

$$P(u_n) \geq n-1,$$

for $n > 30$.

Stewart [38], when $\alpha$ and $\beta$ are real, and Shorey and Stewart [33], otherwise, extended the work of Stewart [36] to Lucas sequences. Let $u_n$ be the $n$th term of a non-degenerate Lucas sequence with $r_1$ and $r_2$ coprime. Let $\varphi(n)$ denote Euler's function, let $q(n)$ denote the number of square-free divisors of $n$ and let $\kappa$ denote a positive real number with $\kappa < 1/\log 2$. They proved that if $n$ $(> 3)$ has at most $\kappa \log\log n$ distinct prime factors then

$$P(u_n) > C_7(\varphi(n)\log n)/q(n),$$

where $C_7$ is a positive number which is effectively computable in terms of $\alpha$, $\beta$ and $\kappa$ only. The proofs depend on estimates for linear forms in the logarithms of algebraic numbers, in the complex case due to Baker [4] and in the $p$-adic case due to van der Poorten [24].

In [42] Stewart proved that estimate (10) holds with $a^n - b^n$ replaced by $u_n$ where $u_n$ is the $n$th term of a non-degenerate Lucas sequence. In fact, see [42], the same estimate also applies with $a^n - b^n$ replaced by $\tilde{u}_n$ where $\tilde{u}_n$ denotes the $n$th term of a non-degenerate Lehmer sequence. (The Lehmer sequences, see [15, 38], are closely related to the Lucas sequences and they possess similar divisibility properties.) For the proofs of these results estimates for linear forms in the logarithms of algebraic numbers again play a central role. In the Archimedean case we apply an estimate of Baker [3] while in the non-Archimedean case we appeal to an estimate of Yu [45].

## 4 Preliminaries for the Proof of Theorem 1

Let $K$ be a finite extension of $\mathbb{Q}$ and let $\wp$ be a prime ideal in the ring of algebraic integers $\mathcal{O}_K$ of $K$. Let $\mathcal{O}_\wp$ consist of 0 and the non-zero elements $\alpha$ of $K$ for which $\wp$ has a non-negative exponent in the canonical decomposition of the fractional ideal generated by $\alpha$ into prime ideals. Then let $P$ be the unique prime ideal of $\mathcal{O}_\wp$ and put $\overline{K_\wp} = \mathcal{O}_\wp / P$. Further for any $\alpha$ in $\mathcal{O}_\wp$ we let $\overline{\alpha}$ be the image of $\alpha$ under the residue class map that sends $\alpha$ to $\alpha + P$ in $\overline{K_\wp}$.

Let $p$ be an odd prime and let $d$ be an integer coprime with $p$. The Legendre symbol $\left(\frac{d}{p}\right)$ is 1 if $d$ is a quadratic residue modulo $p$ and is $-1$ if $d$ is a quadratic non-residue modulo $p$.

**Lemma 1.** *Let $d$ be a square-free integer different from 1. Let $\theta$ be an algebraic number of degree 2 over $\mathbb{Q}$ in $\mathbb{Q}(\sqrt{d})$, let $\theta'$ denote the algebraic conjugate of $\theta$ over $\mathbb{Q}$ and let $a_0$ be the leading coefficient in the minimal polynomial of $\theta$ in $\mathbb{Z}[x]$. Suppose that $p$ is a prime which does not divide $2a_0^2\theta\theta'$. Let $\wp$ be a prime ideal of the ring of algebraic integers of $\mathbb{Q}(\sqrt{d})$ lying above $p$. The order of $\overline{\theta/\theta'}$ in $(\overline{\mathbb{Q}(\sqrt{d})_\wp})^\times$ is a divisor of 2 if $p$ divides $a_0^4(\theta^2 - \theta'^2)^2$ and a divisor of $p - \left(\frac{d}{p}\right)$ otherwise.*

*Proof.* Note that $\gamma = a_0\theta$ is an algebraic integer with algebraic conjugate $\gamma' = a_0\theta'$. Thus $\gamma/\gamma' = \theta/\theta'$ and our result follows from Lemma 2.2 of [42]. □

For any algebraic number $\gamma$ let $h(\gamma)$ denote the absolute logarithmic height of $\gamma$. Thus if $a_0(x-\gamma_1)\cdots(x-\gamma_d)$ in $\mathbb{Z}[x]$ is the minimal polynomial of $\gamma$ over $\mathbb{Z}$ then

$$h(\gamma) = \frac{1}{d}\left(\log a_0 + \sum_{j=1}^{d} \log\max(1, |\gamma_j|)\right).$$

Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers and put $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ and $d = [K : \mathbb{Q}]$. Let $\wp$ be a prime ideal of the ring $\mathcal{O}_K$ of algebraic integers in $K$ lying above the prime number $p$. Denote by $e_\wp$ the ramification index of $\wp$ and by $f_\wp$ the residue class degree of $\wp$. For $\alpha$ in $K$ with $\alpha \neq 0$ let $\mathrm{ord}_\wp \alpha$ be the exponent to which $\wp$ divides the principal fractional ideal generated by $\alpha$ in $K$ and put $\mathrm{ord}_\wp 0 = \infty$. For any positive integer $m$ let $\zeta_m = e^{2\pi i/m}$ and put $\alpha_0 = \zeta_{2^u}$ where $\zeta_{2^u}$ is in $K$ and $\zeta_{2^{u+1}}$ is not in $K$.

Suppose that $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent $\wp$-adic units in $K$. Let $\overline{\alpha_0}, \overline{\alpha_1}, \ldots, \overline{\alpha_n}$ be the images of $\alpha_0, \alpha_1, \ldots, \alpha_n$ respectively, under the residue class map at $\wp$ from the ring of $\wp$-adic integers in $K$ onto the residue class field $\overline{K_\wp}$ at $\wp$. For any set $X$ let $|X|$ denote its cardinality. Let $\langle \overline{\alpha_0}, \overline{\alpha_1}, \ldots, \overline{\alpha_n} \rangle$ be the subgroup of $(\overline{K_\wp})^\times$ generated by $\overline{\alpha_0}, \ldots, \overline{\alpha_n}$. We define $\delta$ by

$$\delta = 1 \quad \text{if} \quad \left[K\left(\alpha_0^{1/2}, \alpha_1^{1/2}, \ldots, \alpha_n^{1/2}\right) : K\right] < 2^{n+1}$$

and

$$\delta = (p^{f_\wp} - 1)/|\langle \overline{\alpha_0}, \overline{\alpha_1}, \ldots, \overline{\alpha_n} \rangle|$$

if

$$\left[K\left(\alpha_0^{1/2}, \alpha_1^{1/2}, \ldots, \alpha_n^{1/2}\right) : K\right] = 2^{n+1}.$$

Denote $\log\max(x, e)$ by $\log^* x$.

**Lemma 2.** *Let $p$ be a prime with $p \geq 5$ and let $\wp$ be an unramified prime ideal of $\mathcal{O}_K$ lying above $p$. Let $\alpha_1, \ldots, \alpha_n$ be multiplicatively independent $\wp$-adic units. Let $b_1, \ldots, b_n$ be integers, not all zero, and put*

$$B = \max(2, |b_1|, \ldots, |b_n|).$$

*Then*

$$\mathrm{ord}_{\wp}(\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1) < Ch(\alpha_1) \cdots h(\alpha_n) \max(\log B, (n+1)(5.4n + \log d))$$

*where*

$$C = 376(n+1)^{1/2} \left(7e\frac{p-1}{p-2}\right)^n d^{n+2} \log^* d \log(e^4(n+1)d) \cdot$$
$$\max\left(\frac{p^{f_p}}{\delta}\left(\frac{n}{f_p \log p}\right)^n, e^n f_p \log p\right).$$

*Proof.* This is Lemma 3.1 of [42] and it follows from the work of Yu [45]. □

The next result we require is proved using class field theory and the Chebotarev Density Theorem.

**Lemma 3.** *Let $d$ be a square-free integer different from 1 and let $p_k$ denote the kth smallest prime of the form $N(\pi_k) = p_k$ where $N$ denotes the norm from $\mathbb{Q}(\sqrt{d})$ to $\mathbb{Q}$ and $\pi_k$ is an algebraic integer in $\mathbb{Q}(\sqrt{d})$. Let $\varepsilon$ be a positive real number. There is a positive number $C$, which is effectively computable in terms of $\varepsilon$ and $d$, such that if $k$ exceeds $C$ then*

$$\log p_k < (1+\varepsilon)\log k.$$

*Proof.* This is Lemma 2.4 of [42]. □

We shall also require an estimate for the rate of growth of a non-degenerate binary recurrence sequence.

**Lemma 4.** *Let $u_n$, as in (4), be the nth term of a non-degenerate binary recurrence sequence. Suppose that $|\alpha| \geq |\beta|$. Then there exist positive numbers $C_1$ and $C_2$, which are effectively computable in terms of $a$ and $b$, such that if $n$ exceeds $C_1$ then*

$$|u_n| > |\alpha|^{n - C_2 \log n}.$$

*Proof.* This is Lemma 3.2 of [37]; see also Lemma 5 of [40]. □

**Lemma 5.** *Let $K$ be a finite extension of $\mathbb{Q}$ and let $p$ be a prime number. Let $\alpha_1, \ldots, \alpha_n$ be non-zero elements of $K$ and let $\alpha_1^{1/p}, \ldots, \alpha_n^{1/p}$ denote fixed pth roots of $\alpha_1, \ldots, \alpha_n$, respectively. Put $K' = K(\alpha_1^{1/p}, \ldots, \alpha_{n-1}^{1/p})$. Then either $K'(\alpha_n^{1/p})$ is an extension of $K'$ of degree $p$ or we have*

$$\alpha_n = \alpha_1^{j_1} \cdots \alpha_{n-1}^{j_{n-1}} \gamma^p$$

*for some* $\gamma$ *in* $K$ *and some integers* $j_1, \dots, j_{n-1}$ *with* $0 \le j_i < p$ *for* $i = 1, \dots, n-1$.

*Proof.* This is Lemma 3 of Baker and Stark [5]. □

**Lemma 6.** *Let* $n$ *be a positive integer and let* $\alpha_0, \alpha_1, \dots, \alpha_n$ *be multiplicatively dependent non-zero elements of a number field* $K$ *of degree* $d \ge 2$ *over* $\mathbb{Q}$. *Suppose that any* $n$ *from* $\alpha_0, \dots, \alpha_n$ *are multiplicatively independent. Then there are non-zero rational integers* $b_0, \dots, b_n$ *with*

$$\alpha_0^{b_0} \cdots \alpha_n^{b_n} = 1$$

*and*

$$|b_i| \le 58(n!e^n/n^n)d^{n+1}(\log d)h(\alpha_0) \cdots h(\alpha_n)/h(\alpha_i)$$

*for* $i = 0, \dots, n$.

*Proof.* This is Corollary 3.2 of Loher and Masser [16]. They attribute the result to Yu. □

**Lemma 7.** *Let* $(u_n)_{n=0}^{\infty}$ *be a non-degenerate binary recurrence sequence as in* (4) *with* $ab\alpha\beta \neq 0$ *and* $a/b$ *and* $\alpha/\beta$ *multiplicatively independent. There exists a positive number* $C$ *which is effectively computable in terms of* $a$, $b$, $\alpha$ *and* $\beta$ *such that if* $p$ *exceeds* $C$ *then*

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

*Proof.* Our proof will be modelled on the proof of Lemma 4.3 in [42]. Let $c_1, c_2, \dots$ denote positive numbers which are effectively computable in terms of $a$, $b$, $\alpha$ and $\beta$. Let $p$ be a prime which does not divide $2(\alpha-\beta)^4 ab\alpha\beta$.

Put $K = \mathbb{Q}(\alpha/\beta)$ and

$$\alpha_0 = \begin{cases} i & \text{if } i \in K \\ -1 & \text{otherwise.} \end{cases}$$

Let $d$ be a non-zero square-free integer for which $K = \mathbb{Q}(\sqrt{d})$. Let $v$ be the largest integer for which

$$\alpha/\beta = \alpha_0^j \theta^{2^v} \tag{13}$$

with $0 \le j \le 3$ and $\theta$ in $K$.

Note that $v$ exists since $\alpha/\beta$ is not a root of unity and thus $\theta$ is not a root of unity. Further, by Dobrowolski's theorem $h(\alpha/\beta) > c_1 > 0$ and

$$h(\alpha/\beta) = 2^v h(\theta).$$

Thus $v$ cannot be arbitrarily large. Observe also that by Lemma 5

$$\left[K\left(\alpha_0^{1/2},\theta^{1/2}\right):K\right]=4.$$

Next we choose $w$ maximal so that there exists $\gamma$ in $K$ with

$$\frac{a}{b}=\alpha_0^{j_0}\theta^{j_1}\gamma^{2^w} \tag{14}$$

and $0\le j_0\le 3$, $0\le j_1\le 2^w$. Such a choice is possible as we shall now show. First observe that

$$2^w h(\gamma)\le h\left(\frac{a}{b}\right)+j_1 h(\theta_1)$$

so

$$h(\gamma)\le c_2. \tag{15}$$

Further we have from (14) that

$$\left(\frac{a}{b}\right)^{-4}\theta^{4j_1}\gamma^{2^{w+2}}=1. \tag{16}$$

Next notice that if two of the three numbers $a/b$, $\theta$ and $\gamma$ are multiplicatively dependent then $a/b$ and $\theta$ are multiplicatively dependent; hence, by (13), $a/b$ and $\alpha/\beta$ are multiplicatively dependent. Therefore we may suppose that any two of the three numbers $a/b$, $\theta$ and $\gamma$ are multiplicatively independent. Thus, by Lemma 6, there are non-zero integers $b_1$, $b_2$, $b_3$, with

$$\left(\frac{a}{b}\right)^{b_1}\theta^{b_2}\gamma^{b_3}=1 \tag{17}$$

and with

$$|b_i|\le c_3 \tag{18}$$

for $i=1,2,3$. It follows from (16) and (17) that

$$\left(\frac{a}{b}\right)^{b_1 2^{w+2}}\theta^{b_2 2^{w+2}}=\left(\frac{a}{b}\right)^{-4b_3}\theta^{4j_1 b_3}.$$

Since $a/b$ and $\theta$ are multiplicatively independent and $b_1$ is non-zero it follows from (18) that $w$ is at most $c_4$.

Next we observe that since $w$ is maximal we have

$$\left[K\left(\alpha_0^{1/2},\theta^{1/2},\gamma^{1/2}\right):K\right]=8 \tag{19}$$

for otherwise by Lemma 5 there is $\gamma_1$ in $K$ and integers $j_0$ and $j_1$ with $0\le j_i<2$ for $i=0,1$ such that

$$\gamma = \alpha_0^{j_0} \theta^{j_1} \gamma_1^2 \tag{20}$$

and substituting for $\gamma$ in (14) using (20) we would contradict the maximality of $w$.

Let $\wp$ be a prime ideal of $\mathcal{O}_K$ lying above the rational prime $p$. Then since $p \nmid \alpha\beta ab(\alpha-\beta)^4$

$$\begin{aligned}\operatorname{ord}_p u_n &\le \operatorname{ord}_{\wp}((a/b)(\alpha/\beta)^n - 1)\\ &\le \operatorname{ord}_{\wp}\left((a/b)^4(\alpha/\beta)^{4n} - 1\right).\end{aligned}$$

Thus, by (13) and (14),

$$\operatorname{ord}_p u_n \le \operatorname{ord}_{\wp}\left(\gamma^{2^{w+2}} \theta^{4j_1 + 2^{v+2}n} - 1\right). \tag{21}$$

For any real number $x$ let $[x]$ denote the greatest integer less than or equal to $x$. Put

$$k = \left[\frac{\log p}{51.8 \log\log p}\right]. \tag{22}$$

Then, for $p > c_5$, $k > 2$ and

$$\max\left(p\left(\frac{k}{\log p}\right)^k, e^k \log p\right) = p\left(\frac{k}{\log p}\right)^k. \tag{23}$$

Our proof now splits depending on whether $\mathbb{Q}(\alpha/\beta) = \mathbb{Q}$ or not. Let us first suppose that $\mathbb{Q}(\alpha/\beta) = \mathbb{Q}$ so that $\alpha$ and $\beta$ are integers. For any positive integer $j$ let $p_j$ denote the $j-2$th smallest prime which does not divide $2p(\alpha-\beta)^4 ab\alpha\beta$. We put

$$m = 4j_1 + 2^{v+2}n \tag{24}$$

and

$$\alpha_1 = \theta / p_3 \cdots p_k.$$

Then

$$\gamma^{2^{w+2}} \theta^m = \alpha_1^m \gamma^{2^{w+2}} p_3^m \cdots p_k^m$$

so by (21)

$$\operatorname{ord}_p u_n \le \operatorname{ord}_p(\alpha_1^m \gamma^{2^{w+2}} p_3^m \cdots p_k^m - 1). \tag{25}$$

Note that $\alpha_1, \gamma, p_3, \ldots, p_k$ are multiplicatively independent since $\theta$ and $\gamma$ are multiplicatively independent and $p_3, \ldots, p_k$ are primes which do not divide $2p(\alpha - \beta)^4 ab\alpha\beta$. Further since $p_3, \ldots, p_k$ are different from $p$ and $p$ does not divide $2(\alpha-\beta)^4 ab\alpha\beta$ we see that $\alpha_1, \gamma, p_3, \ldots, p_k$ are $p$-adic units.

We now apply Lemma 2 with $\delta = 1$, $d = 1$, $f_{\wp} = 1$ and $n = k$ to conclude that

$$\operatorname{ord}_p(\alpha_1^m \gamma^{2^{w+2}} p_3^m \cdots p_k^m - 1) \le c_6(k+1)^3 \left(7e\frac{p-1}{p-2}\right)^k$$
$$\max\left(p\left(\frac{k}{\log p}\right)^k,\ e^k \log p\right) \log(2^{w+2}m) h(\alpha_1) h(\gamma) \log p_3 \cdots \log p_k. \tag{26}$$

For any non-zero integer $n$ let $\omega(n)$ denote the number of distinct prime factors of $n$. Put

$$t = \omega(2p(\alpha-\beta)^4 ab\alpha\beta) \tag{27}$$

and let $q_i$ denote the $i$th prime number. Note that

$$p_k \le q_{k+t}$$

and thus

$$\log p_3 + \cdots + \log p_k \le (k-2)\log q_{k+t}.$$

By the prime number theorem with error term, for $k > c_7$,

$$\log p_3 + \cdots + \log p_k \le 1.001(k-2)\log k. \tag{28}$$

By the arithmetic-geometric mean inequality

$$\log p_3 \cdots \log p_k \le \left(\frac{\log p_3 + \cdots + \log p_k}{k-2}\right)^{k-2}$$

and so, by (28),

$$\log p_3 \cdots \log p_k \le (1.001 \log k)^{k-2}. \tag{29}$$

Since $h(\alpha_1) \le h(\theta) + \log p_3 \cdots p_k$ it follows from (28) that

$$h(\alpha_1) \le c_8 k \log k.$$

Further

$$2^{w+2}m = 2^{w+2}(4j_1 + 2^{v+2}n) < c_9 n$$

and so

$$\log(2^{w+2}m) < c_{10} \log n. \tag{30}$$

Thus, by (23), (25), (26) and (28)–(30),

$$\operatorname{ord}_p u_n < c_{11} k^4 p \left(7e\frac{p-1}{p-2}\frac{1.001k\log k}{\log p}\right)^k \log n.$$

Therefore, by (22), for $p > c_{12}$

$$\mathrm{ord}_p\, u_n < p e^{-\frac{\log p}{51.9 \log\log p}} \log n. \tag{31}$$

We now suppose that $[\mathbb{Q}(\alpha/\beta):\mathbb{Q}] = 2$. Let $\pi_3, \ldots, \pi_k$ be elements of $\mathcal{O}_K$ with the property that $N(\pi_i) = p_i$ where $N$ denotes the norm from $K$ to $\mathbb{Q}$ and where $p_i$ is the $(i-2)$th smallest rational prime number of this form which does not divide $2p\alpha\beta ab(\alpha-\beta)^4$. We now put $\theta_i = \pi_i/\pi_i'$ where $\pi_i'$ denotes the algebraic conjugate of $\pi_i$ in $\mathbb{Q}(\alpha/\beta)$. Notice that $p$ does not divide $\pi_i\pi_i' = p_i$ and if $p$ does not divide $(\pi_i - \pi_i')^2$ then

$$\left(\frac{(\pi_i-\pi_i')^2}{p}\right) = \left(\frac{d}{p}\right)$$

since $\mathbb{Q}(\alpha/\beta) = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\pi_i)$. Thus, by Lemma 1, the order of $\theta_i$ in $(\overline{\mathbb{Q}(\alpha/\beta)_{\wp}})^{\times}$ is a divisor of 2 if $p$ divides $(\pi_i^2 - \pi_i'^2)^2$ and a divisor of $p - \left(\frac{d}{p}\right)$ otherwise. Since $p$ is odd and $p$ is different from $p_i$ we observe that the order of $\theta_i$ in $(\overline{\mathbb{Q}(\alpha/\beta)_{\wp}})^{\times}$ is a divisor of $p - \left(\frac{d}{p}\right)$.

Recall (22) and put

$$\alpha_1 = \theta/\theta_3 \cdots \theta_k.$$

Then $\alpha_1^m \theta_3^m \cdots \theta_k^m = \theta^m$ and by (21) and (24) we see that

$$\mathrm{ord}_p\, u_n \le \mathrm{ord}_{\wp}(\alpha_1^m \gamma^{2^{w+2}} \theta_3^m \cdots \theta_k^m - 1). \tag{32}$$

Observe that $\alpha_1$, $\gamma$, $\theta_3, \ldots, \theta_k$ are multiplicatively independent since $\theta$ and $\gamma$ are multiplicatively independent and $p_3, \ldots, p_k$ are primes which do not divide $2(\alpha-\beta)^4 ab\alpha\beta$ and the principal prime ideals $[\pi_i]$ for $i = 3, \ldots, k$ do not ramify since $p_i \nmid 2d$. Since $p_3, \ldots, p_k$ are different from $p$ and $p$ does not divide $2(\alpha-\beta)^4 ab\alpha\beta$ we see that $\alpha_1$, $\gamma$, $\theta_3, \ldots, \theta_k$ are $p$-adic units.

Notice that

$$K\left(\alpha_0^{1/2}, \theta^{1/2}, \gamma^{1/2}, \theta_3^{1/2}, \ldots, \theta_k^{1/2}\right) = K\left(\alpha_0^{1/2}, \alpha_1^{1/2}, \gamma^{1/2}, \theta_3^{1/2}, \ldots, \theta_k^{1/2}\right).$$

Further, by (19),

$$\left[K\left(\alpha_0^{1/2}, \theta^{1/2}, \gamma^{1/2}, \theta_3^{1/2}, \ldots \theta_k^{1/2}\right) : K\right] = 2^{k+1}, \tag{33}$$

since otherwise by Lemma 5 there is an integer $i$ with $3 \le i \le k$ and integers $j_0, \ldots, j_{i-1}$ with $0 \le j_b \le 1$ for $b = 0, \ldots, i-1$ and an element $\psi$ of $K$ for which

$$\theta_i = \alpha_0^{j_0} \theta^{j_1} \gamma^{j_2} \theta_3^{j_3} \cdots \theta_{i-1}^{j_{i-1}} \psi^2. \tag{34}$$

But then the order of the prime ideal $[\pi_i]$ on the left-hand side of (34) is even which is a contradiction. Thus (33) holds.

Since $p$ does not divide the discriminant of $K$ and $[K:\mathbb{Q}]=2$ either $p$ splits, in which case $f_\wp = 1$ and $\left(\frac{d}{p}\right)=1$, or $p$ is inert, in which case $f_\wp=2$ and $\left(\frac{d}{p}\right)=-1$, see [14]. Put

$$\delta = (p^{f_\wp}-1)/|\langle\overline{\alpha_0},\overline{\alpha_1},\overline{\gamma},\overline{\theta_3},\ldots,\overline{\theta_k}\rangle|.$$

Observe that if $\left(\frac{d}{p}\right)=1$ then

$$p^{f_\wp}/\delta \le p. \tag{35}$$

Let us now determine $|\langle\overline{\alpha_0},\overline{\alpha_1},\overline{\gamma},\overline{\theta_3},\ldots,\overline{\theta_k}\rangle|$ in the case $\left(\frac{d}{p}\right)=-1$. We have shown that the order of $\overline{\theta_i}$ is a divisor of $p+1$ for $i=3,\ldots,k$. Since $\alpha$ and $\beta$ are conjugates $N(\alpha/\beta)$, the norm from $K$ to $\mathbb{Q}$ of $\alpha/\beta$ is 1. Therefore by (13), $N(\theta)=\pm 1$. Similarly $a$ and $b$ are conjugates over $\mathbb{Q}$ so $N(a/b)=1$ and thus $N(\gamma)=\pm 1$. By Hilbert's Theorem 90, see Theorem 14.35 of [10], $\theta^2=\rho/\rho'$ where $\rho$ and $\rho'$ are conjugate algebraic integers in $K$. Similarly, by (13) and (14), $\gamma^2=\lambda/\lambda'$ where $\lambda$ and $\lambda'$ are conjugate algebraic integers in $K$.

Note that we may suppose that the principal ideals $[\rho]$ and $[\rho']$ have no non-trivial principal ideal divisors in common. Further since $p$ does not divide $2(\alpha-\beta)^2ab\alpha\beta$ and since $\left(\frac{d}{p}\right)=-1$, $[p]$ is a principal ideal of $\mathcal{O}_K$ and $p$ does not divide $\rho\rho'$. The order of $\theta^2$ in $(\overline{K_\wp})^\times$ is a divisor of $p+1$ by Lemma 1 and thus $\theta$ has order a divisor of $2(p+1)$. By the same reasoning as above we find that the order of $\gamma^2$ in $(\overline{K_\wp})^\times$ is a divisor of $p+1$ and so, by Lemma 1, $\gamma$ has order a divisor of $2(p+1)$. Since $\alpha_0^4=1$ and, as we have already established, the order of $\theta_i$ is a divisor of $p+1$ for $i=3,\ldots,k$ we see that

$$|\langle\overline{\alpha_0},\overline{\theta},\overline{\gamma},\overline{\theta_3},\ldots,\overline{\theta_k}\rangle| \le 2(p+1)$$

hence

$$|\langle\overline{\alpha_0},\overline{\alpha_1},\overline{\gamma},\overline{\theta_3},\ldots,\overline{\theta_k}\rangle| \le 2(p+1).$$

Therefore

$$\delta = (p^2-1)/|\langle\overline{\alpha_0},\overline{\alpha_1},\overline{\gamma},\overline{\theta_3},\ldots,\overline{\theta_k}\rangle| \ge (p-1)/2. \tag{36}$$

We now apply Lemma 2, noting, by (35) and (36), that

$$p^{f_\wp}/\delta \le 2p^2/(p-1).$$

Thus, by (23),

$$\begin{aligned}\operatorname{ord}_\wp(\alpha_1^m\gamma^{2^{w+2}}\theta_3^m\cdots\theta_k^m-1) \le c_{12}k^3\log p\left(7e\frac{p-1}{p-2}\right)^k \\ 2^k p\left(\frac{k}{\log p}\right)^k(\log m)h(\alpha_1)h(\gamma)h(\theta_3)\cdots h(\theta_k).\end{aligned} \tag{37}$$

Observe that $\theta_i = \pi_i/\pi_i'$ and that $p_i(x-\pi_i/\pi_i')(x-\pi_i'/\pi_i) = p_i x^2 - (\pi_i^2+\pi_i'^2)x + p_i$ is the minimal polynomial of $\theta_i$ over the integers since $[\pi_i]$ is unramified. Now either the discriminant of $K$ is negative in which case $|\pi_i| = |\pi_i'|$ or it is positive in which case there is a fundamental unit $\varepsilon > 1$ in $\mathcal{O}_K$. As in [42] we may replace $\pi_i$ by $\pi_i \varepsilon^u$ for any integer $u$. Without loss of generality we may suppose that $p_i^{1/2} \leq |\pi_i| \leq p_i^{1/2}\varepsilon$ and hence that $p_i^{1/2}\varepsilon^{-1} \leq |\pi_i'| \leq p_i^{1/2}$. Therefore

$$h(\theta_i) \leq \frac{1}{2}\log p_i \varepsilon^2 = \frac{1}{2}\log p_i + \log \varepsilon \quad \text{for } d > 0$$

and

$$h(\theta_i) \leq \frac{1}{2}\log p_i \quad \text{for } d < 0.$$

Put

$$R = \begin{cases} \log \varepsilon & \text{for } d > 0 \\ 0 & \text{for } d < 0. \end{cases}$$

Then

$$h(\theta_i) \leq \frac{1}{2}\log p_i + R$$

for $i = 3, \ldots, k$. We also can ensure that

$$h(\theta_3 \cdots \theta_k) \leq \frac{1}{2}\log p_3 \cdots p_k + R$$

and so

$$h(\alpha_1) \leq h(\theta) + \frac{1}{2}\log p_3 \cdots p_k + R. \tag{38}$$

Let $t$ be given by (27) and let $q_i$ denote the $i$th prime number which is representable as the norm of an element of $\mathcal{O}_K$. Note that

$$p_k \leq q_{k+t}$$

and so

$$\log p_3 + \cdots + \log p_k \leq (k-2)\log q_{k+t}.$$

Therefore by Lemma 3 for $k > c_{13}$

$$(\log p_3 + 2R) + \cdots + (\log p_k + 2R) < (k-2)(1.0005\log k + 2R) < 1.001(k-2)\log k \tag{39}$$

and so, by the arithmetic-geometric mean inequality,

$$(\log p_3 + 2R)\cdots(\log p_k + 2R) < (1.001\log k)^{k-2}.$$

Thus, since $p_k$ is at least $k$, for $k > c_{14}$,

$$2^{k-2}h(\theta_3)\cdots h(\theta_k) \le (\log p_3 + 2R)\cdots(\log p_k + 2R) < (1.001\log k)^{k-2}. \qquad (40)$$

By (38) and (39)

$$h(\alpha_1) < c_{15}k\log k$$

and by (13), (14) and (24)

$$m \le c_{16}n. \qquad (41)$$

Thus, by (32), (38), (40) and (41),

$$\mathrm{ord}_p\, u_n \le c_{17}k^4 p\log p\left(7e\frac{p-1}{p-2}1.001\frac{k\log k}{\log p}\right)^k \log n.$$

Therefore, by (22), for $p > c_{18}$, we obtain (31) in this case also and our result follows. □

## 5 Proof of Theorem 1

Let $K = \mathbb{Q}(\alpha)$ and let $\mathcal{O}_K$ denote the ring of algebraic integers of $K$. For any $\theta$ in $\mathcal{O}_K$ let $[\theta]$ denote the ideal in $\mathcal{O}_K$ generated by $\theta$. We have

$$u_n = r_1u_{n-1} + r_2u_{n-2} \quad \text{for } n = 2,3,\ldots.$$

Let $l$ denote the greatest common divisor of $r_1^2$ and $r_2$. Then $\alpha^2/l$ and $\beta^2/l$ are algebraic integers in $K$. Further $\frac{r_1^2+2r_2}{l}$ and $(r_2/l)^2$ are coprime hence, as in Lemma A.10 of [34], $\left(\left[\frac{\alpha^2}{l}\right],\left[\frac{\beta^2}{l}\right]\right) = ([1])$. We may put

$$v_n = l^{-n}u_{2n} = a\left(\frac{\alpha^2}{l}\right)^n + b\left(\frac{\beta^2}{l}\right)^n$$

and

$$w_n = l^{-n}u_{2n+1} = a\alpha\left(\frac{\alpha^2}{l}\right)^n + b\beta\left(\frac{\beta^2}{l}\right)^n,$$

for $n = 0,1,2,\ldots$. Recall $r_2 = \alpha\beta$. For any prime $p$ which does not divide $r_2$ we have

$$\mathrm{ord}_p(u_{2n}) = \mathrm{ord}_p(v_n) \quad \text{and} \quad \mathrm{ord}_p(u_{2n+1}) = \mathrm{ord}_p(w_n).$$

Further $a/b$ and $\alpha/\beta$ are multiplicatively independent if and only if $a/b$ and $(\alpha/\beta)^2$ are multiplicatively independent. Similarly $a/b$ and $\alpha/\beta$ are multiplicatively independent if and only if $a\alpha/b\beta$ and $(\alpha/\beta)^2$ are multiplicatively independent.

Therefore, by considering the non-degenerate binary recurrence sequences $(v_n)_{n=0}^{\infty}$ and $(w_n)_{n=0}^{\infty}$ in place of $(u_n)_{n=0}^{\infty}$, we may assume, without loss of generality, that $([\alpha],[\beta]) = [1]$.

Let $c_1, c_2, \ldots$ denote positive numbers which are effectively computable in terms of $a$, $b$, $\alpha$ and $\beta$. By the result of Luca given in (8) the theorem follows if $a/b$ and $\alpha/\beta$ are multiplicatively dependent. We may assume therefore that $a/b$ and $\alpha/\beta$ are multiplicatively independent. For any integer $h$ and prime $p$ define $|h|_p$ by

$$|h|_p = p^{-\operatorname{ord}_p h}.$$

It follows from the proof of Theorem 1 of [40] that for any prime $p$ and integer $n \geq 2$

$$\log\left(|u_n|_p^{-1}\right) < c_1 p^2 (\log n)^2. \tag{42}$$

By Lemma 7 for $p > c_2$,

$$\log\left(|u_n|_p^{-1}\right) < p \log p \exp(-\log p/51.9 \log\log p) \log n. \tag{43}$$

By Lemma 4

$$\log|u_n| > c_3 n. \tag{44}$$

Write

$$|u_n| = p_1^{\ell_1} \cdots p_r^{\ell_r} \tag{45}$$

where $p_1, \ldots, p_r$ are distinct primes and $\ell_1, \ldots, \ell_r$ are positive integers. It follows from (42)–(45) that

$$\frac{n}{\log n} < c_4 \sum_{i=1}^{r} p_i \log p_i \exp(-\log p_i/51.9 \log\log p_i). \tag{46}$$

Put $p_r = P(u_n)$. The right-hand side of inequality (46) is at most

$$r p_r \log p_r \exp(-\log p_r/51.9 \log\log p_r)$$

and so by the prime number theorem

$$c_5 \frac{n}{\log n} < p_r^2 \exp(-\log p_r/51.9 \log\log p_r).$$

Therefore

$$P(u_n) = p_r > c_6 n^{1/2} \exp(\log n/103.99 \log\log n),$$

and our result now follows.

**Acknowledgements** Research 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. P.B. Allen, On the multiplicity of linear recurrence sequences. J. Number Theory **126**, 212–216 (2007)
2. F. Amoroso, E. Viada, On the zeros of linear recurrence sequences. Acta Arith. **147**, 387–396 (2011)
3. A. Baker, A sharpening of the bounds for linear forms in logarithms. Acta Arith. **21**, 117–129 (1972)
4. A. Baker, The theory of linear forms in logarithms. In *Transcendence Theory: Advances and Applications*, ed. by A. Baker, D.W. Masser (Academic, London, 1977), pp. 1–27
5. A. Baker, H.M. Stark, On a fundamental inequality in number theory. Ann. Math. **94**, 190–199 (1971)
6. A.S. Bang, Taltheoretiske undersøgelser. Tidsskrift for Mat. **4**, 70–78, 130–137 (1886)
7. Y. Bilu, G. Hanrot, P.M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers. J. reine angew. Math. **539**, 75–122 (2001)
8. G.D. Birkhoff, H.S. Vandiver, On the integral divisors of $a^n - b^n$. Ann. Math. **5**, 173–180 (1904)
9. R.D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. Ann. Math. **15**, 30–70 (1913)
10. H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields* (Springer, New York, 1978)
11. P. Erdős, Some recent advances and current problems in number theory. In *Lectures on Modern Mathematics*, vol. III, ed. by T.L. Saaty (Wiley, New York, 1965), pp. 196–244
12. J.H. Evertse, On sums of $S$-units and linear recurrences. Compositio Math. **53**, 225–244 (1984)
13. K. Ford,F. Luca, I. Shparlinski, On the largest prime factor of the Mersenne numbers. Bull. Austr. Math. Soc. **79**, 455–463 (2009)
14. E. Hecke, Lectures on the theory of algebraic numbers, in *Graduate Texts in Mathematics*, vol. 77 (Springer, New York, 1981)
15. D.H. Lehmer, An extended theory of Lucas' functions. Ann. Math. **31**, 419–448 (1930)
16. T. Loher, D. Masser, Uniformly counting points of bounded height. Acta Arith. **111**, 277–297 (2004)
17. F. Luca, Arithmetic properties of members of a binary recurrent sequence. Acta Arith. **109**, 81–107 (2003)
18. E. Lucas, Théorie des fonctions numériques simplement périodiques. Amer. J. Math. **1**, 184–240, 289–321 (1878)
19. K. Mahler, Eine arithmetische Eigenschaft der rekurrierenden Reihen. Mathematica (Leiden) **3**, 153–156 (1934–1935)
20. K. Mahler, Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen. Proc. Akad. Wetensch. Amsterdam **38**, 50–60 (1935)
21. L. Murata, C. Pomerance, On the largest prime factor of a Mersenne number. In *CRM Proc. Lecture Notes*, vol. 36, ed. by H. Kisilevsky, E.Z. Goren (American Mathematical Society, Providence, 2004), pp. 209–218
22. R. Murty, S. Wong, The *ABC* conjecture and prime divisors of the Lucas and Lehmer sequences. In *Number Theory for the Millennium*, vol. III, ed. by M.A. Bennett, B.C. Berndt, N. Boston, H.G. Diamond, A.J. Hildebrand, W. Philipp, A.K. Peters (Natick, MA, 2002), pp. 43–54
23. E.M. Matveev, An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers II (Russian). Izv. Ross. Akad. Nauk Ser. Mat. **64**, 125–180 (2000)
24. A.J. van der Poorten, Linear forms in logarithms in the $p$-adic case. In *Transcendence Theory: Advances and Applications,* ed. by A. Baker, D.W. Masser (Academic, London, 1977), pp. 29–57
25. A.J. van der Poorten, H.P. Schlickewei, The growth conditions for recurrence sequences. Macquarie Math. Reports 82–0041 (1982)

26. A. Schinzel, On primitive prime factors of $a^n - b^n$. Proc. Cambridge Philos. Soc. **58**, 555–562 (1962)
27. A. Schinzel, The intrinsic divisors of Lehmer numbers in the case of negative discriminant. Ark. Mat. **4**, 413–416 (1962)
28. A. Schinzel, On two theorems of Gelfond and some of their applications. Acta Arith. **13**, 177–236 (1967)
29. A. Schinzel, Primitive divisors of the expression $A^n - B^n$ in algebraic number fields. J. reine angew. Math. **268/269**, 27–33 (1974)
30. H.P. Schlickewei, Linearformen mit algebraischen Koeffizienten. Manuscripta Math. **18**, 147–185 (1976)
31. W.M. Schmidt, The zero multiplicity of linear recurrence sequences. Acta Math. **182**, 243–282 (1999)
32. W.M. Schmidt, Zeros of linear recurrence sequences. Publ. Math. Debrecen **56**, 609–630 (2000)
33. T.N. Shorey, C.L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers II. J. London Math. Soc. **23**, 17–23 (1981)
34. T.N. Shorey, R. Tijdeman, *Exponential Diophantine Equations*. Cambridge Tracts in Mathematics, vol. 87 (Cambridge University Press, Cambridge, 1986)
35. I.E. Shparlinski, Prime divisors of recurrent sequences. Isv. Vyssh. Uchebn. Zaved. Math. **215**, 101–103 (1980)
36. C.L. Stewart, The greatest prime factor of $a^n - b^n$. Acta Arith. **26**, 427–433 (1975)
37. C.L. Stewart, Divisor properties of arithmetical sequences. Ph.D. thesis, Cambridge, 1976
38. C.L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. Proc. London Math. Soc. **35**, 425–447 (1977)
39. C.L. Stewart, Primitive divisors of Lucas and Lehmer numbers. In *Transcendence Theory: Advances and Applications*, ed. by A. Baker, D.W. Masser (Academic, London, 1977), pp. 79–92
40. C.L. Stewart, On divisors of terms of linear recurrence sequences. J. Reine Angew. Math. **333**, 12–31 (1982)
41. C.L. Stewart, On the greatest square-free factor of terms of a linear recurrence sequence. In *Diophantine Equations*, ed. by N. Saradha (Narosa Publishing House, New Delhi, 2008), pp. 257–264
42. C.L. Stewart, On divisors of Lucas and Lehmer numbers. Acta Math. (to appear)
43. C.L. Stewart, K. Yu, On the *abc* conjecture II. Duke Math. J. **108**, 169–181 (2001)
44. M. Waldschmidt, A lower bound for linear forms in logarithms. Acta Arith. **37**, 257–283 (1980)
45. K. Yu, P-adic logarithmic forms and a problem of Erdős. Acta Math. (to appear)
46. K. Yu, L.-k. Hung, On binary recurrence sequences. Indag. Mathem., N.S. **6**, 341–354 (1995)
47. K. Zsigmondy, Zur Theorie der Potenzreste. Monatsh. Math. **3**, 265–284 (1892)